Audit Report

OIG-09-045

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, 2008 to June 30, 2009

August 28, 2009

Office of Inspector General

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

August 28, 2009

MEMORANDUM FOR VAN ZECK, COMMISSIONER
BUREAU OF THE PUBLIC DEBT

FROM: 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, 2008 to June 30, 2009

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, 2008 to June 30, 2009. 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, 2008 to June 30, 2009. 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, 2009,
- 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, 2008 to June 30, 2009, 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 August 27, 2009 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, 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, 2008 to June 30, 2009

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, 2009. 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, 2009. 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, 2008 to June 30, 2009. 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, 2008 to June 30, 2009.

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, 2009, and the information about tests of the operating effectiveness of specific controls covers the period from July 1, 2008 to June 30, 2009. 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

August 27, 2009

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.

As of June 30, 2009 ARC provided financial management services to approximately 50 customer agencies. Financial management services include accounting, budgeting, reporting, travel, procurement 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
Accounts and Reports Branch (ARB)	Reporting Services
Accounting Services Branch (ASB)	Document Processing
Treasury Reporting Branch (TRB)	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
Program Support Branch (PSB)	Deposit Services SPS Operations

Travel Services Division (TSD):

Temporary Duty Services Branch (TDSB)	Temporary Duty Travel Services Operate/Maintain GovTrip Provide GovTrip Training Services Document Processing
Relocation Services Branch (RSB)	Relocation Services Operate/Maintain moveLINQ Record and process relocations Tax Reporting

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

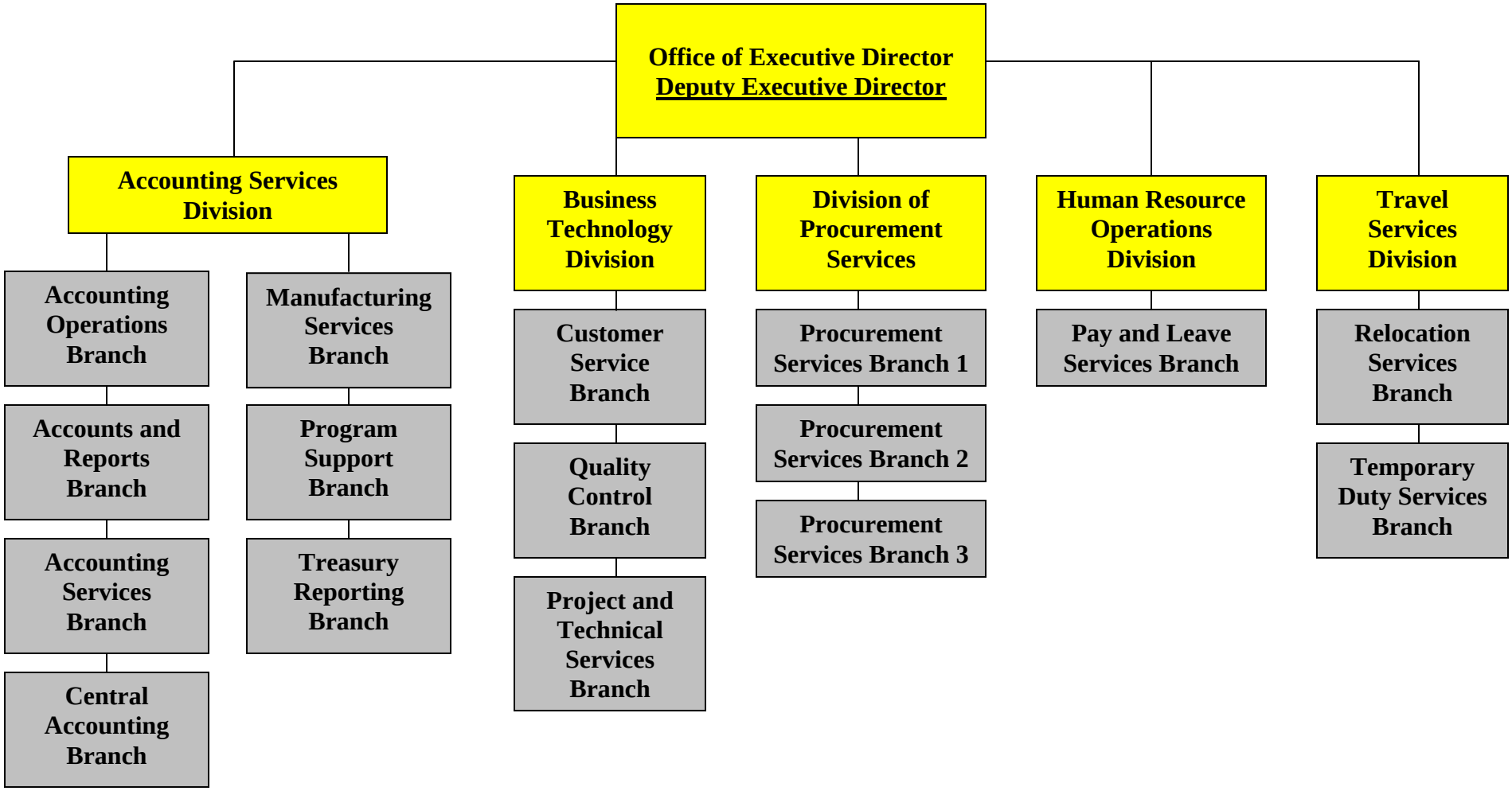
Human Resources Operations Division (HROD):

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

Division of Procurement Services (DPS):

Procurement Services Branch 1 (PSB1)	Acquisition Services
Procurement Services Branch 2 (PSB2)	Acquisition Services
Procurement Services Branch 3 (PSB3)	Acquisition Services

ARC Organizational Chart



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 preferred method 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 method (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 officers 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 U.S. 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 at least bi-weekly (weekly if payroll adjustment files are applicable) 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 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: FMS 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 Temporary Duty

Travel Services consist of the following:

- Operating and maintaining the E-Gov Travel system (GovTrip) 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 Federal Financials (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 Oracle 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 Oracle.

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 an approved *Form PD5409E – Administrative Resource Center (ARC) Online Applications Access Request* or have their approving official or agency travel contact 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 or agency travel contact. Changes to a user's role require a resubmitted PD5409E or e-mail approval from the traveler's approving official or agency travel contact.

Relocation Services

Relocation Services consist of the following:

- Operating and maintaining moveLINQ, a government relocation expense management system in compliance with the Federal Travel Regulations (FTR), Joint Travel Regulations (JTR) and Joint Federal Travel Regulations (JFTR) to record and process permanent change of station moves for customer agencies
- Researching and implementing relocation regulations and Agency/Bureau relocation travel policies
- System Administration
- Providing customer service
- Providing system support and training to internal users
- Evaluating, recommending, and implementing approved changes to the existing system, including working with the moveLINQ vendor, mLINQS, on system enhancements and deficiencies
- Processing relocations through the moveLINQ system
- Processing obligations and disbursements via interface to Oracle Federal Financials (Oracle)

Relocation travel documents (authorizations, amendments, advances, and vouchers) are entered by ARC into moveLINQ. Prior to being submitted in moveLINQ, the vouchers are reviewed for accuracy by a second ARC employee. Completed documents are faxed or digitally scanned and e-mailed to the traveler and/or approving official for review and approval, as appropriate. For customers that we process payments, approved documents are interfaced and reconciled to Oracle daily.

Access to moveLINQ is restricted to ARC users with a valid logon and password. The process for requesting, establishing, issuing, and closing user accounts is controlled through the use of the moveLINQ Online Application Access Request Form which requires supervisor approval. Changes to a user's identification (i.e. name change) require a resubmitted moveLINQ Online Application Access Request Form or e-mail from the user copying his/her supervisor or manager. Changes to a user's role require a resubmitted Application Access Request Form or e-mail approval from the user's supervisor or manager.

Procurement Services

Procurement Services consist of the following:

- Awarding contracts and purchase orders in accordance with Federal Acquisition Regulations and Treasury Acquisition Regulations
- Contract administration

Requests for procurement actions are initiated by customers through requisitions. The requisitions contain a performance work statement or requirements document, estimated dollar amount for the goods or service, validation that funds are available and approval from an authorized official. Requisitions may be sent electronically through PRISM or manually.

Upon receipt of a completed requisition, ARC procurement personnel will develop an acquisition strategy based upon the item or service being purchased and the expected dollar amount of the purchase. Using information from the requisition, ARC personnel will develop and publicize the solicitation requesting proposals. ARC personnel will conduct the evaluation of the proposals with technical team of experts from our customer agencies. With input from the technical team, an ARC contracting officer will select the vendor that best meets the customer's requirements.

Following award of the contract, ARC personnel will provide contract administration services. This includes executing approved and authorized contract modification, resolving issues that arise during the life of the contract, monitoring delivery schedules and closing out the contract at completion.

System Platform Services

ARC maintains system support staff that provide customer services and training activities. Customer support is provided via phone or e-mail. ARC maintains a training course curriculum that is generally provided in a hands-on classroom environment.

ARC performs all system access activities in accordance with established procedures for granting, changing, and removing user access. Included in these procedures are independent reviews of system access activity and user inactivity.

ARC performs all system change activities in accordance with established procedures for evaluating, authorizing, and implementing. To this end ARC maintains responsibility for System Integration Testing, providing customers an opportunity to perform User Acceptance Testing, and approving production changes.

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

Control Environment

ARC Financial Management Service operations are 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.

ARC employees are responsible for processing and reporting accounting activity, providing system support and development services, procurement, and travel services for its 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 Acquisition Regulations, Federal Travel Regulations, FMS 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 Oracle 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

Migration to Commercial Host (Oracle on Demand)

ARC is migrating the hosting of Oracle Federal Financials and PRISM to Oracle Corporation's Oracle on Demand service in three phases. As the hosting company for ARC, Oracle on Demand staff serve as the database and systems administrator and provides back up and recovery services. The Oracle and PRISM systems physically reside in a caged federal environment within Oracle on Demand's Austin Data Center and will only be accessible via VPN between BPD and Oracle on Demand. The first phase for production use (C1) included all but two customer agencies. Phase one was completed on April 14, 2009. The second phase (C2), for one customer agency was completed on May 26, 2009; and the third phase (C3) for one customer agency is scheduled to be completed in February 2010.

Oracle Federal Financials (Oracle)

Prior to migration ARC operated Oracle version 11i, with the Oracle 9i database, which runs within BPD's perimeter security zones and accesses data in the perimeter security zones using Linux as its operating system. BPD's Office of Information Technology (OIT) served as the Oracle database administrator and provides primary support for tape backup and recovery. Security was also provided by OIT through firewall rules and router access control lists. Oracle on Demand operates Oracle version 11i, Oracle 10g database in a Linux operating system environment.

The following Oracle system information is relevant for the entire period – July 1, 2008 through June 30, 2009. 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 accesses the database IP to IP on a specified port that was defined in the Access Control List. Internet access is via a 128-bit Secure Sockets Layer (SSL) encrypted connection. The application is compliant with Section 508 of the Rehabilitation Act Amendment for 1998 for Americans with Disabilities (ADA). Functions of Oracle include budget execution, general ledger, purchasing, accounts payable, accounts receivable, fixed assets, and manufacturing. 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.

GovTrip

ARC uses Northrop Grumman Mission System's (NGMS) GovTrip travel system (system selected by the U.S. Department of the Treasury as its E-Gov Travel solution). NGMS developed and hosts GovTrip. GovTrip is a web-based, self-service travel system that incorporates traditional reservation and fulfillment support and a fully-automated booking process. GovTrip uses 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 daily batch process. GovTrip users consist of travelers, document preparers, budget reviewers, approving officials and administrators.

moveLINQ

ARC uses mLINQS relocation expense management system, moveLINQ, to meet their relocation management program, payment system and reporting requirements. moveLINQ is an E-Gov Travel Services and Federal Travel Regulations, Chapter 302 compliant web-based system that

automates relocation expense management processes, policy and entitlement for both domestic moves and international relocations. The application is used for household goods shipment and storage arrangements, employee travel arrangements, third party real estate payments and relocation tax administration, including W-2 preparation. Approved documents interface to Oracle for obligation or payment during a daily scheduled batch process. moveLINQ users consist of authorized TSD personnel. OIT hosts the moveLINQ system and serves as the Microsoft SQL database administrator and provides primary support for tape backup and recovery.

Procurement Request Information System Management (PRISM)
Prior to migration ARC operated the Compusearch PRISM system as its procurement system for customer agencies serviced by Oracle. ARC operated PRISM version 6.0, with the Oracle 9i database, which runs within BPD's perimeter security zones and accesses data in the perimeter security zones using Linux as its operating system. OIT served as the PRISM database administrator and provides primary support for tape backup and recovery. Security was provided by OIT through firewall rules and router access control lists. Oracle on Demand operates PRISM on Windows operating system and Oracle 10g database in a Linux operating system environment.

The following PRISM system information is relevant for the entire period – July 1, 2008 through June 30, 2009. PRISM uses a two-tier web-based infrastructure with a front-end Internet user interface using Windows as its operating system and a database residing on the secure network. The application 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. Internet access is via a 128-bit SSL encrypted connection. Transactions entered through PRISM interface real-time with Oracle.

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 firewall rules and router access control lists.

PRISM, GovTrip, and moveLINQ are feeder systems that interface with Oracle. webTA feeds data to the National Finance Center (NFC) that is then interfaced with Oracle. ARC and Oracle on Demand personnel maintain Oracle, PRISM, moveLINQ, and the payroll interface that feeds NFC data to Oracle.

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.
- Approve and return relocation travel authorizations to RSB for processing in moveLINQ in a timely manner.
- 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 or constructive acceptance date according to the Prompt Payment Act.
- Approve travel vouchers and accurately enter the vouchers into GovTrip in the proper period.
- Approve and return relocation travel vouchers to RSB for processing in moveLINQ in a timely manner.
- 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 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, 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 and approved 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 17 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$HLINK II, GWA TDO Payments, Intragovernmental Payment and Collection transactions (IPACs)	Each month, Treasury's FMS issues the FMS 6652, *Statement of Differences*, to agency location codes (ALC) when differences are identified between the cash activity reported by the agency on the FMS 224, *Statement of Transaction*s, and data reported to Treasury's CA$HLINK II, GWA TDO Payments, and IPAC systems. ARC accountants minimize month-end disbursement differences by comparing preliminary FMS 224 data to data obtained from Treasury's CA$HLINK II, GWA TDO Payments, and IPAC systems.
	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 Oracle 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.
Dun & Bradstreet	Central Contractor Registration (CCR)	Primary registrant database for the U.S. Federal Government; collects, validates, stores and disseminates data in support of customer agency acquisition missions.
Bureau of the Public Debt	FedInvest	Used to purchase and redeem Government Account Series (GAS) securities; data source for customer agency federal investment interfaced transactions with Oracle.
Oracle Corporation	Oracle on Demand	ARC has migrated the hosting of Oracle and PRISM to Oracle on Demand for the two of the three customer environments (C1 and C2) supported by ARC. C1 was cutover to Oracle on Demand for production use on April 14, 2009, and C2 on May 26, 2009. The third environment, C3, is scheduled to be migrated to Oracle on Demand in February 2010. Oracle on Demand staff serve as the database and systems administrator and provides back-up and recovery services for Oracle and PRISM.

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.

PRISM System Interface

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 the accounting system through an interface between PRISM and 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;
- Data validations;
- Pre-populated fields for default or standard entries;
- Validation of funds availability; and
- Non-editable fields (i.e., total when amount is per unit).

The interface between PRISM and Oracle is monitored periodically throughout the day by systems analysts. The analysts periodically monitor a report that identifies transactions that have been in the Pending Financial Approval status for more than 15 minutes and a report that identifies transactions that were disapproved during the Pending Financial Approval status. The analysts monitor the reports to ensure transactions are processed timely and to identify and investigate any issues. 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.

Manually Recorded Obligations – Customer Agency Approval

For obligations not processed through the interface, customer agencies and/or Procurement send ARC a 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.

Temporary Duty 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 Oracle 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 Oracle as obligations in the general ledger. A Travel Order Status 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. In addition, GovTrip prevents a user from both entering and approving travel authorizations unless they have authorized access.

Relocation Travel System Interface

RSB personnel enter PCS travel authorizations into moveLINQ, print and send them to Approving Officials for review and approval. When the signed document is received by RSB, Relocation Coordinators stamp the document in moveLINQ with a status of "submitted". All "submitted" documents are interfaced daily via batch process to Oracle which records an obligation in the general ledger. Each day an interface file is generated from moveLINQ 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 Oracle as obligations in the general ledger. A Travel Order Status exception report is generated and reviewed daily to identify and correct data interface errors and exceptions between moveLINQ and Oracle. To correct transactions of this nature, the transactions are manually entered into the system. Submitted authorizations in moveLINQ are reconciled daily by an accounting technician with an Oracle generated report to ensure that all moveLINQ authorizations have been interfaced and processed in Oracle. A weekly review of the reconciliation process is performed by a Travel Analyst and any identified issues are resolved.

Budget Execution System Controls

Customer agencies can establish and monitor both legally established and internally developed budget plans in Oracle to ensure obligations are 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 and a high level budget is loaded. Upon receipt and input of a detailed financial plan, controls will be established at the 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. Budget plans input into Oracle by ARC Staff are reviewed and signed off on by an ARC Supervisor.

Document Numbering

All accounting entries recorded into Oracle 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, Oracle 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.
- Approve and return relocation travel authorizations to RSB for processing in moveLINQ in a timely manner.
- 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 determined that the procedures were formally documented for the processing of obligations.
- Inquired of a Financial Systems Analyst in the Quality Control Branch (QCB) and was informed that the system validates data prior to the interface to the Oracle system.
- Observed the validation tables in the PRISM system and noted that the system was configured to validate obligation document types and to ensure accuracy and completeness of the data interfaced from the PRISM system to the Oracle System.
- Observed the PRISM Support Desk Staff monitoring the “Pending Financial Approval” and “Disapproved during Pending Financial Approval” reports and noted that the reports appeared to be monitored, backlogs were not building up, and an issue was noted at the time of observation but was investigated and resolved.

- For a selection of manually entered obligations, inspected evidence of customer agency approval and determined that manually entered obligations were approved prior to being entered into Oracle by ARC Staff.
- Observed the daily GovTrip interface and noted that approved travel authorizations interfaced into the Oracle system and recorded as an obligation.
- For a selection of dates, inspected GovTrip to Oracle interface reconciliations and determined that daily reconciliations were performed to ensure that data from the GovTrip system interfaced to the Oracle System.
- Inspected screen prints from an ARC staff member entering travel vouchers into GovTrip and determined that the system required the travel vouchers to be routed to an approving official.
- Inspected screen prints of an approving official attempt to enter and approve travel vouchers and determined that GovTrip prevented a user from both entering and approving travel vouchers.
- Observed the daily moveLINQ interface and noted that approved relocation authorizations were interfaced into the Oracle system and recorded as an obligation.
- For a selection of days inspect the reconciliation of authorization from moveLINQ to the Oracle System and determined that the interface activity was reconciled to ensure all approved authorizations were completely and accurately interfaced to the Oracle System.
- For a selection of weeks inspected the review evidence of the reconciliation process performed by a RSB Accountant/Travel Assistant and determined that the review was performed weekly and any identified issues were resolved.
- For a selection of customer agencies inspected evidence and determined that for the year they specified their budget controls, they were input by CSB staff, and then reviewed by a supervisor for completeness and accuracy.
- 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. When invoices are sent to ARC, ARC obtains customer agency approval through an executed receiving document, or ARC submits the invoice to an 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, GovTrip, and moveLINQ).

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.

Temporary Duty Travel Vouchers

Customer agencies enter temporary duty 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 Oracle which records a disbursement in the general ledger. Each day an interface file is received from the GovTrip System 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 Oracle as disbursements in the general ledger. The travel voucher is then matched against an existing authorization. A Travel Voucher Status 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. In addition, GovTrip prevents a user from both entering and approving travel vouchers.

Statistical Sampling of Temporary Duty Travel Vouchers

Temporary Duty Services Branch (TDSB) staff completes a post audit review of temporary duty 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 in which the customer agency has declared the overpayment a debt of the government. The traveler sends a check to cover the overpayment.

Relocation Services Travel Vouchers

RSB personnel enter and audit each PCS travel voucher in moveLINQ, print and then send them to Approving Officials for review and approval. When the signed document is received by RSB, Relocation Coordinators stamp the document in moveLINQ with a status of "submitted". All "submitted" documents are interfaced daily via batch processing to Oracle which records a disbursement in the general ledger. Submitted vouchers in moveLINQ are reconciled daily by an Accounting Technician with an Oracle generated report to ensure that all moveLINQ vouchers have been processed in Oracle. A weekly review of the reconciliation process is performed by a Travel Analyst.

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. 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 FMS 224, *Statement of Transactions*, and data reported to Treasury's CA$HLINK II, GWA TDO Payments, and IPAC systems. ARC accountants minimize month-end disbursement differences by comparing preliminary FMS 224 disbursement data to data obtained from Treasury's CA$HLINK II, GWA TDO Payments, 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 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 and a high level budget is loaded. Upon receipt and input of a detailed financial plan, controls will be established at the 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 into Oracle require a transaction or document identification number. System controls 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, Oracle 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 or constructive acceptance date according to the Prompt Payment Act.
- Approve travel vouchers and accurately enter the vouchers into GovTrip in the proper period.
- Approve and return relocation travel vouchers to RSB for processing in moveLINQ in a timely manner.

- 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 determined that the procedures were formally documented for the processing of disbursements.
- For a selection of invoices inspected documentation of Customer Agency authorization and related general ledger entries and determined that disbursements were authorized and processed timely.
- For a selection of Intergovernmental Payment and Collection transactions inspected documentation of Customer Agency authorization and related general ledger entries and determined that disbursements were authorized and processed timely.
- Observed an accountant process an invoice over $2,500 and determined that the system automatically routed the invoice to a secondary lead accounting technician or an accountant for review and approval.
- For a selection of months inspected evidence and determined that the 100% post audit management reviews were conducted monthly on all invoices greater than $2,500 which were both processed and approved by the same individual.
- Observed the daily GovTrip interface and noted that approved travel authorizations interfaced into the Oracle system and were recorded as an obligation.
- For a selection of days inspected GovTrip voucher reconciliations and determined that approved vouchers in GovTrip were reconciled daily to Oracle by an accounting technician.
- Observed a user in GovTrip attempting to approve their own travel voucher and noted that the system automically prevented the user from approving their own travel voucher.
- For a selection of months inspected evidence of the statistical review of invoices less than $2,500 and determined that the statistical review was performed subject to statistical sampling by a lead accounting technician or an accountant.
- For a selection of months, inspected evidence of the supervisor review of temporary duty travel voucher invoices over $2,500 that were processed and approved by the same individual and determined that the supervisor reviewed the invoices and performed follow-up to validate the self-approval.
- Observed relocation vouchers interfaced into Oracle and determined that the approved vouchers were interfaced via automated batch process.
- For a selection of days inspected evidence and determined that the vouchers in moveLINQ were reconciled daily by an Accounting Technician within an Oracle generated report.
- For a selection of weeks inspected reconciliation and determined that a weekly reconciliation process was performed by an RSB Accountant/Travel Assistant.
- For a selection of days, inspected evidence that the ARC SPS certifying officer compared the number and dollar amount of payments and determined that the review was completed daily to ensure interfaces were uploaded completely.

- For a selection of invoices subject to the Prompt Payment Act, inspected documentation and determined that 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).
- For a selection of late payments, inspected evidence and determined that proper interest was calculated and paid based on the number of days the payment was late.
- For an example late payment recalculated the interest owed and determined that Oracle calculated interest and generated an interest payment to the vendor.
- For a selection of months, inspected the Statement of Differences and determined that supervisors reviewed the reconciliations.
- For identified differences from the selection of months and customer agencies, inspected evidence and determined that the accounting technicians or another accountant corrected differences prior to the close of the accounting period or in the subsequent accounting period if necessary based on timing.
- For a selection of customer agencies inspected evidence and determined that for the year they specified their budget controls, they were input by CSB staff, and then reviewed by a supervisor for completeness and accuracy.
- 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 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 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 FMS 224, *Statement of Transactions*, and data reported to Treasury's CA$HLINK II and IPAC systems. ARC accountants minimize month-end differences relating to collections by comparing preliminary FMS 224 collection data to Treasury's CA$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 if necessary, 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 Oracle 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, Oracle 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, and cash receipts, 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, cash receipts, receivables, advances, and write-offs and observed ARC personnel process transactions and noted that the transactions were processed in accordance with the procedures.
- For a selection of unfilled customer orders inspected documentation of Customer Agency authorization and determined that transactions are authorized by Customer Agencies.
- For a selection of receivables inspect documentation of Customer Agency authorization and determined that the transactions were authorized by Customer Agencies.
- For a selection of cash receipts, inspected documentation of Customer Agency authorization and determined that transactions were authorized by Customer Agencies.
- For a selection of months, inspected Statement of Differences reconciliations and determined that reconciliations were documented and that any correcting entries were posted by an accounting technician or another accountant and reported in the subsequent accounting period.

- For a selection of quarters, inspected the Report on Receivables Due from the Public reconciliations and determined that reconciliations were documented.
- 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 quarterly selection of intra-governmental confirmations and reconciliations and determined that confirmations were sent, reconciliations were documented, and trading partners identified.
- Inspected a quarterly selection of non-Treasury and non-Homeland Security customer agency intra-governmental Fiduciary Confirmation System balances and determined that fiduciary account balances were reconciled with trading partner balances.
- Inspected a selection of non-fiduciary transaction confirmations of ARC customer agencies and determined that ARC accountants prepared and submitted confirmations to the appropriate trading partners in accordance with the elimination reconciliation guidance.
- Inspected a selection of transaction(s)/balance(s) reconciliations and determined that upon submitting the confirmations to the trading partners, ARC worked with the trading partners to reconcile transactions/balances and identify and record any necessary adjustments.
- Inspected a selection of reconciliations and determined that confirmations were performed for non-Treasury customer agencies.
- Observed an ARC staff member attempt to enter into Oracle, a transaction with a document number that had already been entered into Oracle noted 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.

Safeguarding Checks

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 accounting technician or administrative staff member 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 the ARC administrative staff member's drawer until it is ready to be deposited.

Manual Deposits – Segregation of Duties

When the check is ready for manual 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 ARC administrative staff member 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 ARC administrative staff member 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, an ARC accounting technician or administrative staff member will 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 ARC accounting technician or administrative staff member. Upon settlement with the FRB, the ARC accounting technician reconciles the batch list with the paper checks and signs off to indicate the reconciliation is complete. After reconciliation, the checks are stamped "VOID" by the ARC accounting technician or administrative staff member and held awaiting confirmation of the deposit in the Federal Reserve's deposit application. Upon confirmation, the ARC accounting technician or administrative staff member destroys the voided checks. The cash receipt is recorded in Oracle by an independent ARC accounting 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 determined that ARC had documented procedures for the safeguarding and recording of deposits.

- Inspected the checks received by the mailroom and the associated batch tickets and determined that a batch ticket with the number of checks received was generated.
- From a selection of batch tickets generated by the mailroom, inspected notes and determined that copies of batch tickets were sent via confidential mail to the appropriate ARC branch.
- Inspected a selection of check logs and determined that an ARC administrative staff member who did not have accounting system access to post account receivable transactions, received, opened and logged all checks received in the branch's check deposit log.
- Inspected a selection of checks received and associated batch tickets and determined that the number of checks received was compared to the number of checks listed on the batch ticket.
- Inspected a selection of check deposit records and check issuance attributes and determined that checks were deposited in a timely manner after the purpose and validity of the check's issuance were identified.
- For a selection of un-deposited checks from the check deposit log, observed the checks and noted they were properly secured in a locked drawer.
- For a selection of checks ready for deposit, observed that the deposit tickets and the checks were placed in a locked bag and picked up by the mail clerk.
- Inspected a selection of signed check deposit logs and determined that a copy of the checks was retained by the ARC administrative staff member for comparison with the receipt and deposit ticket signed by the bank teller.
- 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 exceptions were resolved.

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 determined that the procedures were formally documented for the processing of payroll accruals.
- For a selection of months, inspected payroll accrual invoices for a selection of customer agencies for entry into the system and determined that payroll accruals were entered timely.
- For a selection of months for a selection of customer agencies, inspected supervisor signed payroll verification spreadsheets and payroll accrual invoices for entry into Oracle and determined that payroll accruals were verified and entered timely and then reviewed and approved by a supervisor or manager.

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 first and/or second weeks after the end of a pay period, depending on the payroll provider and the need to record payroll adjustments. Upon converting the data into a format that can be uploaded into Oracle, 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 Oracle. 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 Oracle. 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 Oracle 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 ARC's 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 determined that consistent use of the procedures by staff was likely to help prevent the inaccurate, unauthorized, or untimely entry of payroll disbursements into ARC information systems.
- Inspected an interface error report and determined that during the interface, input files were checked for errors and interface error reports were created if errors were identified and determined that the 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, Undisbursed Appropriation Account Ledger 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 Oracle. 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 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 balance sheet accounts except where account subledgers are not made available to ARC, 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 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 bureaus and other reporting entities 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 Oracle 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 covered by the Chief Financial Officer Act and the Accountability of Tax Dollars Act of 2002. The statements are 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,* and *Statement of Custodial Activity* (when applicable) for all customer agencies. ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements to ensure compliance with the reporting requirements. ARC investigates and resolves any differences between TFM financial statement crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Department of Treasury and Department of Homeland Security customer agencies, quarterly financial statements are produced by departmental systems using the data submitted in TIER. Quarterly consolidated financial statements are submitted to the Director of OMB and the Congress by the Department. ARC accountants compare the quarterly financial statements to ARC's internally prepared financial statements, which is further reviewed by a supervisor, and any differences are resolved.

Financial Statement Variance Analysis

For both Department of Treasury and Department of Homeland Security customer agencies, accountants prepare a quarterly financial statement variance analysis. Explanations for variances that exceed Department materiality thresholds must be provided to the Department. The Department submits a consolidated analysis to OMB. The bureau variance analysis is reviewed by an ARC supervisory accountant and approved by the bureau CFO or designee prior to submission to the Department. The Homeland Security bureau variance analysis is also certified by an ARC manager as part of the CFO certification letter.

For non-Treasury and non-Homeland Security customer agencies, accountants prepare a quarterly financial statement variance analysis for interim periods based on the guidance in OMB Circular

A-136. Explanations for variances that exceed the OMB Circular A-136 guidelines are provided to OMB. The variance analysis is reviewed by an ARC supervisory accountant prior to submission to OMB.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures for the processing of transactions consistent with the USSGL and determined that the procedures were documented.
- Observed the processing of a transaction to an inappropriate USSGL account and noted the existence of Oracle cross-validation rules.
- Inspected a list of users with access to change posting models and determined that the system administrators had access to administer posting models.
- For a selection of posting model changes and additions, inspected ARC supervisory approval of the changes and inspect TFM/USSGL guidance and determined that the changes and additions were authorized and that they were in agreement with TFM/USSGL guidance.
- Inspected evidence of the annual review of USSGL account titles and descriptions and determined that the annual review was performed by ARC supervisors and managers.
- For a selection of months, inspected monthly general ledger account reconciliations and determined that the reconciliations were performed, any exceptions were resolved and the reconciliation was reviewed by an ARC supervisor.
- Inspected a selection of FACTS I edit check reports and determined that FACTS I were completed, reviewed, and any issues were resolved.
- Inspected a selection of Reporting and Reconciliation Internal Control Checklists and determined that the FACTS I was completed.
- Observed the staff run the Oracle job that creates the FACTS II bulk data upload file and noted that the Oracle edit checks were applied to the data, and that the ARC accountant resolved any exceptions.
- Inspected a selection of TIER Submission Checklists and determined that TIER submissions were reviewed by an ARC supervisor.
- For a selection of quarters for a selection of customer agencies, inspected ARC comparison of FMS financial statement crosswalk with ARC's internally prepared financial statements and determined that ARC complied with reporting requirements.
- Inspected results ARC investigation of Treasury's financial statement crosswalk and ARC's internally prepared financial statements and determined that ARC investigated and resolved any differences.
- Inspected a quarterly selection of financial statement reviews and determined that the reconciliations were reviewed and approved by an ARC supervisor.
- For a selection of months, inspected reconciliation of financial statements prepared by Treasury to internally prepared financial statements and determined that reconciliations were performed, any exceptions were resolved and 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 Oracle 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, 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 Oracle. 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 maintain the Treasury's monthly data quality scorecard to be able to review as needed in order to monitor the quality of the data submitted.

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 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 and a high-level budget is loaded. Upon receipt and input of a detailed financial plan, controls will be established at the 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 into Oracle 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, Oracle 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 noted that the processing was in accordance with the procedures.
- For a selection of accruals, inspected documentation of Customer Agency authorization and supervisory accountant review and determined that the accruals were authorized and reveiwed appropriately.

- For a selection of months, inspected non-invoice batch payroll leave accruals and determined that the files were sent to ARC for processing and posting of summary payroll data to the core accounting system.
- For a selection of months, inspected non-invoice non-batch leave accrual and determined that a supervisory accountant reviewed the manually calculated leave accruals to ensure they were properly calculated and input into Oracle.
- 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 scorecard documentation and determined that the scorecards were maintained for supervisory review if neccesary.
- 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 if any exceptions identified they were resolved.
- For a selection of customer agencies inspected evidence and determined that for the year they specified their budget controls, they were input by CSB staff, and then reviewed by a supervisor for completeness and accuracy.
- Observed an ARC staff member attempt to enter a transaction into Oracle with a document number that had already been entered into Oracle 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 TIER,Treasury's data warehouse within Treasury's submission timeline which is generally 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 TIER, Homeland Security's data warehouse, within Homeland Security's submission timeline which is generally 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 department defined data quality standards. In order to monitor the quality of the data submitted, supervisory accountants and managers review, as needed, Treasury's monthly data quality scorecard.

EFT and Prompt Payment

ARC follows the Treasury guidelines for the *EFT* and *Prompt Payment* reports for its customers. ARC accountants or lead accounting technicians 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 covered by the Chief Financial Officer Act 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* and *Statement of Custodial Activity* (when applicable) for all customer agencies. ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements to ensure compliance with the reporting requirements. ARC investigates and resolves any differences between TFM financial statement crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Department of Treasury and Department of Homeland Security customer agencies, quarterly financial statements are produced by departmental systems using the data submitted in TIER. Quarterly consolidated financial statements are submitted to the Director of OMB and the Congress by the Department. ARC accountants compare the quarterly financial statements to ARC's internally prepared financial statements, for supervisory review, and resolves any differences.

Financial Statement Variance Analysis

For both Department of Treasury and Department of Homeland Security customer agencies, accountants prepare a quarterly financial statement variance analysis. Explanations for variances that exceed Department materiality thresholds must be provided to the Department. The Department submits a consolidated analysis to OMB. The bureau variance analysis is reviewed by an ARC supervisory accountant prior to submission to the Department. The Homeland Security bureau variance analysis is also certified by an ARC manager as part of the CFO certification letter.

For non-Treasury and non-Homeland Security customer agencies, accountants prepare a quarterly financial statement variance analysis for interim periods based on the guidance in OMB Circular A-136. Explanations for variances that exceed the OMB Circular A-136 guidelines are provided to OMB with the quarterly financial statement submission. The variance analysis is reviewed by an ARC supervisory accountant prior to submission to OMB.

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 and determined that ARC had documented procedures for the preparation of government-wide reports.
- 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 scorecard documentation and determined that the scorecards were maintained for supervisory review if neccesary.

- 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 financial statements prepared by FARS to internally prepared financial statements and determined that reconciliations were reviewed and that any differences 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, any exceptions were resolved and are reviewed by a supervisory accountant before submission.
- For a selection of quarters, inspected the Report on Receivables Due from the Public reconciliations and determined that reconciliations were documented.
- 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 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 and a high-level budget is loaded. Upon receipt and input of a detailed financial plan, controls will be established at the 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.

Reconciliations – Fund Balance With Treasury (Activity and Balances)

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 FMS 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 FMS 224 disbursement data to month-to-date data obtained from CA$HLINK II, GWA TDO Payments, 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 reconciliations of GWA Account Statement balances to general ledger FBWT balances. 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.
- Approve and return relocation travel vouchers to RSB for processing in moveLINQ in a timely manner.
- 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 the 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 customer agencies inspected evidence and determined that for the year they specified their budget controls, were input into Oracle by CSB staff, and reviewed by a supervisor for completeness and accuracy.
- For a selection of months, inspected budgetary to proprietary account relationship reconciliations and determined that the reconciliations were performed and that any exceptions were resolved.
- For a selection of months for a selection of customer agencies inspected evidence and determined that the accountants perform reconciliations, of GWA Account Statement balances to general ledger FBWT balances and supervisory review was completed.

No exceptions noted.

Control Objective 11 – Budget

Controls provide reasonable assurance that budget entries are 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 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 and a high-level budget is loaded. Upon receipt and input of a detailed financial plan, controls will be established at the 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 FBWT balances. 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 into Oracle require a transaction or document identification number. System controls prohibit the use of duplicate document numbers on budget 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, Oracle 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 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 budget entries and determined that they were consistent with the control description.
- For a selection of customer agencies, inspected evidence and determined that for the year they specified their budget controls, they were input by CSB staff, and then reviewed by a supervisor for completeness and accuracy.
- For a selection of months, inspected monthly general ledger account reconciliations and determined that reconciliations were performed, any exceptions were resolved and the recompilation was reviewed by a supervisor.
- For a selection of months for a selection of customer agencies, inspected evidence and determined that the accountants performed reconciliations, of GWA Account Statement balances to general ledger FBWT balances and supervisory review was completed.
- 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 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. The approver compares the hardcopy documentation to Oracle and approves the journal entry.

Customer Agency Control Considerations

- Send valid and approved 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 the processing of manual journal entries and determined that procedures were documented.
- Inspected the list of Oracle users with the ability to create manual journal entries and determined that they were assigned a supervisor in Oracle and were subject to the automated approval work flow.
- Inspected the list of Oracle users with the ability to approve manual journal entries and the list of users with the ability to enter manual journal entries and determined that users without a specified supervisor did not have the ability to enter a manual journal entry.
- For a selection of journal entries, inspected hardcopy supporting documentation and related Oracle journal entries and determined that the manual journal entries had proper hardcopy documentation and were authorized.

No exceptions noted.

Control Objective 13 - Federal Investments

Controls provide reasonable assurance that Federal investments are authorized, reviewed, processed timely, reconciled, and properly documented in accordance with ARC policies and procedures.

Description of Controls

ARC accountants process purchases of Federal investments in accordance with customer agency instruction. Instructions include the type and amount of securities to be purchased or the amount of residual cash to be retained. An independent accountant reviews investment purchases.

All investment activity is recorded in general ledger through a daily interface between the Federal Investment System (FedInvest) and Oracle. Accountants reconcile investment general ledger accounts to the FedInvest application on a monthly basis to ensure all investment activity has been properly recorded. A supervisor reviews investment account reconciliations.

Tests of Operating Effectiveness and Results of Testing

- For a selection of customer agencies, inspected investment instructions and determined that they were provided to ARC and defined the investment objectives for the agencies.
- For a selection of investment purchases, inspected evidence and determined that an independent accountant reviewed the purchases.
- For a selection of months for a selection of customer agencies, inspected evidence and determined that the accountants reconciled investment general ledger accounts to the FedInvest application in a timely manner.

No exceptions noted.

Control Objective 14 – 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.), 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 and determined that ARC had documented procedures for Suppliers and Banks record changes.
- Inspected a list of users with access to update, modify, or delete Suppliers and Banks records and determined that users had the appropriate privileges.
- Inspected a list of users with access to process vendor payments and determined that users had the appropriate privileges.
- For a selection of changes to Suppliers and Banks records, inspected the reviewed report signed by the reviewing employee and determined that the Suppliers and Banks record changes were reviewed and approved.

No exceptions noted.

PROCUREMENT PROCESSING CONTROLS

Control Objective 15 – Acquisitions and Contracts

Controls provide reasonable assurance that acquisitions are compliant with Federal laws, regulations and policies.

Description of Controls

All simplified acquisitions, commercial item contracts and Uniform Contract Format contract files contain a checklist of file contents, which is completed by a Contract Specialist. A standardized contract file format is also maintained. The checklist and file contents are reviewed by a warranted Contracting Officer, as evidenced by their signature on the award document, to ensure adequacy of documentation and compliance with laws, regulations and policies. Contract officers are warranted by Treasury for certain dollar limits based on experience and training.

Tests of Operating Effectiveness and Results of Testing

- Inspected a selection of simplified acquisitions, commercial item contracts, and Uniform Contracts and determined that a standard format was used and each included a checklist, with the following exception noted:
    - Two of the 25 simplified acquisition files inspected did not include the checklist as defined in the control description.
- For a selection of simplified acquisitions, commercial item contracts, and Uniform Contracts inspected the checklists and determined that the documentation was reviewed by a Warranted Contracting Officer.
- Inspected the contract officer's authorization levels and determined that Warranted Contracting Officers had specified dollar limits.

No exceptions noted, except as described above.

Control Objective 16 – Sufficiently Funded Requisitions

Controls provide reasonable assurance that contract obligations are supported by approved requisitions.

Description of Controls

A Contract Specialist or Contracting officer ensures that each acquisition file is supported by a sufficiently funded requisition. Requisitions are approved by program officials through the PRISM system. Approval specifies that funds are available at the time of the requisition and are then reserved for this purchase through a commitment. Approving officials are granted dollar threshold approval rights by the customer agency. These thresholds are maintained in the PRISM system.

Tests of Operating Effectiveness and Results of Testing

- Inspected a selection of acquisitions and evidence from PRISM and determined that the requisitions were approved by program officials through the PRISM system.
- Inspected the approval limits in the PRISM system and determined that the use of the approval limits in PRISM were configured properly.

No exceptions noted.

GENERAL COMPUTER CONTROLS

Control Objective 17 – 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, GovTrip, and moveLINQ have been documented. The logical access controls are based on Treasury and BPD policies and standards (Treasury Information Technology Security Program TDP-85-01 Volume I), 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 an 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 mailbox by an authorized individual 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 80 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 90 days. After 90 days of inactivity, the user's account will be end-dated. Annually, the ARC sends out a list of system users to each customer agency for review. The Oracle Support Team updates the permissions for users based on the responses received from the customer agencies.

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).

Only CSB and QCB employees along with the SYSADMIN account controlled by Information Technology Support Branch 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. 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.

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. Project and Technical Services Branch (PTSB) can be assigned System Administrator responsibility when management 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 needed.

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

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 all users by calling the Oracle Support Team. Oracle Support Team personnel are responsible for verifying the caller's identity. Once the user logs onto the accounting system, they must establish their own unique password. An Oracle user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

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. When five or more unsuccessful access attempts were made, 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 an 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 80 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 90 days. After 90 days of inactivity, the user's account will be end-dated. Annually, the ARC sends out a

list of users to each customer agency for review. Included for review are requisitioner and buyer approval limits by user. 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. 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.

Updates to a user's PRISM responsibilities are audited by independent employees within CSB. The changes to functional access privileges are reviewed and compared to the changes to the 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 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

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 all users by calling the PRISM Support Team. PRISM Support Team 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. A user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

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. When five or more unsuccessful access attempts were made, 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 are not required to submit 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

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

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 the agency to use in performing a periodic review of access. The list is limited to those timekeepers and supervisors who are not currently responsible for validating or approving time for an active employee at the customer agency. The review ensures that these employees who do not currently validate or approve time on a regular basis still require their role as a timekeeper or supervisor.

User access within webTA is further limited by the role the user is 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. Once the user logs onto the system, they must establish their own unique password. A user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

GovTrip

Access to GovTrip is restricted to users with a valid logon ID and password. All users must complete the self-registration process. An account token will be forwarded to the user by the TSD helpdesk after the self-registration information is verified for the user to activate their account. 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 an approved *Administrative Resource Center Online Applications Access Request* or have an approving official 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 or agency travel contact. 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 staff creates reports of GovTrip users and distribute the reports to customer agency Travel for review and verification of the accounts.

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

- System administrators (NGMS only)
- Application administrators; Designated TDSB staff
- Application administrators; Customer Service Help Desk Tier 2, Designated TDSB staff

- Customer Service Help Desk Tier 1, Designated TDSB Staff
- Approving Officials and Budget Reviewers
- User; Traveler and Document Preparer
- Terminated Users; Invitational Travelers

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

Users must establish their own unique GovTrip password. A user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

moveLINQ

Access to moveLINQ is restricted to authorized TSD users with a valid logon ID and password. The process for requesting, establishing, issuing, and closing user accounts is controlled through the use of the moveLINQ Online Application Access Request Form which requires supervisor approval. The form defines the user's access specifications, which will allow the user to perform his/her duties in moveLINQ. Changes to a user's identification (i.e., name change) or to the user's role in moveLINQ also require a moveLINQ Online Application Access Request Form or e-mail from the user's supervisor or manager. The user access list is reviewed by management every time a change is made or six months from the last review, whichever is longer.

User IDs are assigned to authorized TSD employees consistent with their network logon ID. A temporary password is assigned to moveLINQ users in person or by phone. Once the user logs onto moveLINQ, they must establish their own unique password which is encrypted. A user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

moveLINQ has user access roles that separate permissions from highest to lowest into these categories:

- Administrator
- SAR (Non-Admin)
- AUTH TSD Management
- Relocation Coordinator Level 1
- Relocation Coordinator Level 2
- Tech – RITA Only
- Special OA
- Tech
- Viewer

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

See Control Objective 19 for further discussion of the physical access control process.

Customer Agency Control Considerations

Customer agencies should establish controls to:

- Review and approve listing of users with current Oracle, 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 the security policies and procedures were documented for Oracle.
- Inspected PRISM user account management procedures and password procedures and determined that security policies and procedures were documented for PRISM.
- Inspected webTA user account management procedures and password procedures and determined that security policies and procedures were documented for webTA.
- Inspected GovTrip user account management procedures and password procedures and determined that security policies and procedures were documented for GovTrip.
- Inspected moveLINQ user account management procedures and password procedures and determined that security policies and procedures were documented for moveLINQ.
- Inspected screen prints of a logon session and determined that Oracle users required a valid login ID and password and that logins/sessions were encrypted with 128-bit SSL encryption.
- For a selection of new Oracle users, inspected user access request forms and determined that the forms were completed, access authorized, and contained employees signature to denote that they understood the privacy act requirements.
- For a selection of changes to Oracle user profiles, inspected authorizing documentation and determined that updates to access rights were authorized.
- Inspected a selection of requests for termination of customer agencies employees' Oracle access and evidence of when the account was end dated in the Oracle system and determined that requests for termination of access from customer agencies was competed in a timely manner.
- From the selection of inactive Oracle user account reviews, inspected evidence and determined that the accounts inactive for 80 or more days were end dated in the system.
- For a selection of customer agencies, inspected evidence of the annual Oracle user access review and determined that the annual reviews were performed.
- Inspected the list user accounts and access in Oracle and determined that each user's access was restricted to distinct operating units or customer agencies.
- Inspected the user roles assigned to the Oracle System Administrators and compared them to the BTD Allowable Responsibilities Table, and determined that the functional user permissions were restricted commensurate with job responsibilities.
- Observed and inspected a screenshot of an Oracle System Administrator attempt to add responsibilities to their user ID, and noted that System Administrators could not add responsibilities to their user IDs.

- For a selection of occurrences, inspected documentation authorizing the use of temporary Oracle Administrator Access and determined that the access was documented, and approved and revoked when no longer needed.
- Inspected the access control lists for the Oracle database and the host server and determined that the function user permissions were restricted commensurate with job responsibilities.
- Inspected the Oracle user list and determined that the accounts followed the naming convention.
- Inquired of the Supervisory Financial Systems Analyst and was informed that passwords were distributed to new external users via telephone after confirmation of user identity.
- Inquired of the Supervisory Financial Systems Analyst and was informed that upon initial login new accounts must establish a new password.
- Inspected Oracle profile options and determined that Oracle was configured to disconnect sessions if they remained inactive for 30 minutes.
- 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, observed the password lifespan days established for the individual users and noted 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 violation logs were reviewed.
- Inspected a screen print of a logon session and determined that user ID and password were required and that PRISM logins/sessions were encrypted with 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 a list of PRISM users and determined that separated employees did not retain access to the PRISM.
- For a selection of days, inspected the PRISM inactive reviews and determined that the reviews were performed on a daily basis.
- Inspected evidence of distribution of PRISM user lists for review and determined that user account lists were distributed on an annual basis for review.
- Observed and inspected a screenshot of the production PRISM system for a user and noted that system was configured as defined in the control and in the New User Setup document.
- Inspected a selection of modified PRISM access reviews and determined that they were reviewed by an independent reviewer.
- Inspected the access control lists for the PRISM backend database and the host server and determined that the System Administrator and DBA privileges were commensurate with job responsibilities.

- Inspected the PRISM user list and determined that accounts appear to the naming convention, using first initial and second initial if necessary and last name.
- Observed the PRISM Support Team member creating a new account in the PRISM system and noted that upon first login the user was immediately directed to reset their password.
- Inspected PRISM password settings and determined that failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.
- Inspected PRISM configuration settings and determined that the PRISM sessions were configured to time-out if they remained inactive for 30 minutes.
- For a selection of dates, inspected PRISM violation logs and evidence of review and determined that violations logs were reviewed.
- Observed a logon session and noted that the webTA logins/sessions required user name and password.
- Observed a user log into webTA and noted 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.
- Inspected a list of separated employees and a list of webTA users and determined that the separated employees did not retain access to the webTA application, server, or database.
- For a selection of customer agencies, inspected evidence of distribution of a list of webTA supervisors and timekeepers for annual user account review by the customer agency and determined that annual reviews of access were completed.
- Inquired of ARC management and was informed the privileges provided within webTA were provided based on the concept of least privilege.
- Inspected the BPD user privileges with webTA and determined that users were assigned in a role based security configuration.
- Inspected the BPD user privileges within webTA and determined that users assigned HR Administrators did not have Administrator access.
- Inspected the webTA user privileges for a selection of customer agencies and determined that users were assigned in a role based security configuration, and if users assigned HR Administrator did not have Administrator Access.
- Inspected the webTA user privileges for a selection of customer agencies and the BPD group and the BTD phone list and determined that users with Administrator access were restricted to employees in BTD group.
- Observed webTA for an initial login and noted that the user was required to create a new password at first login.
- 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 10 minutes.
- Observed a user access the GovTrip system and noted that a user needed to be authenticated prior to accessing the system.
- For a selection of new GovTrip users, inspected user access request forms or e-mails and determined that the forms or e-mails 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 the separated employees did not retain access to the GovTrip application.
- Inspected evidence of distribution of GovTrip user lists for review and determined that user account lists were distributed on an annual basis for review.
- Inquired of ARC management and was informed that the privileges provided within GovTrip were provided based on the concept of least privilege.
- Inspected the user privileges with GovTrip and determined that users were assigned in a role based security configuration from highest to lowest.
- Observed a GovTrip user attempt to change their password to an invalid setting and determined that the system automatically prevented the use of password that did not confirm to the requirements, with the following exception noted:
    - The password settings in GovTrip did not enforce one aspect of the password complexity requirements.

      Remediation efforts were performed by BPD. A patch for the enforcement of password configuration settings was placed into production on June 20, 2009. Observed an ARC employee on June 22, 2009, attempt to change a password to an invalid setting and determined that GovTrip automatically prevented the use of invalid password settings that did not conform to the requirements.
- Observed a moveLINQ user login to the web based system and noted that they were required to enter a user ID and password.
- Inspected a selection of reviewed moveLINQ user access lists and determined that the review of access was performed.
- Inspected documentation for a selection of added moveLINQ users and determined that the requests were documented and approved.
- Inspected a selection of moveLINQ modification requests and determined that the requests were documented and approved.
- Inspected a selection of moveLINQ termination requests and determined that the removal of access was documented and performed.
- Inspected the list of ARC separations and the active list of movLINQ accounts and determined there were no accounts of terminated employees on the system.
- Inspected the current moveLINQ user list and determined that accounts were assigned with a network IDs.
- Observed and noted that a moveLINQ user must reset their passwords upon initial login.

- Observed a moveLINQ user attempt to change their password to non-compliant passwords to test length and complexity requirements and noted that the system prevented the changes.
- Observed a moveLINQ user enter the incorrect password 3 times and determined that the system locked the user account.
- Inspected the user privileges with moveLINQ and determined that users were assigned in a role based security configuration from highest to lowest.

No exceptions noted, except as described above.

Control Objective 18 – System Changes

Controls provide reasonable assurance that system application 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. Prior to the Oracle on Demand migrations, ARC System Administrators served as facilitators of the formal change management process using iETSolutions Workcenter (iET), a COTS application, maintained by BPD's Office of Information Technology, that provides change management, incident tracking, and service request logging capabilities. Beginning with the migration to Oracle on Demand in April and May 2009, ARC System Administrators continue as facilitators of the formal change management process via MetaLink, Oracle's on Demand's web based service request system.

Additional information regarding the Oracle migration is contained in the Information and Communication section of this report.

Oracle and PRISM

For Oracle and PRISM, ARC uses iET/Metalink 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/Oracle on Demand.

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. PTSB staff develops customizations in separate development instances. QCB staff test changes by running test scripts and analyzing the results. Upon successful completion of testing, QCB staff approves the change request and forward it to the performer of the change, OIT/Oracle on Demand database administrators. After the approved request has been completed, the performer updates the request in iET/MetaLink 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 System Administrators document the emergency change in iET on the next business day.

webTA

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.

GovTrip

GovTrip is hosted and maintained by NGMS at their facility. NGMS informs 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.

moveLINQ

moveLINQ is hosted by OIT and maintained at BPD. mLINQS informs the RSB Manager and moveLINQ System Administrators of scheduled updated system releases and the changes contained therein. System changes are also initiated by moveLINQ System Administrators who make enhancement requests to mLINQS for changes to be included by mLINQS in future scheduled release updates. moveLINQ System Administrators test all moveLINQ changes in a moveLINQ test environment. If any of the changes included in a scheduled moveLINQ release update fail the System Administrators testing, RSB may delay implementation of the update until the release passes the testing. RSB has documented procedures for testing and implementing moveLINQ changes. RSB uses the Bureau's iETSolutions Workcenter (iET) to track changes to the system.

Tests of Operating Effectiveness and Results of Testing

- Inspected written procedures and determined that ARC had documented procedures for the testing, approving, and documenting changes.
- Inspected the access control lists for the Oracle database and the host server and determined that the System Administrator and Database Administrator (DBA) privileges were commensurate with job responsibilities.
- Inspected the access control lists for the PRISM back-end database and the host server and determined that the System Administrator and DBA privileges were commensurate with job responsibilities.
- Inspected the webTA system maintenance agreement and determined that the agreement contained system maintenance provisions and that it was current.
- Inspected a selection of webTA upgrades and emergency changes processed in the iET system and determined that the documentation of testing and approval was completed.
- Inspected the GovTrip system maintenance agreement and determined that the agreement contained system maintenance provisions and that it was current.
- For a selection of GovTrip changes, inspected documentation of testing and determined that the changes were tested prior to implementation in production.

- Inspected written procedures and determined that the testing of GovTrip changes were in accordance with the procedures.
- Inspected the moveLINQ system maintenance agreement and determined that the agreement contained system maintenance provisions and that it was current.
- For a selection of moveLINQ changes, inspected documentation of testing and determined that changes were tested prior to implementation in production.
- Inspected written procedures for testing moveLINQ changes and determined that change procedures were formally documented.
- Observed iET and noted that the system was designed to retain the necessary change management documentation and noted when a change to iET was made.
- Inspected a selection of changes processed in the iET system and determined that the changes were tested and approved prior to implementation to the production environment.
- Inspected a selection of emergency changes processed in the iET system and determined that the emergency change process was followed and properly documented.
- Inspected the Oracle on Demand maintenance agreement and determined that the agreement contained system upgrade and maintenance provisions.
- For a selection of Oracle on Demand changes via MetaLink,, inspected documentation of testing and determined that the changes were tested prior to implementation in production.

No exceptions noted.

Control Objective 19 – Non-interruptive System Service

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

Description of Controls

Prior to the Oracle on Demand migrations, Oracle, PRISM, webTA, and moveLINQ servers resided in OIT's data center. The hosting of Oracle and PRISM for two of the three ARC customer environments were migrated to Oracle on Demand with the cutover dates of April 14, 2009 and May 26, 2009, respectively.

Additional information regarding the Oracle migration is contained in the Information and Communication section of this report.

BPD has documented policies and procedures for controlling physical access to BPD buildings and to the data center. These include:

- Identification of sensitive/critical areas to which access needs to be restricted.
- Physical access controls designed to detect unauthorized access.
- Procedures for log reviews and investigation of violations.

The Security Branch issues employee badges, after performing security background checks and fingerprinting.

Employees are required to have badges available at all times upon request.

Terminated employees are required to surrender identification badges and are removed from the Physical Access Control System (PACS) system immediately.

Physical access to the OIT Data Center is restricted to authorized users only. An employee needing access to the data center must have his/her Branch Manager request access. The requests are made through iET, a workflow system that is used to approve data center access. After the Branch Manager completes and submits the iET request form, requests are forwarded to OIT's data center managers for approval in the iET. If OIT approves the request, the BPD Division of Security and Emergency Preparedness (DSEP) Security Branch grants access via PACS. Only designated DSEP specialists have access to PACS. Access to all sensitive areas requires use of a badge. The use of a badge provides an audit trail that is reviewed by OIT management monthly for potential access violations. Any unauthorized access attempts are followed-up on by contacting the individual's supervisor.

Individuals without badge access to the data center must be escorted to the command center and are required to sign in/out of a Visitor log to be issued a data center visitor badge. Visitor badges do not have access to the data center, but rather designate the individual as a visitor. This log is maintained at the main entrance to the data center.

Vendors that are authorized to have a badge are issued a one-day badge and must leave their access badge onsite following completion of work in the data center. A log of One-Day badges is maintained and reviewed daily.

OIT performs a monthly review and reconciliation of individuals with data center access to individuals authorized to have data center access. Additionally, OIT performs an annual review and recertification of individuals with access to the data center. 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 or whether to provide authorization for their access.

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

The hosting of Oracle for two of the three customer environments were migrated to Oracle on Demand. The cutover dates were April 14, 2009 and May 26, 2009, respectively.

After the migration, Oracle on Demand performed the following controls for Oracle:

For C1, Oracle production archive logs are sent to an off-site contingency location every 30 minutes. For C2, Oracle nightly production back-up is used to refresh the off-site contingency site. The Oracle contingency sites are tested annually as part of the bureau-wide Business Functionality Test (BFT) exercise.

Oracle on Demand performs daily backups of the database, application code tree, archive logs, and control files and store on a file server for 5 days. Additionally, semi-weekly backups are performed of the database, application code tree, archive logs, and control files, and are stored on tape and retained for five weeks.

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 the Oracle Corporation. The Oracle Support Team is available for users to call if they are experiencing difficulties with the system.

From July 1, 2008 through the cutover dates, OIT performed the following controls for Oracle:

At no less frequently than 15-minute intervals, the Oracle production archive logs were sent to the off-site Oracle CONTINGENCY server via the Oracle archiver. The Oracle CONTINGENCY server was tested annually as part of a bureau-wide BFT.

OIT performs complete backups of the AppTier and database nightly. The databases are copied to the CONTINGENCY server nightly for failover and redundancy. OIT copies the AppTier to CONTINGENCY on an as needed basis. Additionally, OIT perform differential backups of the production system nightly and perform 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 20 for further discussion of the backup process.

PRISM

The hosting of PRISM for two of the three customer environments have been migrated to Oracle on Demand; The cutover dates were April 14, 2009 and May 26, 2009, respectively.

After migration, Oracle on Demand performed the following controls for PRISM:

For C1, PRISM production archive logs are sent an off-site contingency location every 30 minutes. For C2, PRISM nightly production back-up is used to refresh the off-site contingency site. The PRISM contingency sites are tested annually as part of the bureau-wide (BFT) exercise.

Oracle on Demand performs daily backups of the database, application code tree, archive logs, and control files and store on a file server for 5 days. Additionally, semi-weekly backups are performed of the database, application code tree, archive logs, and control files, and are stored in tape and retained for five weeks.

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.

From July 1, 2008 through the cutover dates, OIT performed the following controls for PRISM:

At no less frequently than 15-minute intervals, the PRISM production archive logs were sent to the off-site PRISM CONTINGENCY server via the Oracle archiver. The PRISM CONTINGENCY server was tested annually as part of a bureau-wide BFT.

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 20 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 20 for further discussion of the backup process.

GovTrip

ARC TSD staff investigates and attempts to resolve any system issues noticed by the ARC staff or reported to TSD by GovTrip users. When possible, TSD staff resolves GovTrip issues. If TSD staff 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.

moveLINQ

ARC purchases new license agreements annually from mLINQS, which include all upgrades and service packs, monthly per diem rates, Federal travel regulation updates, and unlimited technical support.

moveLINQ System Administrators investigate any system issues noticed by the OIT Database Administrators or reported to them by moveLINQ users. When possible, moveLINQ System Administrators resolve moveLINQ issues. If the administrator cannot resolve an issue, the issue is escalated to mLINQS, the vendor. The System Administrator notifies the users of the length of the expected problem and notifies them again when the issue is resolved.

At no less frequently than 15-minute intervals, the moveLINQ database is automatically replicated to the off-site moveLINQ CONTINGENCY server. The moveLINQ CONTINGENCY server is tested annually as part of a bureau-wide BFT.

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 20 for further discussion of the backup process.

RSB maintains the data in the moveLINQ system for six years and three months.

Tests of Operating Effectiveness and Results of Testing

- Inspected physical access policies and procedures for the data center and determined that they were documented and that they included the identification of sensitive/critical areas to which access needs to be restricted, physical access controls designed to detect unauthorized access, and procedures for log reviews and investigation of violations.
- Observed physical access controls of BPD buildings and the OIT data center and noted that the security guards, video cameras, badge readers, and locked doors were in place and in operation to restrict access.
- Observed persons entering BPD buildings and noted that persons were required to place any materials, packages, bundles, etc. onto an x-ray machine, and additionally were required to pass through a walkthrough metal detector.
- Observed persons entering BPD buildings and noted that an activation of the walkthrough metal detector resulted in further screening by the security guard, utilizing a handheld metal detector to identify the source of activation.

- Observed an entrant swipe their badge into the access control system and noted that the controls system granted access to authorized personnel.
- Inspected a list of employees with card key access to the data center and tape storage room from the card security system and an OIT phone list showing employees requiring access to the data center and tape storage room and determined that physical access to the OIT data center was restricted to authorized employees only.
- For a selection of employees and contractors granted access to the data center, inspected the iET record for granting access and determined that access was approved by the data center manager.
- For a selection of dates, inspected visitor logs and determined that visitor logs were used.
- For a selection of dates, inspected the daily shift logs and determined that an inventory of vendor badges was performed.
- Inspected documentation of the monthly review of physical access privileges to the data center and determined that access privileges were reviewed.
- Inspected documentation of the semi-annual review of physical access privileges to the data center and determined that access privileges were reviewed.
- Inspected documentation of the annual recertification of physical access privileges to the datacenter and determined that access privileges were recertified.
- 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.
- 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.
- 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.
- 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 reviews these logs and alerts.
- Observed HP Openview and noted that this application was installed and in use by OIT staff and provided record of availability of network infrastructure.
- 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 uninterruptible power supply (UPS), and the emergency power generator and determined that the generator and UPS were maintained.
- Observed deployed environmental controls and noted that environmental controls were present.

- Observed the Oracle system operations manuals and determined that the manuals were available to support personnel.
- Observed internal application setup and security documentation, as well as various manuals and documentation produced by Oracle and determined that Oracle support personnel had adequate access to materials.
- Inspected the agreement with the offsite storage vendor and determined that a formal agreement was in place for the offsite storage of digital data received on a weekly basis.
- Inspected the Oracle CONTINGENCY server test documentation records and determined that the server was tested as a part of the bureau-wide Business Functionality Test.
- Inspected a daily selection of AppTier and database backup records and determined that AppTier and databases were copied to the CONTINGENCY server nightly for failover and redundancy.
- Inspected a nightly selection of the Oracle production system backups and determined that nightly differential and weekly full tape backups had been performed.
- Observed Oracle picking and packing lists to note that daily backup tapes were sent to an offsite facility on a weekly basis for eight weeks and that the monthly backup tapes were then sent to a long-term offsite facility.
- Observed PRISM application setup and security documentation and system manuals and noted 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 the PRISM system logs and determined that the logs documented the offsite storage of data on a weekly basis.
- Inspected the PRISM CONTINGENCY server test documentation records and determined the server was tested as a part of the bureau-wide Business Functionality Test.
- Inspected a nightly selection of the PRISM production system backups and determined that nightly differential and weekly full tape backups were performed.
- Observed PRISM picking and packing lists and noted that daily backup tapes were sent to an offsite facility on a weekly basis for eight weeks and that the monthly backup tapes were then sent to a long-term offsite facility.
- Inspected ARC's maintenance agreement for webTA and determined that it was current.
- Inspected a nightly selection of the webTA production system backups and determined that nightly differential and weekly full tape backups were performed.
- Observed webTA picking and packing lists noted that daily backup tapes were sent to an offsite facility on a weekly basis for eight weeks and that the monthly backup tapes were sent to a long-term offsite facility.
- Inspected the GovTrip incident escalation procedures and determined that the incident escalation procedures were documented and available to support ARC staff personnel in investigating and attempting to resolve any system issues.
- Inspected the GovTrip incident escalation procedures and determined that if a TSD staff could not resolve an issue, the issue was escalated to NGMS.

- Observed GovTrip backup rotation logs and determined that offsite backup tape retention was six years and three months.
- Inspected ARC's maintenance agreement with mLINQS and determined that the agreement required mLINQS to provide software and technical support for moveLINQ.
- Inspected RSB System Administrators escalation procedures and determined that if an RSB Administrator could not resolve an issue, the issue was escalated to mLINQS.
- Inspected the agreement with the offsite storage vendor and determined that a formal agreement was in place for the offsite storage of moveLINQ data on a weekly basis.
- Inspected a yearly selection of moveLINQ CONTINGENCY server test documentation records and determined that the server was tested as a part of the bureau-wide Business Functionality Test.
- Inspected a nightly selection of the moveLINQ production system backups and determined that nightly differential and weekly full tape backups were performed.
- Observed moveLINQ picking and packing lists and noted that daily backup tapes were sent to an offsite facility on a weekly basis for eight weeks and that the monthly backup tapes were then sent to a RSB long-term offsite facility for six years and three months.

No exceptions noted.

Control Objective 20 – Records Maintenance

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

Description of Controls

The hosting of Oracle and PRISM for two of the three customer environments have been migrated to Oracle on Demand. The cutover dates were April 14, 2009 and May 26, 2009. Effective on these dates, data backups of Oracle and PRISM are now performed by Oracle on Demand. Oracle on Demand performs daily backups of the database, application code tree, archive logs, and control files and store on a file server for 5 days. Additionally, semi-weekly backups are performed of the database, application code tree, archive logs, and control files and are stored on tape and retained for 5 weeks.

Additional information regarding the Oracle migration is contained in the Information and Communication section of this report.

Both prior to and post Oracle on Demand migrations, OIT/Division of Technology Services (DTS) performs data backups of the moveLINQ application.

From July 1, 2008 through the cutover dates, OIT performed the following controls:

OIT/DTS performs backups of specified distributed systems and applications as identified by the data owners. These backups are performed by the guidelines set forth in the Standard Operating Procedures. Once the backups have been completed, the media can be moved to an alternate facility as long as the data is encrypted. Once media is identified as needing to be moved off-site, Enterprise Infrastructure Branch (EIB)/Data Archival and Retrieval Team (DART) is notified with the specified media ID numbers and the desired retention period. EIB/DART will remove the specified media from the tape library and send it to CAPS in sealed containers. The location of media is tracked by the various systems that create the images on the media using data backup utilities. In addition EIB/DART maintains copies of all contingency site transmittal sheets that list the media sent in each shipment. Once a week media is picked up and returned by the off-site storage provider. Long-term offsite storage is provided through a contract. Authority to recall tapes from off-site is limited to those individuals identified on a list maintained by the off-site storage provider.

Based on the requirements for the data in the accounting, procurement and relocation systems, backup tapes are created daily, weekly, and monthly. Daily tapes are retained onsite for four weeks in the data center tape vault. Weekly and monthly tapes are stored offsite with a tape storage vendor. Weekly tapes are retained for eight weeks offsite and monthly tapes for two years to indefinitely depending on the data contained. For the HR time clock system tapes are created weekly and stored off site for two to eleven years depending on the data.

When tapes are returned from long-term storage, 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 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.

Record Storage

Filesurf is a National Archives and Records Administration (NARA) approved records storage system used by ARC. 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 either stored in boxes or they are scanned and stored electronically.

Data records that will be retained in hard copy are packed into boxes and 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 FileSurf. BPD's 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. The destruction date is calculated using the approved retention period and the latest document date.

Hard copy data records may also be scanned and saved electronically in FileSurf. PDF data records are stored in FileSurf folders based on the data's calculated destruction date using the approved retention period and the latest document date. This method provides for quicker access to archived data.

For relocation documents, active hard copy records are locked after hours. Inactive and closed hard copy records are maintained in a locked onsite storage room.

Tests of Operating Effectiveness and Results of Testing

- Observed the online tape management system and deteremined that data was encrypted prior to being written to tape and sent off site.
- Inspected a list of individuals with authority to recall tapes from offsite storage and their job descriptions and determined that authority to recall tapes was commensurate with job responsibilities.
- Observed the online tape management system and contingency site Tape Manifests and noted that tapes were kept at three separate locations.
- Inspected the agreement with the offsite storage vendor and determined that a formal agreement was in place for the offsite storage of media.
- Observed Operations Personnel step through the process of opening received packages of tapes from contingency site and noted that they compared the contents of the package to the tape management records.
- Inspected full physical inventory documents of all backup tapes that were in BPD's possession and determined that the annual tape inventory was performed.
- 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 successfully completed.

- Observed the location of the on-site hard copy records and noted that the hard copy records were stored on-site in folders for specified time period.
- Inspected an example of hard copy records offsite shipment box and determined that appropriate descriptions were documented.
- Inspected an example of hard copy records offsite shipment logs and determined that the hard copy records were labeled and stored.
- Inspected hard copy records destruction logs and determined that the hard copy records were labeled and stored.
- Observed the FileSurf system and noted that the records could be created, requested, and saved electronically using FileSurf, which was maintained by IMB.
- Observed the location of the active hard copy data records and noted that the hard copy records were locked after hours.
- Observed the location of the inactive hard copy data records and noted that the hard copy records were stored in a locked onsite storage room.
- Inspected the list of authorized individuals that had access to the onsite storage room and determined that only authorized individuals have access.

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 Business Continuity Plan (BCP), last updated January 2008. 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 Disaster Recovery Plan (DRP).

OIT uses the NetBackup from Veritas to backup networked systems. Short-term storage of Oracle tapes are maintained at a Contingency Alternate Processing Site (CAPS) facility. Long-term tape storage is maintained at an offsite location.

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 where they are retained for seven years.

OIT performs complete backups of the production database and AppTier nightly. OIT copies the AppTier to CONTINGENCY on an as needed basis. All critical datasets are retained for at least three years at a long-term offsite facility.

At 15-minute intervals, the Oracle production system archive logs are copied to the off-site Oracle CONTINGENCY server via the Oracle archiver. The Oracle CONTINGENCY server is tested annually as part of a bureau-wide BFT exercise.

OIT performs differential backups of the webTA 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.

OIT performs differential backups of the moveLINQ production database nightly and performs a full tape backup weekly. The nightly backups are sent to an offsite facility on a weekly basis where they are kept for eight weeks. The monthly backup tapes are sent to a long-term offsite facility. At 15-minute intervals, the moveLINQ database is automatically replicated to the off-site moveLINQ contingency server. The moveLINQ application is tested annually as part of a bureau-wide BFT exercise.

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 building management protects ARC and OIT facilities. Alarms are active 24 hours a day, 7 days a week, and are tied-to a local alarm services company 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. Oracle has been classified as a critical application.

As part of the ARC BCP, should ARC facilities become unavailable, essential ARC personnel will relocate to the CAPS facility to reestablish their essential functions. ARC 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 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, 2009, and have issued our report thereon dated August 27, 2009. 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, 2009. The control objectives were specified by the management of 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, 2008 to June 30, 2009, 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, 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

August 27, 2009