Audit Report

OIG-20-044

FINANCIAL MANAGEMENT

Report on the Bureau of the Fiscal Service's Description of Administrative Resource Center's Financial Management Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2019 to June 30, 2020

September 17, 2020

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

**OFFICE OF
INSPECTOR GENERAL**

September 17, 2020

**MEMORANDUM FOR TIMOTHY E. GRIBBEN, COMMISSIONER
BUREAU OF THE FISCAL SERVICE**

FROM:	James Hodge /s/ Director, Financial Audit
SUBJECT:	Report on the Bureau of the Fiscal Service's Description of Administrative Resource Center's Financial Management Services and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2019 to June 30, 2020

We hereby transmit the attached subject report. Under a contract monitored by our office, KPMG LLP (KPMG), an independent certified public accounting firm, examined the Bureau of the Fiscal Service's description of Administrative Resource Center's (ARC) financial management services (accounting, human resources, travel, and procurement services, general computer, and monitoring controls) "ARC's system"; and the suitability of the design and operating effectiveness of these controls. This report includes management's description of ARC's system, management's written assertion, and KPMG's independent service auditor's report. 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 Standards for Attestation Engagements Number 18, *Attestation Standards: Clarification and Recodification*.

In its examination, KPMG found in all material respects:

- the description fairly presents ARC's system that was designed and implemented throughout the period July 1, 2019 to June 30, 2020;

- the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2019 to June 30, 2020, and subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2019 to June 30, 2020; and
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2019 to June 30, 2020 if complementary subservice organization and customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2019 to June 30, 2020.

In connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an examination in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on Fiscal Service's description of ARC's controls, the suitability of the design of these controls and the operating effectiveness of controls tested. KPMG is responsible for the attached independent service auditor's report dated September 14, 2020, and the conclusions expressed therein. However, our review disclosed no instances where KPMG did not comply, in all material respects, with generally accepted government auditing standards.

If you wish to discuss this report, please contact me at (202) 927-0009, or a member of your staff may contact Mark S. Levitt, Manager, Financial Audit, at (202) 927-5076.

Attachment

**Department of the Treasury
Bureau of the Fiscal Service**

**Administrative Resource Center
Financial Management Services
Accounting, Human Resources, Travel, and Procurement Processing
General Computer and Monitoring Controls**

**Report on Administrative Resource Center's Description of Its Financial
Management Services and the Suitability of the Design and Operating
Effectiveness of Its Controls (SSAE 18 SOC 1® - Type 2 Report)
For the Period July 1, 2019 to June 30, 2020**

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
ADMINISTRATIVE RESOURCE CENTER
FINANCIAL MANAGEMENT SERVICES

**REPORT ON ADMINISTRATIVE RESOURCE CENTER'S DESCRIPTION OF ITS
FINANCIAL MANAGEMENT SERVICES AND THE SUITABILITY OF THE DESIGN AND
OPERATING EFFECTIVENESS OF ITS CONTROLS**

Table of Contents

**I.   INDEPENDENT SERVICE AUDITOR'S REPORT
PROVIDED BY KPMG LLP**

Independent Service Auditor's Report

Deputy Inspector General, Department of the Treasury
Deputy Commissioner, Fiscal Accounting and Shared Services

Scope

We have examined Bureau of the Fiscal Service's description of Administrative Resource Center's (ARC's) financial management services (accounting, human resources, travel, and procurement services, general computer, and monitoring controls) "ARC's system" used for processing customer agencies' transactions throughout the period July 1, 2019 to June 30, 2020 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "ARC's Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of ARC believes are likely to be relevant to customer agencies' internal control over financial reporting, and the description does not include those aspects of ARC's system that are not likely to be relevant to customer agencies' internal control over financial reporting.

The information included in Section V "Other Information Provided by the Administrative Resource Center" is presented by management of ARC to provide additional information and is not a part of ARC's description of its system made available to customer agencies during the period July 1, 2019 to June 30, 2020. Information about ARC's contingency planning has not been subjected to the procedures applied in the examination of the description of ARC's system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of ARC's system and, accordingly, we express no opinion upon it.

ARC uses subservice organizations identified in Section III to perform some of the services provided to customer agencies that are likely to be relevant to those customer agencies' internal control over financial reporting. The description includes only the control objectives and related controls of ARC and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by ARC can be achieved only if complementary subservice organization controls assumed in the design of ARC's controls are suitably designed and operating effectively, along with the related controls at ARC. Our examination did not extend to controls of the subservice organizations and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer agency controls assumed in the design of ARC's controls are suitably designed and operating effectively, along with related controls at ARC. Our examination did not extend to such complementary customer agency controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary customer agency controls.

Service organization's responsibilities

In Section II, ARC has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. ARC is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and assertion, providing the services covered by the

description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and applicable Government Auditing Standards issued by the Comptroller General of the United States. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2019 to June 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:
- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent limitations
The description is prepared to meet the common needs of a broad range of customer agencies and their auditors who audit and report on customer agencies' financial statements and may not, therefore, include every aspect of ARC's system that each individual customer agency may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives stated in the description is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion
In our opinion, in all material respects, based on the criteria described in ARC's assertion:
    a. the description fairly presents ARC's system that was designed and implemented throughout the period July 1, 2019 to June 30, 2020;
    b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively

throughout the period July 1, 2019 to June 30, 2020, and subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2019 to June 30, 2020; and

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2019 to June 30, 2020 if complementary subservice organization and customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2019 to June 30, 2020.

Restricted use

The purpose of this report is solely to provide information for customer agencies of ARC's system during some or all of the period July 1, 2019 to June 30, 2020, and their auditors who audit and report on such customer agencies' financial statements or internal control over financial reporting, to support evaluations of the effect of ARC's controls on customer agencies' financial statements. Accordingly, this report is not suitable for any other purpose.

KPMG LLP

September 14, 2020
McLean, Virginia

II.   MANAGEMENT'S ASSERTION

September 14, 2020

Administrative Resource Center's Assertion

We have prepared the Bureau of the Fiscal Service's Administrative Resource Center's (ARC's) description of its financial management services (accounting, human resources, travel, and procurement services, general computer, and monitoring controls) ("ARC's system" or "the system") used for processing customer agencies' transactions during some or all of the period July 1, 2019 to June 30, 2020 and the customer agencies' auditors, who audit and report on such customer agencies' financial statements or internal control over financial reporting, and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organization(s) and customer agencies of the system themselves, when assessing the risks of material misstatement of customer agencies' financial statements.

ARC uses the subservice organization(s) identified in Section III to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting. The description includes only ARC's control objectives and related controls and excludes the control objectives and related controls of the subservice organization(s). The description also indicates that certain control objectives specified in the description can be achieved only if complementary subservice organization controls assumed in the design of our controls are suitably designed and operating effectively along with the related controls at ARC. The description does not extend to controls of the subservice organization(s).

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer agency controls assumed in the design of ARC's controls are suitably designed and operating effectively, along with related controls at ARC. The description does not extend to controls of the customer agencies.
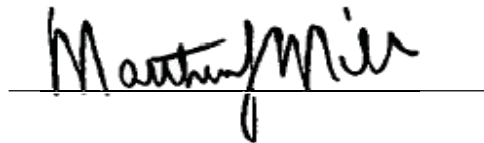
We confirm, to the best of our knowledge and belief, that:

a) The description fairly presents ARC's system performed by ARC on behalf of the customer agencies during some or all of the period July 1, 2019 to June 30, 2020 including ARC's processing of their transactions and the controls that are likely to be relevant to customer agencies' internal control over financial reporting. The criteria we used in making this assertion were that the description:

i.   presents how the system made available to customer agencies was designed and implemented to process relevant customer agency transactions, including, if applicable:

   (1)   the types of services provided, including, as appropriate, the classes of transactions processed;
   (2)   the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for customer agencies;
   (3)   the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and how other information is prepared for customer agencies;
   (4)   how the system capture and address significant events and conditions other than transactions;
   (5)   the process used to prepare reports and other information for customer agencies;
   (6)   services performed by a subservice organization(s), if any, including whether the carve-out method or the inclusive method has been used in relation to them;
   (7)   the specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary customer agencies' controls and complementary subservice organization(s)' controls assumed in the design of the service organization(s)' controls; and
   (8)   other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities and monitoring activities that are relevant to the financial management services provided.

ii.   includes relevant details of changes to ARC's system during the period covered by the description.
iii. does not omit or distort information relevant to ARC's system, while acknowledging that the description is prepared to meet the common needs of a broad range of customer agencies of the system and their auditors, and may not, therefore, include every aspect of the financial management services that each individual customer agency of the system and its auditor may consider important in its own particular environment.

b) The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period July 1, 2019 to June 30, 2020 to achieve those control objectives if subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2019 to June 30, 2020. The criteria we used in making this assertion were that:

   i.   the risks that threaten the achievement of the control objectives stated in the description have been identified by ARC management;
   ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Sincerely,

Matthew J. Miller
Deputy Commissioner,
Fiscal Accounting and Shared Services

III. DESCRIPTION OF CONTROLS PROVIDED BY THE ADMINISTRATIVE RESOURCE CENTER

OVERVIEW OF OPERATIONS

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

ARC divisions and branches, provide the following services for customer agencies:

Agency Payable and Receivable Division (APRD)	Services Provided
Accounts Payable Branch (APB)	Accounting Services
	Document Processing
	Reporting Services
Accounts Receivable Branch (ARB)	Accounting Services
	Document Processing
	Reporting Services
	Debt Collection Services
	Treasury Report on Receivables Reporting

Transaction Management Division (TMD)	Services Provided
Agency Intragovernmental Branch (AIB)	Provides Intragovernmental Business Services
Pensions, Grants and Loans Branch (PGL)	Accounting Services
	Provides Pension, Grants, and Loans Activity Services
Payroll, Vendors, and Cards Branch (PVC)	Accounting Services
	Supplier Table Update and Maintenance
	Record and Reconcile Payroll
	1099 Reporting
	Purchase Card Processing

Funds Management Division (FMD)	Services Provided
Funds Management Branch (FMB)	Document Processing
	Reporting Services
	Investment Activities
Agency Cash Branch (ACB)	Provides Cash Related Services
	Disbursements to Non-federal Entities
	Check Scanning Services
	Fund Balance with Treasury Reconciliation
	Accounting Services
Budget Execution Branch (BEB)	Accounting Services
	Reporting Services
	Budget Services

Agency Reporting and Analysis Division (ARAD)	Services Provided
Reporting and Analysis Branch 1 (RAB1)	Accounting Services

Reporting and Analysis Branch 2 (RAB2)	Reporting, Analysis, and Audit Support Services
	Accounting Services
Reporting and Analysis Branch 3 (RAB3)	Reporting, Analysis, and Audit Support Services
	Accounting Services
	Reporting, Analysis, and Audit Support Services

Operations Support Division (OSD)	**Services Provided**
Service Desk Branch (SDB)	Financial Management System Support and Training
	Develop and Maintain Robotic Process Automation
User Support Branch (USB)	Financial Management System Support and Training
Operations Support Branch 1 (OSB1)	Operate and Maintain Financial Management Systems

Systems and Project Support Division (SPSD)	**Services Provided**
Business Liaison Branch (BLB)	Internal Project Support Services
Project Support Branch 1 (PSB1)	Application Development, Analysis, and Project Management Services
Development Support Branch (DSB)	Application Development, Analysis, and Project Management Services
Security and Compliance Branch (SCB)	Security and Compliance Related Services

Travel Services Division (TSD)	**Services Provided**
Relocation Services Branch (RSB)	Operate and Maintain moveLINQ
	Record and process relocations
	Tax Reporting
	Civilian & commissioned relocation services
Temporary Duty Services Branch (TDSB)	Operate and Maintain E-Gov Travel Services (ETS) systems: SAP Concur (ConcurGov)
	ETS Training Services
	Document Processing
	Transaction Processing

Human Resources Operation Division (HROD)	**Services Provided**
Payroll and Processing Branch (PPB)	Processes and monitors personnel payroll transactions
Workforce Relations Branch (WRB)	Processes and monitors personnel actions
Employee Benefits Branch (EBB)	Processes and monitors personnel benefit actions
Business Systems Branch (BSB)	HR Business System Support Services

Division of Procurement Services (DPS)	**Services Provided**
Treasury Acquisitions Branch (TAB)	Acquisition Services
Fiscal Service Acquisitions Branch (FSAB)	Acquisition Services
Non-Treasury Acquisitions Branch (NTAB)	Acquisition Services

Employment Services Division (ESD)	Services Provided
Classification and Enterprise Support Branch (CESB)	Position Classification Services
Staff Acquisition Branch (SAB)	Staff Acquisition Services

These services are provided by the divisions as shown in the ARC organizational chart below:
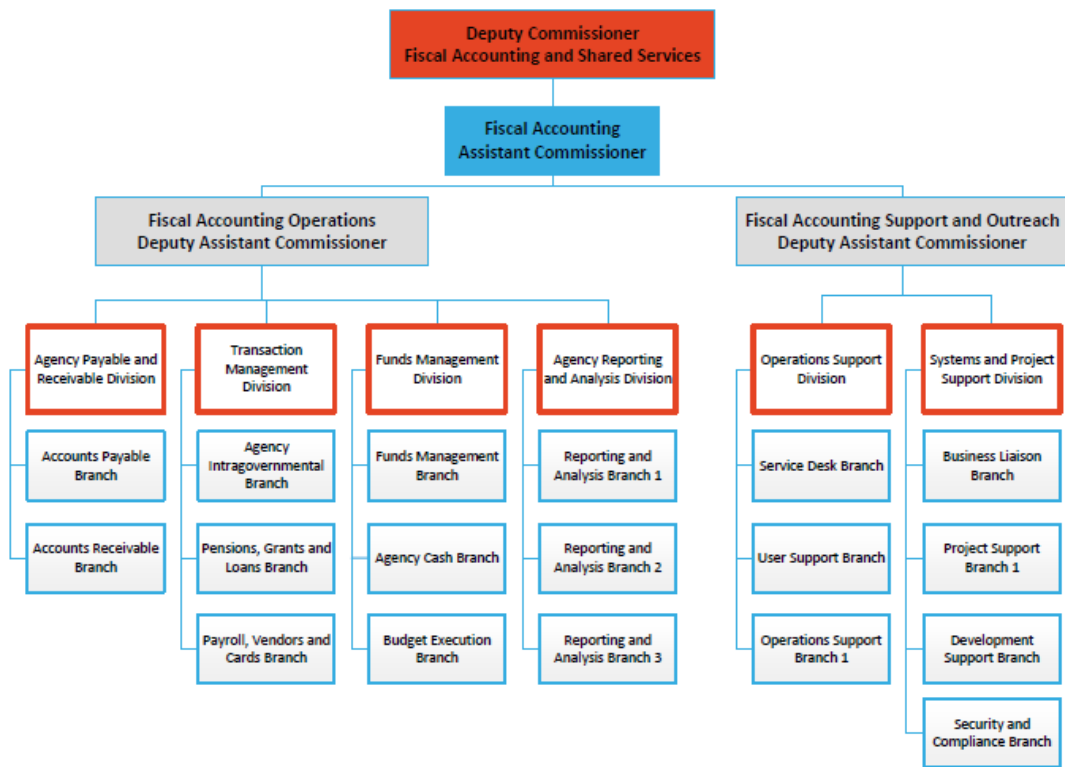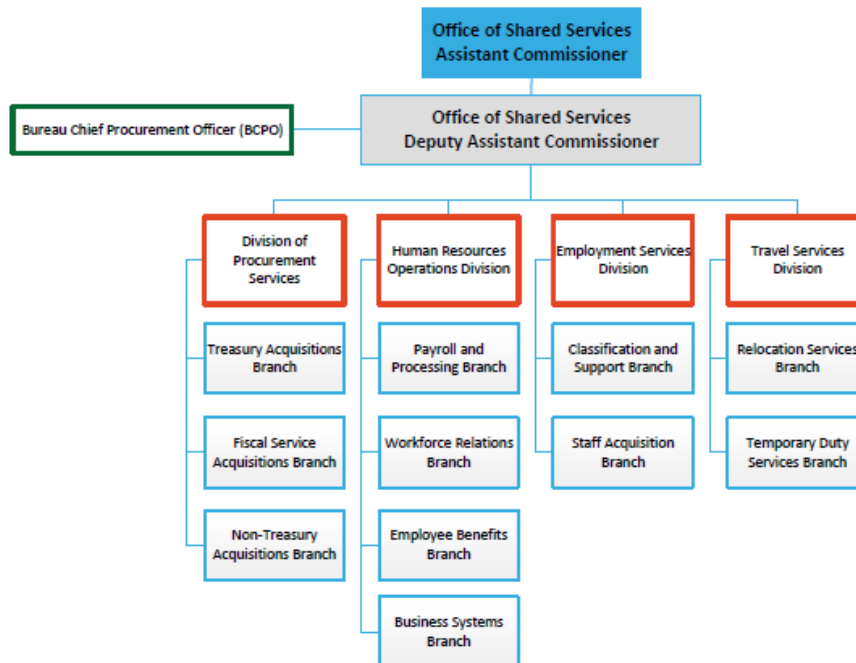
Accounting Services

Accounting Services consists of the following:

- Recording financial transactions in Oracle Federal Financials (Oracle), 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.
- Managing and verifying general ledger transactions in the core accounting system.

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, ARC meets with customer agencies to learn and understand the authorizing legislation and mission. This enables ARC to assist agencies 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 expenditure levels. The levels used are established based on the customer agency's authorizing legislation, apportionment level, or their request to control funds 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 requisition. In the event that the actual order amount is greater than the approved purchase request amount, a modification to the requisition 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 requisition, 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, Intragovernmental 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 CitiManager Card Management System. CitiManager allows customer agency cardholders and certifying officers to electronically reconcile, route, approve, and submit the purchase card statement to ARC for payment.

Generally, ARC customer agencies use three methods of receiving and monitoring the status of supplier invoices. The preferred method, due to efficiencies in processing and approvals from electronic workflow, requires that supplier invoices be submitted via the Invoice Processing Platform (IPP). The vendor submits an invoice through IPP and the invoice is routed to the invoice approver designated on the purchase order. In the second method, invoices are submitted directly to ARC to be manually processed (non-IPP), ARC has controls that ensure that all invoices are logged 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 third 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 determine whether 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 invoice approvers. If receiving reports are not submitted, the invoice approver 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 invoice approver 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 of manual invoices, 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 Payment Act and Electronic Funds Transfer (EFT) Rules or returns the invoice to the customer for clarification or additional information. Invoices processed via IPP are subject to a post payment audit. Non-IPP invoices less than $2,500 are subject to post payment audit.

ARC transmits EFT and check payment files to 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 approving official for approval. ARC records most IPAC payments in the accounting period the IPAC payment was accomplished.

Third-party payroll services provide to ARC, 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 Fiscal Service'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 utilizes Content Manager (not an in-scope application for the examination), a software application managed by Fiscal Service's Office of Information and Security Services (ISS) to store hardcopy and electronic data records. Content Manager stores the metadata of the hardcopy document, but the digital document is stored on the storage area network (SAN) to allow access to users of the document. ARC generates labels, which are printed and placed on boxes that are to be stored in Fiscal Service's warehouse. The information recorded on the label comes from data entered into Content Manager so the boxes can subsequently be requested by ARC personnel, as they are needed. Once the data is recorded in Content Manager, Fiscal Service warehouse personnel either pick up the box to be placed in storage or deliver the box to the bulk scanning operation which digitize the paper document, 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 to determine what action(s) is/are 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 required external reporting for customer agencies, including the following reports: Statement of Transactions (formerly FMS 224), Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS), Treasury Report or Receivables (TROR), Treasury Information Executive Repository (TIER), quarterly and year-end financial statements, and reports required by the Digital Accountability and Transparency Act (DATA Act). In addition, ARC has created a standard suite of management and external reports that are available to all customer agencies. ARC reconciles general ledger accounts on a monthly basis and ensures that proprietary and budgetary general ledger account relationships are maintained and accurate, and corrects any discrepancies.

Temporary Duty Travel Services

Travel Services consist of the following:

- Operating and maintaining the ETS systems (ConcurGov) 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 an interface to Oracle.

Travel documents (authorizations and vouchers) and miscellaneous employee reimbursements are entered by customer agencies into ConcurGov 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. ConcurGov contains system audits that prohibit documents that do not meet certain Federal Travel Regulations or do not contain the required accounting information from being approved and therefore will not interface to Oracle.

Relocation Services

Relocation Services consist of the following:

- Operating and maintaining moveLINQ, a government relocation expense management system in compliance with the FTR, Department of State Standardized Regulations (DSSR), and Joint Federal Travel Regulations (JFTR) to record and process Permanent Change of Station (PCS), Temporary Change of Station (TCS) and special entitlements such as Home Leave, Evacuation, Medical Evacuation, Rest and Recuperation and Education Travel 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.
- Tax Reporting.

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 e-mailed to the traveler and/or approving official for review and approval, as appropriate. ARC processes payments and the approved documents are interfaced and reconciled to Oracle daily for customer agencies.

Human Resources Services

The HROD provides payroll and personnel actions processing, using the Treasury Department's HRConnect (see page 28 for a description of HRConnect). Personnel actions are initiated by customer agencies in HRConnect, electronically routed internally for review and approval, and then electronically routed to HROD for review, coding and processing. For retirement and death actions, the customer agency supervisor will initiate the transaction and an EBB HR specialist will code the transaction for an EBB supervisor to approve. Once it is approved, the action is sent to PPB to execute the transaction. For removal and non-transfer Terminations (i.e., termination of probationary/trial employee), actions are submitted in HRConnect by a manager. A WRB Employee and Labor Relations (ELR) Specialist reviews, codes and approves the personnel action, and then forwards the personnel action to PPB. For all other separations a PPB HR Assistant determines the type of separation and codes the personnel action for review and approval by a PPB HR Specialist.

Manager submitted personnel actions are routed through an agency's internal approvals before routing to HROD. Depending on the type of personnel action, staff in ESD, PPB or WRB review the information, request any additional information needed, code and authorize the personnel action. After the personnel action is coded and approved, it is released from HRConnect by a PPB HR Assistant. The PPB HR Assistant verifies the action applied in the National Finance Center (NFC) and a different PPB HR Assistant verifies the information in NFC is correct.

Employee submitted personnel actions (such as name changes and changes in Veteran's Preference) bypass the agency review process and route directly to HROD. A PPB HR Assistant reviews the information, requests any additional information needed, and codes the personnel action. The PPB HR Assistant releases the action in HRConnect. The PPB HR Assistant verifies the action applied in NFC and a different PPB HR Assistant verifies the information in NFC is correct.

All FEGLI elections are initiated via an SF-2817, Life Insurance Election form. An EBB HR Assistant or Specialist verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. The EBB HR Assistant then manually inputs the form into HRConnect and verifies the change applied in NFC. A second EBB HR Assistant also verifies the document applied in NFC and that the information in NFC is correct. If a FEGLI election results from a qualifying life event, an EBB HR Assistant requests documentation to verify the employee's eligibility.

FEHB and Thrift Savings Plan (TSP) elections are employee-initiated via the appropriate form. An EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. The EBB HR Assistant then manually inputs the form into HRConnect and verifies the change applied in NFC. A second EBB HR Assistant also verifies the document applied in NFC and that the information in NFC is correct.

Employees receive payment for unused annual leave and compensatory time when certain criteria is met. A PPB HR Specialist enters and releases the payroll document in HRConnect. After NFC's Payroll Computation System (PAYE) runs, the PPB HR Specialist verifies that the employee was paid for the hours.

Employees submit requests for payroll document changes and/or deductions in writing to PPB. A PPB Contact Center Assistant reviews the request and contacts the employee if more information or additional verification is needed. The PPB Contact Center Assistant inputs and releases the request in HRConnect, and the information is sent to NFC via an interface between HRConnect and NFC's Payroll System. The PPB Contact Center Assistant verifies the action applied in NFC and a different PPB Contact Center Assistant verifies the information in NFC is correct. Employees can also submit requests for changes and/or deductions through NFC's Employee Personal Page (EPP), which allows for many self-service options.

HROD serves as the primary contact with NFC and coordinates to resolve any issues with personnel actions that are rejected by NFC.

Acquisition Services

Acquisition Services consist of the following:

- Awarding contracts and purchase orders in accordance with Federal Acquisition Regulations, Treasury Acquisition Regulations and, customer agencies Regulations as applicable.
- Contract Administration.
- Purchase Card Administration.

Requests for procurement actions are initiated 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 the Procurement Request Information System Management (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 a 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 modifications, 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 who 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 Deputy Commissioner of Fiscal Accounting and Shared Services. 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 and contractors working at ARC are responsible for processing and reporting accounting activity, providing system support and development services, procurement processing, 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 Fiscal Service personnel when they are hired. Additional background, credit, and security checks are performed every three to five years. The confidentiality of customer agency organization information is stressed during the new employee orientation program and is emphasized in the personnel manual issued to each employee. Fiscal Service provides a mandatory orientation program to all full time employees and encourages employees to attend other formal outside training. Training available to Fiscal Service employees with related work responsibilities includes, but is not limited to: Prompt Pay and Voucher Examination, Appropriation Law, Federal Acquisition Regulations, Federal Travel Regulations, Reconciling with and Reporting to Treasury, Federal Accounting Fundamentals, USSGL Practical Applications, Budgeting and Accounting – Making the Connection and Computer Security Awareness Training.

All Fiscal Service 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

Fiscal Service 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, travel services, and human resource 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

Fiscal Service 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 and timeliness is defined as seven days to process transactions. An example of a key monitoring control is that ARC's Agency Reporting and Analysis Division, Manager and/or Supervisors review reconciliations from Oracle sub ledgers to the related general ledger accounts. ARC prepares budgetary to proprietary account relationship reconciliations on a monthly basis. In

addition, ARC prepares and reconciles the GTAS submitted reports to the trial balance and statement of budgetary resources each time the GTAS file is submitted. ARC also uses the results of the annual Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting as a tool for identifying opportunities to strengthen controls.

ARC management also obtains and reviews relevant subservice organization system and organization controls (SOC 1) reports. For Fiscal Service systems that do not receive a SOC 1 report, system verification letters are prepared to document the information security controls that are implemented. The system verification letters are also obtained and reviewed by management. ARC will contact the subservice organization to obtain additional information for exceptions if applicable.

Description of Controls Provided
by the Administrative Resource Center

INFORMATION AND COMMUNICATION

Information Systems

Oracle Federal Financials (Oracle), Oracle Business Intelligence (OBI), Discoverer and OneStream

Oracle Managed Cloud Services operates Oracle R12 and Oracle 12.2 databases in a Linux operating system environment. 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 Internet Protocol (IP) address 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. Internet access is via a 128-bit or higher Transport Layer Security (TLS) 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, project accounting, fixed assets, and manufacturing. ARC also currently uses two report writer packages; one called OBI and one called Discoverer. Both packages provide users with the ability to create their own ad-hoc reports for query purposes. Both are intuitive ad-hoc query, reporting, analysis, and Web-publishing tools that empower business users at all levels of the organization to gain immediate access to the Oracle operational database. The information from Discoverer and OBI is obtained directly from the Oracle tables. Discoverer was decommissioned in the Shared Environment for non-System Administrator users on November 30, 2019 and System Administrators' access was removed March 6, 2020. All Shared Environment system users are now using OBI. The Mint Environment system users gained access to OBI on May 29, 2020. The Discoverer decommission of the Mint Environment is targeted for November 2020 but could be extended as late as March 2021. OneStream is a corporate performance management tool hosted by the cloud environment. OneStream is configured to consolidate financial data and automate workflows for financial reconciliations and financial reporting processes.

Procurement Request Information System Management

Oracle Managed Cloud Services, which operates PRISM version 7.3, uses the Windows Server 2012 operating system. PRISM uses an Oracle 11g database running in a Linux operating system environment. 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 Oracle Managed Cloud Services network. The application 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. Internet access is via a 128-bit or higher TLS encrypted connection. Transactions entered through PRISM interface real-time with Oracle.

Invoice Processing Platform

ARC uses the Fiscal Service's IPP electronic invoice processing solution (mandated for all Treasury Bureaus by Treasury). IPP is a web-based electronic invoicing and payment information system that is hosted by the Federal Reserve Bank of St. Louis. Purchase orders are interfaced from Oracle to IPP. Invoices are submitted in IPP by either the vendor or ARC personnel and are routed to the customer agency for approval. Upon approval, the invoice interfaces from IPP to Oracle and the invoice is scheduled for payment. Remittance information then interfaces to a Treasury Fiscal Service Financial Center that provide payment services for federal agency sites. IPP users consist of invoice approvers, viewers and administrators.

webTA

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

The ARC uses webTA (non-HUD) versions 5.0 and 4.2, which run on Red Hat Linux 6 or higher. webTA (non-HUD) uses Oracle 12c database, which runs on the ARC subnet and accesses data in the ARC demilitarized zone (DMZ) using Red Hat Linux 6 as its operating system. Additionally, ARC operates webTA (HUD) version 3.8.35 on a Windows 2012 operating system with Oracle 11g as the database version. The web server is running IIS 8.0 and the application server is running Tomcat 6.1. ISS 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 or higher TLS encrypted connection. External security is provided by ISS through firewall rules and router access control lists.

CitiBank CitiManager Card Management System

The CitiManager Card Management System (CitiManager) resides within Citi's secure single sign-on portal, CitiManager. CitiManager is a maintenance tool enabling Agency/Organization Program Coordinators (A/OPCs) to manage their card programs. Using CitiManager, A/OPCs can establish accounts, set parameters across their program and maintain the accounts. These parameters include but are not limited to authorization controls (credit limits, single purchase limits, and merchant category code blocking). Citi Transaction Management System resides within CitiManager and also allows A/OPCs and/or Finance Managers to load and delete general ledger/accounting allocation codes. CitiManager also provides a means for cardholders to review transactions and allocate them to the proper allocation codes prior to submitting the statement for payment.

ConcurGov

ARC uses SAP Concur's travel system ConcurGov (the system selected by the Treasury as its E-Gov Travel solution). SAP Concur developed and hosts ConcurGov. ConcurGov is a web-based, self-service travel system that incorporates traditional reservation and fulfillment support and a fully-automated booking process. ConcurGov uses system processes and audits to ensure compliance to the FTR and/or Agency policy. ConcurGov 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 real time interface process. ConcurGov 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 built on the Federal Enterprise Architecture (FEA) standard platform. moveLINQ is a 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, customer agency contacts, and relocating employees. The moveLINQ system is hosted by mLINQS, LLC within their contracted Microsoft Azure Government Cloud. The Bureau of Fiscal Service system is hosted separate from other mLINQS customers.

Robotic Process Automation

ARC uses Kofax[1] robotic process automation (RPA) to create and deploy software robots (or bots) to automate repetitive tasks and manual processes. Currently, RPA are used in Control Objectives 2 and 19. ARC's RPAs are developed and managed by SDB's Digital Workforce Support Team (DWST). Access to the Kofax RPA software and the bot code network drive directory is restricted to authorized users by use of Hewlett Packard Service Manager (HPSM) tickets before access is granted. HPSM tickets are also used to track access authorizations to Lightweight Directory Access Protocol (LDAP) groups that limit access to Kofax Management Console, where RPA runs are scheduled and monitored. The Kofax Management Console consists of two separate environments, the non-production, Acceptance (test) environment and the production environment. The non-production environment of Kofax Management Console is used to test new RPAs and RPA changes before they are eventually promoted to production. New RPAs are requested via an RPA intake form and changes to RPAs are requested via an RPA change request form. Once the request is reviewed and approved for development, a JIRA ticket is created. Before a new RPA or RPA change is promoted to production, the code is tested and undergoes a code review. Additionally, new RPAs undergo a security impact analysis. Once approved for production, a non-developer in DWST uploads the RPA code in the production Kofax RPA Management Console and then closes the JIRA ticket.

PRISM, IPP, ConcurGov, moveLINQ, and E-Payroll to Oracle Reporting (EOR) are feeder systems that interface with Oracle. Oracle Managed Cloud Services hosts Oracle, OBI, Discoverer, PRISM and EOR, Microsoft Azure Government hosts OneStream, SAP Concur hosts ConcurGov, the Federal Reserve Bank of St. Louis hosts IPP, mLINQS Hosting Service (MHS) hosts the moveLINQ Software as a Service (SaaS) within their contracted Microsoft Azure Government Cloud Platform as a Service (PaaS) environment, and ARC hosts webTA. ARC performs application administration for all feeder systems.

Communication

Fiscal Service has implemented various methods of communication to help 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 e-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 Fiscal Service's employee training and career development programs, internal training classes, and professional conferences.

---

[1] Kofax is software used by ARC that allows them control access to RPAs that are created to automate business processes. Kofax allows ARC to develop, test, and deploy the RPA.

*Description of Controls Provided
by the Administrative Resource Center*

Control Objectives and Related Controls

The Administrative Resource Center's control objectives and related controls are included in Section IV of this report, "Control Objectives, Related Controls, and Tests of Operating Effectiveness." Although the control objectives and related controls are included in Section IV, they are, nevertheless, an integral part of the ARC's description of controls.

COMPLEMENTARY CUSTOMER AGENCY CONTROLS

ARC's controls related to its system supporting the delivery of ARC's system cover only a portion of overall internal control for each customer agency of ARC. It is not feasible for the control objectives related to ARC's services to be achieved solely by ARC. Therefore, each customer agency's internal control over financial reporting should be evaluated in conjunction with ARC's controls, related tests, and results described in Section IV of this report, taking into account the related Complementary Customer Agency Controls (CCACs) as described below, where applicable. In order for customer agencies to rely on the controls reported on herein, each customer agency must evaluate its own internal control to determine whether the identified CCACs have been implemented and are operating effectively.

Customer agency auditors should determine whether customer agencies have established controls to provide reasonable assurance to:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.
- Send approved requests to record manual obligations to ARC in a timely manner.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Approve and return relocation travel authorizations to RSB for processing in moveLINQ in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to ARC.
- Compare actual expenditure results to budgeted amounts.
- Maintain and communicate to ARC, a list of individuals authorized to request obligations when it is not communicated in the authorizing agreement.
- Review the financial reports provided by ARC to ensure that disbursements transactions are complete and accurate.
- Approve invoices for payment and send approved invoices to ARC in a timely manner.
- Ensure that invoices received at the customer agency are reviewed to determine whether they properly reflect the invoice receipt date and provide correct received and acceptance dates for goods or services according to the Prompt Payment Act.
- Approve travel vouchers and accurately enter the vouchers into ConcurGov in the proper period.
- Maintain and communicate to ARC, a list of individuals authorized to approve invoices and travel vouchers when it is not communicated in the authorizing agreement.
- Properly allocate Citibank charges and obtain Approving Official certification prior to auto-close.
- Provide post payment approval for Citibank auto-closed invoices.
- Maintain and communicate to ARC, a list of individuals and applicable authority limits authorized to request non-referencing payments and expense corrections.
- Send approved and accurate documentation of unfilled customer orders, receivables, and 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 as applicable.

- Customer agency's Chief Financial Officer must certify that the TROR and Debt Collection Activities report submitted to the Treasury is accurate and consistent with agency accounting systems.
- Provide assistance, when requested, to determine a check's purpose and validity prior to deposit.
- Review and confirm leave accrual schedule annually.
- Review the financial reports provided by ARC to ensure that monthly payroll and leave 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 and confirm customer specific payroll disbursement procedures on an annual basis.
- Review and approve, prior to submission, the financial reports prepared by ARC to ensure that reports prepared for external use are complete, accurate, and submitted in a timely manner.
- The Homeland Security bureau variance is also approved by the Homeland Security's CFO or designee.
- 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 provided by ARC to ensure that accruals are complete and accurate.
- Review and approve the annual submission of the Treasury Report on Receivables (TROR) and Debt Collection Activities.
- Provide certification of GTAS to ARC prior to system certification.
- Approve and return relocation travel documents to RSB for processing in moveLINQ 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.
- 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.
- Send valid and approved requests to record manual journal entries to ARC in a timely manner if they are initiated by the customer agency.
- Maintain and communicate to ARC a list of individuals authorized to submit manual journal entries that are initiated by the customer agency.
- Provide ARC current investment guidance that dictates the type and amount of securities to be purchased and the amount of residual cash if any to be retained.
- Provide applicable legislation, and any subsequent legislation revisions, that authorizes the Program Agency to invest with the investment account set-up.
- Work with ARC to confirm significant investment and fund balance activity by e-mail when long-term investments are scheduled to be settled or settled in accordance with current investment guidance.
- Communicate to ARC any known delays to disbursement activity that may impact investments.
- Communicate to ARC any larger than normal disbursement activity that may impact investments
- Review active supplier reports provided by ARC and request to remove suppliers no longer needed in a timely manner.

- Ensure all personnel actions are submitted in HRConnect timely.
- Notify ARC timely regarding exiting employees.
- Review and approve listing of users with current Oracle, PRISM, webTA, ConcurGov, IPP, OneStream, and HRConnect access to ensure appropriateness and provide changes to ARC in a timely manner.
- Notify ARC timely of any changes to HRConnect authorized approvers.

Specific CCACs are provided in Control Objectives 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17, and 19 in the Control Objectives, Related Controls, and Tests of Operating Effectiveness section of this report.

SUBSERVICE ORGANIZATIONS

In order to provide financial management services, ARC relies on systems and services provided by other organizations external to ARC (subservice organizations). The achievement of control objectives depends on whether controls at the subservice organizations anticipated in the design of ARC's controls were implemented and operating effectively. These subservice organizations were not subject to examination by KPMG LLP.

Bureau of the Fiscal Service

Bureau of the Fiscal Service hosts and administers the business applications described below that provide government wide transactions and produce reports and outputs that are relevant to customer agency's internal control over financial reporting.

Central Accounting and Reporting System (CARS) – Treasury's Fiscal Service provides reports to inform agencies of their Fund Balance With Treasury and to assist agencies in reconciling their general ledger balances to Fiscal Service balances. ARC uses account summary and transaction reports to perform reconciliations.

Secure Payment System – ARC uses SPS to process payments for invoices.

Collections Information Repository (CIR), TDO Payments, and IPAC – ARC uses these applications to identify receivables and any cash differences (collections and disbursements).

Treasury Report on Receivables and Debt Collection Activities, Cross Servicing Next Generation System (CSNG) – ARC uses TROR as a primary means for providing data on the status of non-tax debt portfolio. ARC uses the CSNG system to transfer debts for collection to Debt Management Services (DMS).

Over The Counter Channel Application (OTCnet) – Treasury's OTCnet enables Federal Program Agency (FPA) users to report over-the-counter receipts in a secure, web-based system. In addition to the summary deposit information currently required on the paper SF 215, OTCnet collects sub-total accounting information that can feed the FPA's administrative accounting systems as well as the Treasury's central accounting system.

Governmentwide Treasury Account Symbol Adjusted Trial Balance System – GTAS is a web-based system implemented for use in Governmentwide reporting as the primary means of reporting agency trial balance data. This single data collection system is designed to pave the way for more consistent and complete financial data and will allow for analytical reporting.

ARC has customized programs in Oracle that extract the accounting and budgetary data in the required GTAS bulk file format. GTAS has a standardized chart of accounts that is compliant with USSGL guidance issued by the Treasury. Various edit checks are incorporated in the GTAS validation checks. After submitting the adjusted trial balances into GTAS, ARC accountants review the edit reports and resolve any invalid attributes or out-of-balance conditions.

InvestOne – The InvestOne accounting system is a vendor supplied transaction-based accounting system that is a subsystem of the Debt Information Management System (DIMS) used to record and report investment fund activity; it is interfaced with Oracle.

FedInvest – Also a subsystem of DIMS, FedInvest is a vendor-developed, web-based extension to the InvestOne accounting system that provides access to the federal investments information through the Internet.

Invoice Processing Platform – ARC uses IPP to electronically route invoices for approval and payment.

Department of the Treasury

Department of the Treasury hosts and administers the business applications described below that provides reports and outputs that are relevant to customer agency's internal control over financial reporting.

TIER – For ARC's Treasury and the Department of Homeland Security customer agencies, 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 and the Department of Homeland Security bureaus and other reporting entities within the Treasury and the Department of Homeland Security 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 Treasury. After submitting the adjusted trial balances into TIER

Financial Analysis and Reporting System (FARS) – Treasury's FARS produces financial statements using data bureaus have submitted to TIER.

HRConnect – ARC uses HRConnect, the human resources management system owned and administered by the Department of the Treasury, for processing payroll and personnel actions. HRConnect allows HR staff and managers to electronically initiate, approve and track personnel actions and payroll documents. HRConnect is a front-end system for sending personnel action data to the USDA National Finance Center's Payroll/Personnel System.

SAP Concur

ConcurGov – SAP Concur developed and hosts the ConcurGov system, which is an E-Gov travel system. SAP Concur is the vendor for E-Gov travel selected by the Treasury. SAP Concur maintains the data in their Business Data Warehouse for six years.

Oracle Corporation

Oracle Managed Cloud Services – ARC's Oracle, OBI, Discoverer, PRISM, and EOR applications are hosted at Oracle Managed Cloud Services. Fiscal Service retains application administration responsibilities and Oracle Managed Cloud Services provides the computer processing infrastructure and support. Oracle Managed Cloud Services staff serve as the database and system administrators and provides backup and recovery services for Oracle and PRISM.

OneStream

OneStream XF – ARC uses OneStream to consolidate financial data and automate workflows for financial reconciliations and financial reporting.

United States Department of Agriculture (USDA)

National Finance Center (NFC) – ARC uses NFC to process payroll and personnel actions. Personnel data entered in HRConnect is sent to NFC's Payroll/Personnel System (PPS). PPS includes the processing of personnel actions, awards, allotments, performance appraisals, health and life insurance, thrift savings plan (TSP), tax documents, severance pay and leave records. PPS maintains employee data beginning with the hiring of the employee through separation.

PPS also processes payroll and transmits payroll files to ARC after the end of a pay period and the files are used to recorded payroll disbursements.

Various payroll service providers (For Non-Treasury customer agencies)

Various systems – Third-party payroll service providers transmit payroll files to ARC after the end of a pay period. ARC uses these files for recording payroll disbursements.

mLINQS, LLC

moveLINQ – MHS hosts the moveLINQ SaaS within their contracted Microsoft Azure Government Cloud PaaS environment. The moveLINQ system is developed by mLINQS, LLC and updates are applied by MHS within the MHS hosted environment. MHS provides system administration and ARC provides application administration. ARC is responsible for record retention, data processing, and the interface processing of the system output which is provided by MHS to the Oracle system.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

ARC controls related to its system supporting its delivery of financial management services cover only a portion of overall internal control for each customer agency of ARC. It is not feasible for the control objectives related to services provided by ARC to be achieved solely by ARC. Therefore, each customer agency's internal control over financial reporting must be evaluated in conjunction with ARC's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at subservice organizations. Complementary subservice organization controls and ARC's control objectives that depend upon them are described for each of ARC's subservice organizations below.

Fiscal Service

Control Objective 2 – Disbursements, Control Objective 3 – Unfilled Customer Orders, Receivables, and Cash Receipts, Control Objective 4 – Deposits, Control Objective 5 – Payroll and Leave Accruals, Control Objective 7 – USSGL, Control Objective 9 – Governmentwide Reporting Control Objective 10 – Expenditures, Control Objective 11 – Budget, and Control Objective 13 – Federal Investments

- Responsible for maintaining privileged user access and logical security over the servers, and hardware devices, to CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.
- Responsible for granting, reviewing, and removing user access to CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.
- Responsible for performing patching to the operating system and database and application changes to CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.
- Responsible for maintaining physical access and environment controls for CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.
- Responsible for performing data back-ups for CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.
- Responsible for maintaining business process controls that control input, processing, and output of information for CARS, SPS, CIR, TDO Payments, TROR, CSNG, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA.

Treasury

Control Objective 3 – Unfilled Customer Orders, Receivables, and Cash Receipts, Control Objective 5 – Payroll and Leave Accruals, Control Objective 6 – Payroll Disbursements, Control Objective 7 – USSGL, Control Objective 9 – Governmentwide Reporting, Control Objective 17 – Personnel Actions, and Control Objective 18 – Payroll Documents

- Responsible for maintaining privileged user access and logical security over the servers, and hardware devices related to TIER, FARS, and HR Connect.
- Responsible for granting, reviewing, and removing user access to TIER, FARS, and HR Connect.
- Responsible for performing patching to the operating system and database and application changes to TIER, FARS, and HR Connect.

- Responsible for maintaining physical access and environment controls for TIER, FARS, and HR Connect.
- Responsible for performing data back-ups for TIER, FARS, and HR Connect.

SAP Concur

Control Objective 1 – Obligations and Control Objective 2- Disbursements

- Responsible for providing reasonable assurance that ConcurGov transaction processing is accurate and complete.
- Responsible for maintaining privileged user access and logical security over the servers, and hardware devices related to ConcurGov.
- Responsible for providing reasonable assurance that administrative access to data, programs, and application functions are restricted to authorized users in ConcurGov.
- Responsible for providing reasonable assurance that deployment and enhancements of ConcurGov are tested, approved, implemented, and documented within a change control process.
- Responsible for performing patching to the operating system and database and application changes to ConcurGov.
- Responsible for maintaining physical access and environment controls for ConcurGov.
- Responsible for performing data back-ups for ConcurGov.

Oracle Corporation

All Control objectives

- Responsible for providing IT security oversight and security controls within the Oracle IT control environment.
- Responsible for assuring that physical access to computer equipment, storage media and program documentation is restricted to authorized and appropriate personnel to protect systems and data from unauthorized modification in Oracle.
- Responsible for assuring that logical access to Oracle production systems and data is restricted to authorized and appropriate individuals to protect systems and data from unauthorized access and support segregation of duties.
- Responsible for assuring that the Oracle network infrastructure is properly secured, managed, and maintained to enable applications to operate effectively, to protect data from unauthorized changes, and to provide for its availability for processing.
- Responsible for assuring that Oracle code development, configuration changes, and patches for the operating system and database are appropriately initiated and authorized and function in accordance with system specifications to result in valid, complete, accurate, and timely processing of data.
- Responsible for assuring that Oracle application and system processing are executed in a complete, accurate, and timely manner, and incidents are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.
- Responsible for assuring that system capacity, availability, and operations are appropriately provided and monitored to prevent potential loss of data or inability to access data as required in Oracle.
- Responsible for assuring that Oracle data, applications, and operating systems are backed up and procedures are employed to maintain the integrity of the tape media to permit timely restoration.

Federal Reserve Bank St. Louis

Control Objective 2 – Disbursements

- Responsible for providing reasonable assurance that IPP application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, and resolved in a timely manner.
- Responsible for providing reasonable assurance that physical security tools and techniques are configured, administered, and monitored to restrict access to the IPP application.

OneStream XF

Control Objective 7 – USSGL, Control Objective 8 – Accruals, and Control Objective 9 – Governmentwide Reporting

- Responsible for the implementation of logical access security software, infrastructure and architectures.
- Responsible for authorizing access for new internal and external users and to remove credentials when access is no longer authorized.
- Responsible for the identification and authentication of internal and external users when accessing system components.
- Responsible for access to the data, software, functions and other IT resources as authorized, modified or removed based on roles, responsibilities or by system design.
- Responsible for logical access security measures to protect against security or confidentiality threats.
- Responsible for the transmission, movement and removal of information that is restricted to authorized internal and external users.
- Responsible for security, confidentiality incidents, including logical and physical security breaches, failures, and the identification of vulnerabilities, as well as reporting to appropriate personnel.

USDA

Control Objective 5 – Payroll and Leave Accruals and Control Objective 6 – Payroll Disbursements
Control Objective 17 – Personnel Actions, and Control Objective 18 – Payroll Documents

- Responsible for assuring that access to programs, data, and computer resources is restricted to authorized users, processes, and devices.
- Responsible for assuring changes to application programs are authorized, tested, documented, approved, and implemented to support complete, accurate, and timely processing and reporting of transactions.
- Responsible for performing patching to the operating system and database and application changes to their payroll applications.
- Responsible for maintaining physical access and environment controls for their payroll applications.
- Responsible for performing data back-ups for their payroll applications.

Various Payroll Service Providers (For Non-Treasury customer agencies)

Control Objective 5 – Payroll and Leave Accruals and Control Objective 6 – Payroll Disbursements

- Responsible for processing and reconciling customer agencies' payroll information.
- Responsible for maintaining privileged user access and logical security over the servers, and hardware devices related to their payroll applications.
- Responsible for granting, reviewing, and removing user access to their payroll applications.
- Responsible for performing patching to the operating system and database and application changes to their payroll applications.
- Responsible for maintaining physical access and environment controls for their payroll applications.
- Responsible for performing data back-ups for their payroll applications.

mLINQS, LLC

Control Objective 1 – Obligations, Control Objective 2 – Disbursements, Control Objective 10 – Expenditures

- Responsible for maintaining privileged user access and logical security.
- Responsible for granting, reviewing, and removing user access.
- Responsible for performing patching to the operating system and database and application changes.
- Responsible for maintaining physical access and environment controls.
- Responsible for performing data back-ups.

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

Information Provided by KPMG LLP

This report, when combined with an understanding of the controls at customer agencies, is intended to assist auditors in planning the audit of customer agencies' financial statements or customer agencies' internal control over financial reporting and in assessing control risk for assertions in customer agencies' financial statements that may be affected by controls at ARC.

Our examination was limited to the control objectives and related controls specific by ARC in Section III and IV of the report, and did not extend to controls in effect at customer agencies.

It is the responsibility of each customer agency and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the customer agency in order to assess total internal control. If internal control is not effective at customer agencies, ARC's controls may not compensate for such weaknesses.

ARC's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by ARC. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by ARC, we considered aspects of ARC's control environment, risk assessment process, monitoring activities, and information and communications.

The following clarifies certain terms used in this section to describe the nature of the tests performed:

- Inquiry – Inquiring of management and others within the service organization who, in the service auditor's judgment, may have relevant information.

- Observation – Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing.

- Inspection – Involves examining records or documents, whether in paper form or electronic form.

- Recalculation – Consists of checking the mathematical accuracy of documents or records. Recalculation may be performed manually or electronically.

- Reperformance – Involves the independent execution of procedures or controls that were originally performed as part of the entity's internal control.

In addition, as required by paragraph .35 of Attestation Standards - Clarification and Recodification (AT-C) section 205, *Examination Engagements* (American Institute of Certified Public Accountants (AICPA), Professional Standards), and paragraph .30 of AT-C section 320, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Procedures used included:

- Inspecting the source of the information;
- Inspecting the query, script, parameters used to generate the information;
- Observing the generation of information; and
- Inspecting management's reconciliation of reports.

ACCOUNTING PROCESSING CONTROLS

Control Objective 1 – Obligations

Controls provide reasonable assurance that obligations are authorized, complete, accurate, documented, and processed timely in accordance with 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 PRISM and Oracle 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.

In the event the status change requires a document to be released to the Oracle database, an analyst will be required to notate why the action was performed. Every business day an analyst is responsible for executing and reviewing a report to identify all PRISM documents that were released the previous business day. Each document that is returned is researched to determine if any variances exist between PRISM and Oracle. The action taken when completing this task is reviewed by the supervisor or a delegated authority.

The analyst reviews an additional report designed to identify procurement and accounting system obligation mismatches to assist in their troubleshooting efforts. Each business day, the report will be executed to identify all documents meeting the determined criterion, and each document identified on the report is independently reviewed by an analyst who was not involved in the initial transaction. The actions taken to complete task is reviewed by the supervisor or a delegated authority.

Manually Recorded Obligations – Customer Agency Approval

For obligations not processed through the interface, customer agencies and/or Procurement sends ARC a signed copy of the agreement or Miscellaneous Obligation Form to obligate the funds. Upon receipt from the customer agency and/or Procurement, the ARC technician responsible for processing the customer agency's accounting transactions reviews the documentation to ensure submissions match authorization authority and adequate accounting information has been received, and manually enters the obligation into Oracle. Obligations posted in Oracle are available for both ARC and customer agency review through ad hoc OBI and Discoverer (for Mint) reports.

Temporary Duty Travel System Interface

Fiscal Service travelers and shared service travel customers enter travel authorizations into ConcurGov 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 via real time interface processing to Oracle which records an obligation in the general ledger. Daily interface files are received from ConcurGov which is used for processing, report generation, and identification of exceptions. The files are 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 ConcurGov and Oracle. Rejected transactions are manually entered into the system. Approved authorizations in ConcurGov are reconciled daily by an accounting technician with an Oracle generated report to ensure that all ConcurGov authorizations have been interfaced and processed in Oracle. ConcurGov prevents a user from both entering and approving travel authorizations unless they have authorized access.

Relocation Travel System Interface

The RSB personnel enter PCS travel authorizations into moveLINQ and electronically routes them to Approving Officials for review and approval. Approving Officials electronically sign the authorization with their assigned status. When the signed document is received by RSB, Relocation Coordinators stamp the document in moveLINQ with a status of "approved". All "approved" documents are interfaced daily via batch process to Oracle which records an obligation in the general ledger. Approved 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.

Budget Execution System Controls

Customer agencies can institute 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 various accounting strings at the allocation levels.

Budget execution system controls can be set to prevent expenditures beyond the budget plan amount or allow expenditures over the budget plan amount at any level of the budget plan. Expenditures beyond the apportionment and appropriation levels (legal levels) is prohibited. System controls are designed to prevent the user from apportioning more than was appropriated and allocating more than was apportioned. Decisions on control settings that permit or prevent expenditures beyond the budget plan levels are determined by the customer agency. System controls are applied at the fund level after passage of appropriation legislation and a high-level

budget is loaded at the appropriation level. Upon receipt and input of a detailed financial plan, controls are established at the allocation level when desired by the customer agency.

Budget execution settings are determined by the customer agency and set-up in Oracle by the USB ARC staff. System settings are reviewed with the customer agency on an annual basis, input by USB staff, and then reviewed by a supervisor for completeness and accuracy.

<u>Document Numbering</u>

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.

<u>Complementary Customer Agency Controls</u>

Customer agencies should establish controls to:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.
- Send approved requests to record manual obligations to ARC in a timely manner.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Review and approve listings of users with current Oracle, PRISM, webTA, ConcurGov, IPP, and OneStream access to ensure appropriateness.
- Approve and return relocation travel authorizations to RSB for processing in moveLINQ in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to ARC.
- Compare actual expenditure results to budgeted amounts.
- Maintain and communicate to ARC a list of individuals authorized to request obligations when it is not communicated in the authorizing agreement.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of obligations and determined the procedures were formally documented for the processing of obligations.
2. Observed a demonstration of the PRISM system and noted the system validated data for obligations based on information provided by the customer agency and determined proper authorization was granted prior to the interface with the accounting system.
3. Observed the PRISM Support Team Staff monitor the "Pending Financial Approval" and "Disapproved during Pending Financial Approval" reports and noted the reports were monitored, there were no backlogs, and issues noted were investigated and resolved.
4. For a selection of days, inspected evidence that the report used to identify all PRISM documents released the previous business day were reviewed and determined the reports were reviewed and actions taken on any variances noted were reviewed by a supervisor.
5. For a selection of days, inspected evidence that the report used to identify accounting system obligation mismatches was reviewed and determined that actions were taken for documents identified on the report and it was reviewed by the supervisor.

6. For a selection of manually entered obligations for a selection of customer agencies, inspected evidence of customer agency approval and determined manually entered obligations were approved prior to being entered into Oracle by ARC Staff.
7. Observed the daily ConcurGov interface and noted approved travel authorizations interfaced into Oracle, and Oracle recorded the obligation to the general ledger.
8. For a selection of days for a selection of customer agencies, inspected the ConcurGov to Oracle interface reconciliations and determined a daily reconciliation was performed, any data interface errors or exceptions identified were corrected, any rejected transactions were manually entered into the system, and all approved travel authorizations were interfaced and processed by Oracle.
9. Observed a ConcurGov user who is not authorized to approve a travel authorization attempt to approve a travel authorization within the system and noted the workflow functionality within ConcurGov required travel authorizations to be routed to an authorized approving official, thereby preventing the unapproved travel authorization from being interfaced to Oracle.
10. Observed the daily moveLINQ interface and noted approved relocation authorizations were interfaced into the Oracle system and recorded as an obligation.
11. For a selection of days, inspected reconciliations of travel authorizations from moveLINQ to Oracle and determined the interface activity was reconciled daily by an accounting technician and all approved travel authorizations in moveLINQ completely and accurately interfaced with Oracle.
12. For a selection of customer agencies, inspected their budget execution set-up in Oracle and determined the settings were set-up in Oracle by ARC and were annually reviewed by the customer agency.
13. Observed an ARC user attempt to enter a transaction identification number that already existed and noted Oracle issued an error message alerting the user of the duplication and automatically rejected the entry of a duplicate transaction number.

No exceptions noted.

Control Objective 2 – Disbursements

Controls provide reasonable assurance that the disbursements are 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.

IPP Customer Agency Invoice Approvals

ARC only processes disbursements for invoices with customer agency approval. Vendors can submit invoices through the IPP or send invoices to the customer agency or ARC, depending on the instructions in the purchase order.

In order to submit an invoice directly into IPP, the vendor must have an IPP collector account. ARC transmits Oracle supplier table information to the Federal Reserve Bank of St. Louis (FRB) in order to create the collector account or the vendor can contact FRB St. Louis and supply the necessary information themselves. The vendor must include contact information for the government agency they are doing business with, if they initiate enrollment. When an agency uploads their supplier info to IPP they must also match each record to the corresponding collector account. The purchase orders loaded for each supplier are also tied to the collector account. This limits the purchase orders the vendor can view and invoice against. The current IPP configuration requires all invoices reference an approved purchase order.

IPP system validations prevent invoices from being submitted for amounts that exceed the purchase order amount authorized by the Contracting Officer. In addition, IPP requires invoice service periods to fall within the period of performance on the purchase order.

If the vendor submits the invoice through IPP it is automatically routed to the invoice approver designated on the purchase order. This designation is made by the Contracting Officer on the purchase order, which is interfaced to Oracle and then to IPP. Purchase orders manually entered into Oracle and not processed in PRISM include the invoice approver in Oracle per the supporting documentation. An agency invoice approver can only approve an invoice in IPP if it is routed to them, which requires they have an active IPP user account. In order to gain access to IPP, the approver must complete and submit a user access form and a certificate of completion for the required Invoice Approver Training. Customer agency users do not have the ability to approve an invoice unless it is routed to them in IPP. Nor do they have the ability to route invoices to other users for approval. Only IPP invoices that were approved by the invoice approver or Contracting Officer for the purchase order are interfaced to Oracle for payment. Contracting officers may request invoices be routed to them in IPP by ARC IPP administrators in an approver's absence.

The banking information used for the disbursement is maintained in Oracle rather than IPP. A Data Universal Number System (DUNS) number is assigned to the purchase order at time of award. The banking information for the assigned DUNS number is interfaced from System for Award Management (SAM) to Oracle.

A daily reconciliation is performed in order to ensure that all approved IPP invoices are successfully interfaced to Oracle and to ensure that new purchase orders or modifications to purchase orders for IPP vendors are successfully interfaced to IPP.

Non-IPP Customer Agency Invoice Approvals

Non-IPP invoices are either sent to ARC or to the customer agency. Invoices that are directly sent to ARC, the customer agency approval is given 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. If invoices are sent to the customer agency, the customer agency reviews and approves the invoice, and then forwards the invoice and evidence of customer agency approval to ARC.

System controls set at the user identification and/or vendor level ensure that payment of non-IPP invoices greater than or equal to $2,500, which are processed by an accounting technician, must be reviewed and approved by a lead accounting technician or an accountant prior to disbursement.

IPAC Customer Agency Approvals

IPACs that 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.

Citibank Customer Agency Approvals

ARC processes disbursements for Citibank Invoices that have been authorized by an Approving Official/Designee. When the approval window closes in the Citibank Application, ARC receives an auto-close file containing charges yet to be approved. In those instances and after payment, ARC sends a one-time e-mail communication to the customer agency informing them of the auto-closed transactions and requests payment approval.

Temporary Duty Travel Vouchers Approvals

Fiscal Service travelers and shared service travel customers enter travel vouchers into ConcurGov, and electronically routes them to Approving Officials for review and approval. Approving Officials electronically sign the voucher with a status of "approved". All "approved" vouchers are interfaced via real time interface processing to Oracle which records a disbursement in the general ledger. Daily interface files are received from ConcurGov, which is used for processing, report generation, and identification of exceptions. The files are 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 ConcurGov and Oracle. Rejected transactions are manually entered into the system. Approved vouchers in ConcurGov are reconciled daily by an accounting technician with an Oracle generated report to ensure that all ConcurGov vouchers have been interfaced and processed in Oracle. ConcurGov prevents a user from both entering and approving travel vouchers.

Relocation Services Travel Vouchers Approvals

RSB personnel enter and audit each PCS travel voucher in moveLINQ and electronically route them to Employee/Approving Officials for review and approval. Employees and Approving Officials electronically sign the voucher with their assigned status. When the signed document is received by RSB, Relocation Technicians stamp the document in moveLINQ with a status of "approved". All "approved" documents are interfaced daily via batch processing to Oracle which

Control Objectives, Related Controls, and
Tests of Operating Effectiveness

records a disbursement in the general ledger. Approved 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.

IPP Review

All invoices processed by IPP are subject to post payment random sampling. ARC reviews 10% of all invoices processed by IPP for each customer on a monthly basis. Results are provided to each customer agency. In addition to providing customer agency management feedback of invoice approver performance, the random sampling verifies that the invoice approver or contracting officer on the referenced purchase order approved the invoice in IPP. Sampling also verifies that the invoice submitted by the vendor did not exceed the amount authorized by the contracting officer on the purchase order and that the services provided were within the period of performance authorized by the contract. The post payment monthly random sampling provides continuous monitoring to ensure system controls are operating as intended.

Non-IPP Review

Non-IPP invoices less than $2,500 are subject to a monthly random sample post payment audit. System user access profiles restrict accounting technicians' ability to process documents that require review and approval by a lead technician or accountant and ensure proper segregation of duties is maintained. A 100% post payment audit review is conducted weekly on all invoices resulting in a payment of greater than $2,500 that was both processed and approved by the same individual.

Random Sampling of Temporary Duty Travel Vouchers Review

TDSB staff completes post-payment audit reviews of TDY travel vouchers to verify the accuracy of the interfaced data and compliance with FTR. Agencies falling into FTR or the FTR/ARC category type are subject to a 41-point audit worksheet comprised of 36 critical error checks and 5-noncritical informational checks. The ARC Travel Sampling Plan is broken down into two separate components: Quality Sample and Statistical Sample. The Quality Sample is a weekly sample and includes two parts: 1) A 100% audit of vouchers over $2,500, trips with advances, trips showing duplicate M&IE, and more. 2) A 10% targeted sample of other high-risk vouchers. The Statistical Sample is a monthly random sample which excludes vouchers pulled in the Quality Sample. Errors are sent via e-mail to the traveler and/or document preparer and/or approving official to review and/or take action. Billing documents are created for amounts owed by a traveler, resulting from an overpayment in which the customer agency has declared the overpayment a debt of the United States Government. The traveler uses Pay.gov eBilling to pay the overpayment, or seeks waiver per agency policy.

Payment Date Calculations

Based on the customer agency's contracts with its suppliers, ARC staff enters the later of the invoice receipt date, or the earlier of the formal or constructive acceptance dates in Oracle based on the supporting documentation from the customer agency, or the invoice interfaces to Oracle based on dates provided by the customer agency's approver in IPP. IPP controls prevent the vendor from back dating the IPP invoice receipt date, which is the date that the invoice was successfully created in IPP. The invoice date is entered into Oracle by ARC staff or interfaces from the IPP invoice. On a daily basis, Oracle selects invoices that are due for payment and creates files for manual uploading into the Treasury's SPS. An ARC Data Entry Operator (DEO) submits bulk files created in Oracle via drop zones to Fiscal Service's Kansas City Finance Center PAM. The DEO

creates a summary schedule in Oracle that is imported into SPS. An 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 assigns a due date 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 the interest, and generates an interest payment to the vendor, provided the total interest is one dollar or more.

Reconciliation Citibank Activity

ARC accountants perform reconciliations of CitiManager account statement balances to Accounts Payable transaction details in Oracle which are reviewed by ARC Staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy.

Reconciliation – Fund Balance With Treasury Activity

Treasury provides the following reports to inform agencies of their FBWT activity and balances and to assist agencies in reconciling their FBWT general ledger balances to Treasury's balances:

- CARS Agency Location Code (ALC) Statement (ALC Transactions) provides increases and decreases to balances, for the Reporting ALC by Treasury Account Symbol (TAS).
- CARS Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

As month-end approaches ARC accountants reduce the probability of month-end differences relating to disbursements by performing a month-to-date reconciliation of Treasury's disbursement systems to the Oracle general ledger FBWT disbursement activity.

ARC accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by ARC Staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in the accounting system by an accounting technician or another accountant who neither prepared nor reviewed the FBWT reconciliation.

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 various accounting strings at the allocation levels.

Budget execution system controls can be set to prevent spending beyond the budget planned amount or allow expenditures at any dollar amount of the budget plan. Expenditures beyond the apportionment and appropriation levels (legal levels) is prohibited. System controls are designed to prevent the user from apportioning more than was appropriated and allocating more than was

apportioned. Decisions on control settings that permit or prevent expenditures beyond the budget plan are determined by the customer agency. System controls are applied at the fund level after passage of appropriation legislation and a high-level budget is loaded at the appropriation level. Upon receipt and input of a detailed financial plan, controls are established at the allocation level when desired by the customer agency.

Budget execution settings are determined by the customer agency and set-up in Oracle by the USB ARC staff. System settings are reviewed with the customer agency on an annual basis, input by USB staff, and then reviewed by a supervisor for completeness and accuracy.

Intragovernmental Transactions

ARC adheres to applicable intragovernmental elimination guidance in the Treasury Financial Manual (TFM). This involves recording transactions at a level that allows for identification of ARC's governmental trading partners and for reconciling the transactions/balances with trading partners on a quarterly basis in GTAS. For the non-fiduciary transactions of ARC's Treasury 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. For Non-Treasury customers, if there are any elimination differences that require an explanation, an accountant will enter the explanation in the GTAS module and an ARC Supervisor or an Agency designee will certify the explanation in GTAS. For Treasury customers, the eliminations reporting is handled through the TIER reporting process.

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 site 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.

Complementary Customer Agency Controls

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 received at the customer agency are reviewed to determine whether they properly reflect the invoice receipt date and provide correct received and acceptance dates for goods or services according to the Prompt Payment Act.
- Approve travel vouchers and accurately enter the vouchers into ConcurGov in the proper period.
- Approve and return relocation travel authorizations 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.

- Review and communicate customer agency required levels of budget and expenditure controls to ARC.
- Properly allocate Citibank charges and obtain Approving Official certification prior to auto-close.
- Provide post payment approval for Citibank auto-closed invoices.
- Maintain and communicate to ARC a list of individuals and applicable authority limits authorized to request non-referencing payments and expense corrections.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of disbursements and determined the procedures were formally documented for the processing of disbursements.
2. For a selection of invoices, inspected documentation of customer agency authorization and related general ledger entries and determined disbursements were authorized and processed timely.
3. For a selection of IPAC transactions, inspected documentation of customer agency authorization and related general ledger entries and determined disbursements were authorized and processed timely.
4. For a selection of days, inspected approved IPP invoices and determined the invoices successfully interfaced with Oracle, and new purchase orders for IPP vendors were successfully interfaced with IPP.
5. Observed the daily ConcurGov interface and reconciliation and noted approved travel disbursements were interfaced into Oracle, and Oracle recorded the disbursements to the general ledger.
6. For a selection of days, for a selection of customer agencies, inspected ConcurGov voucher reconciliations and determined approved vouchers in ConcurGov were reconciled to Oracle daily by an accounting technician.
7. Observed a user in ConcurGov attempt to approve their own voucher and noted the system automatically prevented the user from approving their own travel voucher.
8. Observed moveLINQ relocation vouchers interfaced into Oracle and noted the approved vouchers interfaced via automated batch process.
9. For a selection of days, inspected moveLINQ authorizations and determined the authorizations were reconciled daily by an Accounting Technician with an Oracle generated report.
10. Observed an accountant process an invoice over $2,500 and determined the system automatically placed the invoice on hold and routed the invoice to a secondary lead accounting technician or an accountant for review and approval.
11. For a selection of months, inspected evidence of the review of invoices, including IPP invoices less than $2,500, and determined the review performed was subjected to random sampling by a lead accounting technician or an accountant.
12. For a selection of months, inspected an Oracle reports to show a listing of invoices processed and approved by the same individual and noted there were no invoices created; therefore, could not test to determine whether invoices greater than $2,500 were both processed and approved by the same individual and the review was performed appropriately.
13. For a selection of months for a selection of customer agencies, inspected evidence of ARC's review of 10% of all processed invoices by IPP and determined the review was performed appropriately and discrepancies were resolved.
14. For a selection of weeks for a selection of customer agencies, inspected evidence and determined the quality sampling was performed, audit worksheets were completed for selected vouchers and reviewed, and any errors were followed-up on.
15. For a selection of months for a selection of customer agencies, inspected evidence and determined the statistical sampling was performed, audit worksheets were completed for selected vouchers and reviewed, and any errors were followed-up on.

16. For a selection of days, inspected evidence that the ARC SPS certifying officer comparison of the number and dollar amount of payments from SPS payment schedule and Oracle, and determined the review was completed daily and the interfaces uploaded completely.

17. For a selected invoice subject to the Prompt Payment Act, inspected invoice documentation and determined that Oracle was configured to schedule disbursements 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).

18. 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.

19. For a selected late payment, recalculated the interest owed and determined Oracle calculated the Prompt Payment interest accurately.

20. For a selection of months for a selection of customer agencies, inspected evidence of the Reconciliation of Citibank activity performed and determined reconciliation was performed, reviewed, and any differences were resolved.

21. For a selection of months for a selection of customer agencies, inspected reconciliations and determined accountants reconciled CARS Account Statements and Undisbursed Appropriation Account Ledger Reconciliations and supervisory reviews were completed.

22. For a selection of customer agencies, inspected their budget execution set-up in Oracle and determined that the settings were set-up in Oracle and that the active budget execution settings were reviewed with the customer agency on an annual basis.

23. For a selection of quarters for a selection of Non-Treasury customers, inspected the non-fiduciary transaction confirmation completed by ARC accountants and determined a) reconciliations of transactions and balances with trading partners were completed, b) any necessary adjustments were identified and recorded, and c) any elimination differences that required an explanation were entered into the GTAS module and an ARC Supervisor or Agency designee certified the explanation in GTAS.

24. For a selection of quarters for a selection of Treasury customers, inspected the non-fiduciary transaction confirmations completed by ARC accountants and determined reconciliations of transactions and balances with trading partners were completed, any necessary adjustments were identified and recorded, and any elimination reporting was completed using the TIER reporting process.

25. Observed an ARC user attempt to enter a transaction identification number that already exists and noted Oracle issued an error message that alerted the user of the duplication and automatically rejected the entry of a duplicate transaction 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 authorized, 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. No approval is required for checks received for deposit directly by ARC on the customer agency's behalf to satisfy accounts receivable invoices, 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

Treasury provides the following reports to inform agencies of their FBWT activity and balances and to assist agencies in reconciling their FBWT general ledger balances to Treasury's balances:

- CARS ALC Statement (ALC Transactions) provides increases and decreases to balances, for the Reporting ALC by TAS.
- CARS Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

As month-end approaches ARC accountants reduce the probability of month-end differences relating to receipts by performing a month-to-date reconciliation of Treasury's receipt systems to general ledger FBWT receipt activity.

ARC accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by ARC Staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in Oracle by an accounting technician or another accountant who neither prepared nor reviewed the FBWT reconciliation.

Reporting - Receivables

ARC accountants prepare and submit a quarterly TROR and Debt Collection Activities report for all customer agencies. These reports require 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 TROR and Debt Collection Activities report review and reconcile all activity (i.e., new receivables, revenue accruals, collections, adjustments and write-offs) with receivables due from the public on a quarterly basis. An ARC supervisory accountant reviews the report. As applicable, ARC monitors and pursues collection of delinquent balances. On an annual

basis, the customer agency's Chief Financial Officer must certify that the report submitted to the Treasury is accurate and consistent with agency accounting systems.

Intragovernmental Transactions

ARC adheres to applicable intragovernmental elimination guidance in the TFM. 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 in GTAS. For the non-fiduciary transactions of its Treasury 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. For Non-Treasury customers, if there are any elimination differences that require an explanation, an accountant will enter the explanation in the GTAS module and an ARC Supervisor or an Agency designee will certify the explanation in GTAS. For Treasury customers, the eliminations reporting is handled through the TIER reporting process.

Document Numbering

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

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Send approved and accurate documentation of unfilled customer orders, receivables, and 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 as applicable.
- Customer agency's Chief Financial Officer must certify that the TROR and Debt Collection Activities report submitted to the Treasury is accurate and consistent with agency accounting systems.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of unfilled customer orders, and cash receipts, receivables and determined the procedures were formally documented.
2. For a selection of unfilled customer orders, inspected evidence and determined the unfilled customer orders were only processed by ARC after being approved by the customer agency.
3. For a selection of receivables, inspected evidence and determined the receivables were only processed by ARC after being approved by the customer agency.
4. For a selection of cash receipts, inspected evidence and determined the cash receipts were only processed by ARC after being approved by the customer agency.
5. For a selection of months for a selection of customer agencies, inspected reconciliations and determined accountants reconciled the CARS Account Statements and Undisbursed Appropriation Account Ledger Reconciliations and supervisory reviews were completed.

6. For a selection of quarters for a selection of customer agencies, inspected the Treasury Report on Receivables (TROR) and Debt Collection Activities reports completed by ARC accountants and determined they were completed, all activities were reconciled with receivables due from the public, and the reports were reviewed by an ARC supervisory accountant.

7. For a selection of quarters for a selection of Non-Treasury customers, inspected the non-fiduciary transaction confirmations completed by ARC accountants and determined a) reconciliations of transactions and balances with trading partners were completed, b) any necessary adjustments were identified and recorded, and c) any elimination differences that required an explanation were entered into the GTAS module and an ARC Supervisor or Agency designee certified the explanation in GTAS.

8. For a selection of quarters for a selection of Treasury customers, inspected the non-fiduciary transaction confirmations completed by ARC accountants and determined reconciliation of transactions and balances with trading partners were completed, any necessary adjustments were identified and recorded, and any elimination reporting was completed using the TIER reporting process.

9. Observed an ARC user attempt to enter a transaction identification number that already existed and noted Oracle issues an error message alerting the user of the duplication and automatically rejected the entry.

No exceptions noted.

Control Objectives, Related Controls, and
Tests of Operating Effectiveness

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 individually with the supporting documentation that came with each check. Each check with the documentation is saved as a separate file in a central location. The checks, along with the original documentation, are sent to the A3F mail drop by the mail deliverer and signed for if delivery confirmation was requested. An ARC accounting technician (who does not have accounting system access to post accounts receivable transactions) receives, opens and logs all checks received in the ARC's check deposit log. The same technician retrieves the scanned images from a central location and saves each image in the appropriate folder. These scanned files are archived annually. For reconciliation purposes, the check total scanned by mail services is compared to the number received by placing a "Y" in the "Rec'd" column on each check log. This confirms that all checks scanned at mail services were received and logged by the technician.

Checks are to be deposited as soon as possible after the purpose and validity of the check's issuance are identified. The accounting technician is responsible for processing deposits, but the customer agency or its delegate is responsible for researching the check's purpose and validity. The checks are locked in a secure location until they are ready to be deposited.

Over the Counter Channel Application

The Over the Counter Channel Application (OTCnet) is a web-based application that accommodates "check capture" and "deposit reporting and processing" using electronic collection mechanisms instead of paper-based processing.

On the "check capture" side of OTCnet, checks are scanned for deposit and a batch list is created. The batch list is automatically saved temporarily to the server until it is transmitted to the Federal Reserve Bank (FRB) by the ARC accounting technician. Upon settlement with the FRB, the ARC accounting technician reconciles the batch list with the paper checks. After reconciliation, the checks are held awaiting confirmation of the deposit in the Treasury's deposit application. Upon confirmation, the ARC accounting technician destroys the checks. The cash receipt is recorded in Oracle by an ARC staff member other than the individual processing the deposit in OTCnet.

On the "deposit reporting and processing" side of OTCnet, an ARC accounting technician will manually enter the deposit information into the OTCnet system. A deposit ticket and the check(s) are sent in a locked money bag that is picked up by a mail clerk who then delivers it to the local federal depository. A copy of the deposit ticket is retained by the ARC accounting technician for comparison with the deposit receipt from the bank teller and the confirmed deposit ticket from the OTCnet system. The money bag containing the bank teller's deposit receipt is returned to the branch office that processed the deposit. After the bank teller receipt and OTCnet confirmed deposit ticket are compared to the copy retained by the branch, the cash receipt is recorded in Oracle by an ARC accounting technician.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Provide assistance, when requested, to determine a check's purpose and validity prior to deposit.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the safeguarding and recording of deposits and determined the procedures were formally documented for the safeguarding and recording of deposits.
2. For a selection of days, inspected the checks received by the mailroom and the associated deposit check log and determined the deposit check log agreed to the original checks.
3. Inspected a selection of check deposit logs and determined an ARC administrative staff member, who does not have accounting system access to post account receivable transactions, received, opened and logged all checks received in the branch's check deposit log.
4. Inspected a selection of check deposit records and check attributes and determined checks were deposited timely after the purpose and validity of each check's issuance were identified.
5. Inspected a selection of check deposits and the subsequent posting to Oracle by ARC staff, of the OTCnet confirmed check deposit amounts, and determined the total checks were posted completely and accurately to Oracle.
6. Inspected a selection of check deposits and determined the deposit was recorded in Oracle by an ARC staff member other than the individual who processed the deposit.

No exceptions noted.

Control Objective 5 – Payroll and Leave Accruals

Controls provide reasonable assurance that period-end payroll and leave 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

Monthly Payroll accruals are recorded and reviewed on a monthly basis by an accountant and reversed in the subsequent accounting period. The payroll accrual is a prorated calculation performed by the accounting system. 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).

Leave Accruals are recorded and reviewed based on an agreed upon schedule with the customer agency (bi-weekly, monthly, quarterly) and reversed prior to recording the next scheduled leave accrual. The leave accrual calculation is performed by the accounting system based on data provided by the customer agency's payroll service provider. To make its calculation the accounting system requires a payroll accountant to enter specific parameters (e.g., pay period and pay year).

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Review the financial reports provided by ARC to ensure that monthly payroll and leave accruals are complete and accurate.
- Review and confirm leave accrual schedule annually.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of payroll and leave accruals and determined that the procedures were formally documented for the processing of payroll and leave accruals.
2. For a selection of months and quarters, inspected a selection of customer agencies' monthly and quarterly payroll accruals invoices and determined the customer agencies' monthly and quarterly payroll accruals were documented, entered timely and accurately, and reviewed by an ARC accountant.
3. For a selection of months and quarters, inspected a selection of customer agency's leave accruals and determined the leave accruals were documented, entered timely and accurately, and reviewed.

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 service providers transmit payroll files to ARC after each pay period. Payroll files are imported into Oracle. After import, the ARC payroll accountant confirms the file loaded in its entirety by verifying the total payroll costs as indicated on the payroll file to the import summary amount. 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. An OBI or 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 is viewed as invalid and will not be able to be posted to the general ledger. If the payroll service provider has adjustment files for additional transactions between main payroll files, the ARC payroll accountant follows the same procedure for processing these files.

Reconciliation – Payroll Activity

Each month, payroll accountants prepare, for supervisory review, a reconciliation of payroll disbursements recorded in Oracle and payroll disbursements as reflected in Treasury's cash systems. The payroll accountant investigates and resolves any differences identified. All those that require corrections, are posted in either the current accounting period or in a subsequent accounting period.

Complementary Customer Agency Controls

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.
- Review and confirm customer specific payroll disbursement procedures on an annual basis.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of payroll disbursements and determined the procedures were formally documented for the processing of payroll disbursements.
2. For a selection of pay periods, for a selection of customer agencies, inspected interface errors reports and determined during the interface, input files were checked for errors but no errors were identified.

3. For a selection of months for a selection of customer agencies, inspected reconciliations of the payroll disbursements recorded in Oracle to the payroll disbursements as reflected in Treasury's cash systems and determined the reconciliations were completed by an ARC accountant, any differences identified were investigated and resolved, reconciliations were reviewed by a supervisory accountant and any corrections made were posted in the current or subsequent accounting periods.

No exceptions noted.

Control Objective 7 – USSGL

Controls provide reasonable assurance that transactions are processed in accordance with the USSGL and 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, Sub-Ledger Accounting (SLA) 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 authorization from a supervisor or manager to establish new posting models for transaction processing.

On an annual basis, ARC reviews 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 and the new TFM guidance is issued (generally mid-summer), ARC USSGL Team will communicate the appropriate changes to system administrators to ensure the accounting transaction posting models are revised.

General Ledger Account Reconciliations

Accountants perform general ledger account reconciliations (utilizing accounting system sub ledgers or Excel spreadsheets when available) on balance sheet accounts to ensure related accounting transactions were posted to the appropriate general ledger accounts. Upon completion, the subledger reconciliations are reviewed by a supervisor. ARC accountants prepare budgetary to proprietary account relationship reconciliations on a monthly basis to ensure complete general ledger account posting for all recorded transactions. Upon completion, the budgetary to proprietary reconciliations are reviewed by a supervisor. If invalid relationships are identified an accounting technician or an accountant corrects the transaction or prepares an entry to resolve the invalid relationships.

GTAS Edit Checks

ARC submits the GTAS files for its non-Treasury customers, except for the Department of Homeland Security, using a bulk file upload. Accountants create the bulk file 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 GTAS files created from Oracle into the GTAS system. The GTAS system performs USSGL validations and edit checks and either rejects or fails any Treasury Appropriation Fund Symbol (TAFS) that fail the validations or edit checks. ARC investigates and resolves any TAFS rejected or failed by the GTAS system.

Treasury Information Executive Repository Validation Checks

For ARC's Department of the Treasury and Department of Homeland Security customer agencies, GTAS reporting requirements are met using TIER. TIER is a 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 utilizes custom solutions that extract accounting and budgetary data from Oracle to generate necessary TIER data. TIER has a standardized chart of accounts that is compliant with USSGL guidance issued by the Treasury. GTAS 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 (BS), Statement of Net Cost (SNC)* and *Statement of Budgetary Resources (SBR)* for all customer agencies that are covered by the Chief Financial Officer Act and the Accountability of Tax Dollars Act of 2002. Additionally, ARC accountants prepare the *Statement of Changes in Net Position (SCNP),* and *Statement of Custodial Activity (SCA)* (when applicable) for all customer agencies. ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream tables to determine compliance with the TFM reporting requirements. ARC investigates and resolves any differences between TFM crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Department of the Treasury and Department of Homeland Security customer agencies, quarterly financial statements are produced by departmental systems using the data submitted in TIER. Third and fourth quarter consolidated financial statements are submitted to the Director of Office of Management and Budget (OMB) and the Congress by the Department. The *SCNP* and *SCA* are only submitted to the Director of the OMB and the Congress for the fourth quarter. ARC accountants compare the Department of the Treasury and Department of Homeland Security customer agencies quarterly financial statements to ARC's internally prepared financial statements and resolve any differences. The comparison is reviewed by a supervisor.

If applicable for non-Treasury customer agencies, ARC accountants prepare the *BS*, *SNC*, and *SBR* during the third and fourth quarters for review by a supervisor and submission to OMB. During the fourth quarter the *SCNP* and *SCA* may also be included in the supervisor review and submission to OMB. For customers using OneStream, there are additional checks to compare the OneStream trial balance to the Oracle trial balance and GTAS balances.

Financial Statement Variance Analysis

For both Department of the 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 chief financial officer (CFO) or designee prior to submission to the Department. The Homeland Security bureau variance is also approved by the Homeland Security's CFO or designee.

For non-Treasury and non-Homeland Security customer agencies, accountants prepare a third quarter financial statement variance analysis based on the guidance in OMB Circular A-136. The variance analysis is reviewed by an ARC supervisory accountant prior to submission to OMB.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Review and approve, prior to submission, the financial reports prepared by ARC to ensure that reports prepared for external use are complete, accurate, and submitted in a timely manner.
- The Homeland Security bureau variance is also approved by the Homeland Security's CFO or designee.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures in the TFM for the processing of transactions consistent with the USSGL and determined that the procedures were formally documented.
2. Observed the processing of a transaction to an inappropriate USSGL account and noted the Oracle cross-validation rules rejected the transaction.
3. Inspected a list of users with access to change posting models, inquired of management, and determined the users assigned the system administrators role responsibility have appropriate access for making changes to the models.
4. For a selection of newly established posting models, inspected ARC supervisory approval of the new posting model and TFM/USSGL guidance and determined the new posting models were authorized and were in agreement with TFM/USSGL guidance.
5. Inspected evidence of the annual review of USSGL account titles and descriptions and determined the annual review was performed by ARC supervisors and Managers and necessary updates were made.
6. For a selection of months, for a selection of customer agencies, inspected the budgetary to proprietary account relationship reconciliations completed by ARC accountants and determined general ledger accounts postings were completed for all recorded transactions, invalid relationships identified were corrected by an accounting technician or accountant, and reconciliations were reviewed by an ARC supervisor.
7. Observed ARC staff run the Oracle job that creates the GTAS bulk data upload file for non-Treasury/non-Department of Homeland Security customers and determined Oracle runs the data through several edit checks prior to creating the bulk upload file.
8. Observed ARC staff manually load the GTAS files created from Oracle into the GTAS system and noted Oracle and GTAS performs USSGL validations and edit checks and either rejects or fails any TAFS that fail the validations or edit checks.
9. For a selection of months for a selection of customer agencies, inspected the TIER Submission Checklists and determined ARC accountants reviewed GTAS edit reports and resolved any invalid attributes or out-of-balance attributes included in corresponding TIER submissions.
10. For a selection of quarters for a selection of customer agencies, inspected the results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements and determined ARC investigated and resolved any differences.
11. For a selection of quarters for a selection of customer agencies, inspected the reconciliations of the financial statements prepared by the Department to ARC's internally prepared financial statements and determined reconciliations were performed and reviewed by a supervisor, and any differences noted are resolved.

12. For a selection of quarters for a selection of customer agencies, inspected financial statement variance analyses and determined that they were reviewed by an ARC supervisor and approved by the bureau CFO or designee prior to being submitted to the Department.

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.

<u>Description of Controls</u>

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

<u>Revenue and Expense Accruals</u>

ARC staff record period-end accruals for goods and services provided/received, but not billed/invoiced, in Oracle based on instruction provided from the customer agency. The amounts recorded are based on information provided by e-mail from the customer agency or obtained from a subsidiary system, using one of two methods: standard transaction processing method or the automated journal entry process method.

In the standard transaction processing method, ARC staff record accruals in Oracle through standard accrual transaction receipts.

In the automated journal entry process method, accruals are recorded by using the automated journal entry process. With this method, an ARC staff member enters information received from the customer agency or subsidiary system into a spreadsheet template, reviews the spreadsheet and converts it into a data file that is automatically loaded into Oracle. The Oracle entry is reviewed and approved by a supervisory accountant.

<u>Non-Invoice Accruals</u>

Accountants record in Oracle non-invoice related expense accruals for items such as workers' compensation, unemployment insurance liability, year-end payroll accruals and non-batch leave accruals. Workers' compensation and unemployment insurance accruals are based on reports provided from the Department of Labor. Customer agencies provide data for year-end payroll accruals. Customer agencies' payroll service providers or the human resource office provide non batch leave accrual data. An ARC staff member enters accrual data into a spreadsheet template, reviews the spreadsheet and converts it into a data file that is automatically loaded into Oracle. The Oracle entry is reviewed and approved by a supervisory accountant.

<u>General Ledger to Subledger Reconciliation</u>

On a monthly basis, ARC accountants prepare a reconciliation of revenue and expense accrual balances in the general ledger to the sub ledger 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.

<u>Budget Execution System Controls</u>

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 various accounting strings at the allocation levels.

Budget execution system controls can be set to prevent expenditures beyond the budget plan amount or allow expenditures over the budget plan amount at any level of the budget plan. Expenditures beyond the apportionment and appropriation levels (legal levels) is prohibited. System controls are designed to prevent the user from apportioning more than was appropriated and allocating more than was apportioned. Decisions on control settings that permit or prevent expenditures beyond the budget plan levels are determined by the customer agency. System controls are applied at the fund level after passage of appropriation legislation and a high-level budget is loaded at the allocation level. Upon receipt and input of a detailed financial plan, controls are established at the allocation level when desired by the customer agency.

Budget execution settings are determined by the customer agency and set-up in Oracle by USB staff. System settings are reviewed with the customer agency on an annual basis, input by USB staff, and then reviewed by a supervisor for completeness and accuracy.

<u>Document Numbering</u>

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 processed through standard accrual 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.

Complementary Customer Agency Controls

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.
- Review and communicate customer agency required levels of budget and expenditure controls to ARC.
- Review the financial reports provided by ARC to ensure that accruals are complete and accurate.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of accruals and determined that the process for processing accruals was formally documented.
2. For a selection of period-end accruals for goods and services provided or received, but not billed or invoiced for a selection of customer agencies, inspected evidence of the Oracle entry and determined the accounting technician followed the instructions provided from the customer agency and the Oracle entry was reviewed and approved by a supervisory accountant.
3. For a selection of customer agencies, inspected evidence of the year-end payroll accrual data loaded into Oracle and determined the entry was imported successfully and posted to the general ledger.
4. For a selection of quarters for a selection of customer agencies, inspected evidence of the non batch leave accrual data loaded into Oracle and determined the entry was reviewed and approved by a supervisory accountant.
5. For a selection of months for a selection of customer agencies, inspected evidence of the reconciliation of revenue and expense accrual balances in the general ledger to the sub ledger detail and determined any differences noted were corrected by an accounting technician or

accountant in a subsequent accounting period, and the reconciliation was reviewed by a supervisor.
6. For a selection of customer agencies, inspected their budget execution set-up in Oracle and determined the settings were set-up in Oracle and the active budget execution settings were annually reviewed with the customer agency.
7. Observed an ARC staff member attempt to enter a transaction identification number that already existed and noted Oracle issued an error message alerting the user of the duplication and automatically rejected the entry.

No exceptions noted.

Control Objective 9 – Governmentwide Reporting

Controls provide reasonable assurance that Governmentwide reporting is complete, accurate, timely, and performed in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for the preparation of Governmentwide reports.

GTAS

ARC policies require the submission of GTAS reports based on Fiscal Service's criteria for these applications. GTAS is a web-based system for use in the Governmentwide reporting setting as the primary means of reporting agency trial balance and eliminations data. This single data collection system is designed to pave the way for more consistent and complete financial data and allows for better analytical reporting. All submissions must pass all GTAS data validations and 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 GTAS submissions require certification by an ARC supervisor or manager, or other designated customer agency representative.

TIER

Generally, Treasury customer agencies are required to submit financial accounting and budgetary data each month to TIER, Treasury's data warehouse within Treasury's submission timeline. The Department of Homeland Security customer agencies are required to submit financial accounting and budgetary data each month to TIER, Homeland Security's data warehouse, within Homeland Security's submission timeline. 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 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.

Prompt Payment

ARC prepares monthly Prompt Payment reports for its customers following Treasury guidelines. Independent accountants or analysts review all reports.

Financial Statement Crosswalks

ARC accountants prepare a *BS, SNC, and SBR* for all customer agencies that are covered by the Chief Financial Officer Act and the Accountability of Tax Dollars Act of 2002. Additionally, ARC accountants prepare the *SCNP and SCA* (when applicable) for all customer agencies. ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream table to ensure compliance with the reporting requirements. ARC investigates and resolves any differences between TFM crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Department of the Treasury and Department of Homeland Security customer agencies, quarterly financial statements are produced by departmental systems using the data submitted in

TIER. Third and fourth quarter consolidated financial statements are submitted to the Director of OMB and the Congress by the Department. The *SCNP and SCA* are only submitted to the Director of the OMB and the Congress for the fourth quarter. ARC accountants compare the quarterly financial statements to ARC's internally prepared financial statements and resolve any differences. The comparison is reviewed by a supervisor.

If applicable for non-Treasury customer agencies, ARC accountants prepare the *BS*, *SNC*, and *SBR* during the third and fourth quarters for review by a supervisor and submission to OMB. During the fourth quarter the SCNP and SCA may also be included in the supervisor review and submission to OMB. For customers using OneStream, there are additional checks to compare the OneStream trial balance to the Oracle trial balance and GTAS balances.

Financial Statement Variance Analysis

For both Department of the Treasury and Department of Homeland and 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 is also approved by the Homeland Security's CFO or designee.

For non-Treasury and non-Homeland Security customer agencies, accountants prepare a third quarter financial statement variance analysis based on the guidance in OMB Circular A-136. The variance analysis is reviewed by an ARC supervisory accountant prior to submission to OMB.

Receivables

ARC accountants prepare and submit a quarterly TROR and Debt Collection Activities report for all customer agencies. These reports are reviewed by an ARC supervisory accountant prior to submission to Treasury. On an annual basis, the customer agency's CFO must certify that the report submitted to the Treasury is accurate and consistent with agency accounting systems.

DATA Act

Generally, Treasury and Homeland Security customer agencies are each required to submit a customized Award Financial File each month to their respective TIER or repositories. To meet this requirement, ARC utilizes Oracle to generate an Award Financial File for Treasury and Homeland Security customer agencies. ARC submits the Award Financial File into TIER for Treasury customer agencies and request the Treasury customer agency to validate the data. ARC sends an Award Financial File to Homeland Security customer agencies.

For non-Treasury and non-Homeland Security customer agencies, DATA Act reporting is performed on a quarterly basis. For those customers, three files are submitted to the governmentwide DATA Act Broker system (Broker) on a quarterly basis. The Broker has validation checks with the GTAS submissions. The accountants review the reports produced by the Broker. Upon completion of the accountants' review, a reconciliation package is sent to the customer agency for review and approval. Upon receipt of the customer agency approval, ARC updates the status of the DATA Act Files submission to "Certified" on behalf of the customer agency.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Review and approve, prior to submission, 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 and approve the annual submission of the TROR and Debt Collection Activities report.
- Provide certification of GTAS to ARC prior to system certification.
- Customer agency's Chief Financial Officer must certify that the report submitted to the Treasury is accurate and consistent with agency accounting systems.
- The Homeland Security bureau variance is also approved by the Homeland Security's CFO or designee.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures and determined ARC had documented procedures for the preparation of governmentwide reports.
2. For a selection of quarterly GTAS submissions for a selection of customer agencies, inspected evidence of management review and determined selected submissions were reviewed and certified.
3. For a selection of months for a selection of customer agencies, inspected TIER Submission Checklists and determined TIER submissions were reviewed by an ARC supervisor before being processed by TIER.
4. For a selection of months for a selection of customer agencies, inspected the corresponding Prompt Payment reports and determined they were reviewed by a supervisory accountant before submission.
5. For a selection of quarters for a selection of customer agencies, inspected the reconciliation of customer agencies' financial statements prepared by ARC, to ARC's internally prepared financial statements, and determined the reconciliations were reviewed by a supervisor, and any differences noted were resolved.
6. For a selection of quarters for a selection of customer agencies, inspected the financial statement variance analyses and determined it was reviewed by an ARC supervisory accountant prior to being submitted to ARC.
7. For a selection of quarters for a selection of customer agencies, inspected the TROR and Debt Collection Activities and determined the reports were reviewed by an ARC supervisory accountant.
8. For a selection of quarters for a selection of customer agencies, inspected results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements and determined ARC investigated and resolved any differences.
9. For a selection of quarters for a selection of customer agencies, inspected ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements and determined the internally prepared financial statements were in compliance with the customer agency's government wide reporting requirements.
10. For a selection of months for a selection of Treasury customers, inspected supporting documentation and determined the customer's monthly DATA Act submission was appropriately completed, reviewed, and submitted in TIER as required.

11. For a selection of quarters for a selection of non-Treasury and non-Homeland Security customer agencies, inspected supporting documentation and determined the customer's quarterly DATA Act submission was appropriately completed, reviewed, and authorized by the customer agency prior to being submitted in the DATA Act Broker.

No exceptions noted.

Control Objective 10 – Expenditures

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

<u>Description of Controls</u>

ARC has documented procedures related to expenditure controls.

<u>Budget Execution System Controls</u>

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 various accounting strings at the allocation levels.

Budget execution system controls can be set to prevent expenditures beyond the budget plan amount or allow expenditures over the budget plan amount at any level of the budget plan. Expenditures beyond the apportionment and appropriation levels (legal levels) is prohibited. System controls are designed to prevent the user from apportioning more than was appropriated and allocating more than was apportioned. Decisions on control settings that permit or prevent expenditures beyond the budget plan levels are determined by the customer agency. System controls are applied at the fund level after passage of appropriation legislation and a high-level budget is loaded at the appropriation level. Upon receipt and input of a detailed financial plan, controls are established at the allocation level when desired by the customer agency.

Budget execution settings are determined by the customer agency and set-up in Oracle by the USB staff. System settings are reviewed with the customer agency on an annual basis, input by USB staff, and then reviewed by a supervisor for completeness and accuracy.

<u>Reconciliation – Budgetary and Proprietary Account Relationships</u>

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.

<u>Reconciliation – Fund Balance With Treasury Activity</u>

Treasury provides the following reports to inform agencies of their FBWT activity and balances and to assist agencies in reconciling their FBWT general ledger balances to Treasury's balances:

- CARS ALC Statement (ALC Transactions) provides increases and decreases to balances, for the Reporting ALC by TAS.
- CARS Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

As month-end approaches ARC accountants reduce the probability of month-end differences relating to disbursements by performing a month-to-date reconciliation of Treasury's disbursement systems to general ledger FBWT disbursement activity.

ARC accountants perform monthly reconciliations of CARS Account Statement balances to general ledger FBWT balances which are reviewed by ARC staff other than the individual

performing the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in the accounting system by an accounting technician or another accountant who neither prepared nor reviewed the FBWT reconciliation.

Complementary Customer Agency Controls

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 documents to RSB for processing in moveLINQ in a timely manner.
- Send approved requests to record manual obligations to ARC in a timely manner.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Review and approve listing of users with current Oracle, PRISM, webTA, ConcurGov, IPP, OneStream, and HRConnect access to ensure appropriateness and provide changes to ARC in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to ARC.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures related to expenditures and determined that the procedures were formally documented.
2. For a selection of customer agencies, inspected their respective budget plan instructions and determined customer agencies specified their budget controls for the year, the instructions were input by SDB staff, and then reviewed by a supervisor for completeness and accuracy.
3. For a selection of months for a selection of customer agencies, inspected the budgetary to proprietary account relationship reconciliations completed by ARC accountants and determined general ledger accounts postings were completed for all recorded transactions, invalid relationships identified were corrected by an accounting technician or accountant, and the reconciliation was reviewed by an ARC supervisor.
4. For a selection of months for a selection of customer agencies, inspected reconciliations of CARS Account Statement balances to general ledger FBWT balances and determined accountants performed the reconciliations and the reviews were completed by staff other than the individuals who performed the reconciliations, and differences were resolved.

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 institute and monitor both legally established and internally developed budget plans in Oracle to help ensure obligations are authorized and recorded. Budget plans can be established at various accounting strings at the allocation levels.

Budget execution system controls can be set to prevent expenditures beyond the budget plan amount or allow expenditures over the budget plan amount at any level of the budget plan. Expenditures beyond the apportionment and appropriation levels (legal levels) is prohibited. System controls are designed to prevent the user from apportioning more than was appropriated and allocating more than was apportioned. Decisions on control settings that permit or prevent expenditures beyond the budget plan levels are determined by the customer agency. System controls are applied at the fund level after passage of appropriation legislation and a high-level budget is loaded at the appropriation level. Upon receipt and input of a detailed financial plan, controls are established at the allocation level when desired by the customer agency.

Budget execution settings are determined by the customer agency and set-up in Oracle by USB staff. System settings are reviewed with the customer agency on an annual basis, input by USB staff, and then reviewed by a supervisor for completeness and accuracy.

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 Activity

Treasury provides the following reports to inform agencies of their FBWT activity and balances and to assist agencies in reconciling their FBWT general ledger balances to Treasury's balances:

- CARS ALC Statement (ALC Transactions) provides increases and decreases to balances, for the Reporting ALC by TAS.
- CARS Account Statement (Account Summary) provides beginning balance, current month net activity and ending balance.

As month-end approaches ARC accountants reduce the probability of month-end differences relating to disbursements by performing a month-to-date reconciliation of Treasury's disbursement systems to general ledger FBWT disbursement activity.

ARC accountants perform monthly reconciliations of CARS Account Statement balances to general ledger FBWT balances which are reviewed by ARC staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, ARC accountants determine the cause of the difference and the action, if any, that is needed to resolve the discrepancy. If the difference requires correction, an entry is posted in the accounting system by an accounting technician or another accountant who neither prepared nor reviewed the FBWT reconciliation.

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 customer specific 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.

Complementary Customer Agency Controls

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.
- Review and communicate customer agency required levels of budget and expenditure 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.

<u>Tests of Operating Effectiveness and Results of Testing</u>

1. Inspected written procedures for the processing budget entries and determined that the procedures were formally documented.
2. For a selection of customer agencies, inspected their respective budget plan instructions and determined customer agencies specified their budget controls for the year, the budget plan instructions were inputted by SDB staff, and then reviewed by a supervisor for completeness and accuracy.
3. For a selection of months for a selection of customer agencies, inspected reconciliations of CARS Account Statement balances to general ledger FBWT balances and determined accountants performed the reconciliations and the reviews were completed by staff other than the individuals who performed the reconciliations, and differences were resolved.
4. Observed an ARC staff member attempt to enter a transaction with a document number that had already been entered into Oracle and noted Oracle automatically rejected the entry of a duplicate document number.

No exceptions noted.

Control Objective 12 – Manual Journal Entries

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

Description of Controls

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

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 an authorized approver's queue. Documentation supporting the journal entry accompanies each request for approval. The approver compares the documentation to Oracle and approves the journal entry.

A user's profile in OneStream determines whether or not the user can prepare and/or approve a manual journal entry. OneStream system controls require all manual JEs are approved by a supervisor. Once a user has entered a journal entry in OneStream it becomes available for review and approval by any supervisor. Documentation supporting the journal entry accompanies each request for approval. The approver compares the documentation to OneStream and approves the journal Entry or returns it to the preparer for revisions, if necessary.

Document Numbering

Oracle assigns all manual journal entries a specific journal category and journal source and ARC follows a standard document numbering scheme.

A standard document numbering scheme is followed for OneStream manual JEs. OneStream automatically appends a sequential number to the end of the standard document numbering scheme to prevent any duplicate document numbers.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Send valid and approved requests to record manual journal entries to ARC in a timely manner if they are initiated by the customer agency.
- 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

1. Inspected written procedures for the processing of manual JEs and determined that the procedures were formally documented.
2. Inspected the list of Oracle users with the ability to create manual JEs and determined they were assigned a supervisor in Oracle and were subject to the automated approval work flow.

3. Inspected the list of Oracle users with the ability to approve manual JEs and the list of users with the ability to enter manual JEs and determined users without a specified supervisor did not have the ability to enter a manual journal entry.
4. For a selection of manual JEs for a selection of customer agencies, inspected JE evidence and determined that each manual journal entry was assigned a specific journal category and journal source and followed the standard numbering scheme and that the supporting documentation was compared to Oracle prior to being approved.
5. Inspected a listing of OneStream users with the ability to create manual JEs and determined that they were assigned a supervisor in the OneStream workflow.
6. Inspected a listing of OneStream users with the ability to approve manual JEs, and a listing of users with the ability to enter manual JEs and determined users without a specified supervisor do not have the ability to enter a manual journal entry.
7. For a selection of manual JEs, inspected evidence that each manual journal entry followed the standard numbering scheme and supporting documentation was compared to OneStream prior to being approved.

No exceptions noted.

Control Objective 13 – Federal Investments

Controls provide reasonable assurance that federal investments in Government Account Series (GAS) securities are authorized, reviewed, and processed timely, reconciled, and properly documented in accordance with customer agency policies and procedures.

Description of Controls

ARC accountants use FedInvest, a web-based extension of InvestOne, in order to enter investment and redemption transactions. InvestOne is a subsystem of Debt Information Management System (DIMS). The investment activity is recorded in the Oracle general ledger through a daily InvestOne interface.

FedInvest Access

ARC accountants gain access to FedInvest by completing the Bureau of the Fiscal Service FedInvest Logon ID request form which is signed by the applicant's supervisor. ARC ensures that only authorized personnel sign requests and submit transactions in FedInvest. ARC accountants only have access to authorized funds in FedInvest that is required for investment account transaction activity.

Investments

ARC accountants, per customer agency investment guidance, determine the available cash balance for investment by reviewing reports from CARS, CIR, IPAC, and Oracle and accounting for investment/redemption/maturity/interest confirmations of the current day's investment activity. The ARC accountant then enters the request into FedInvest and generates a buy request confirmation report for the entered transaction. Requests are prepared by an ARC accountant and a daily work package is then created with all the supporting documents and then two additional ARC accountants review the entered information for accuracy. Each ARC accountant digitally signs the daily work package to indicate preparation and review. If the preparer or reviewers determine the investment request has been processed incorrectly, then the accountant notifies the Federal Investments and Borrowings Branch (FIBB) so that correcting transactions may be processed before 3:00 pm ET (11:00 am ET for Zero-Coupon Bonds).

Reconciliations

Investment account transactions and corresponding United States Standard General Ledger (USSGL) accounts are reconciled between Oracle and FedInvest to ensure completeness and accuracy.

An ARC accountant performs a daily reconciliation which compares the investment account transactions within FedInvest to the dollar amounts recorded in Oracle to verify the systems reconcile.

An ARC accountant performs a monthly investment reconciliation which compares the investment account transactions, end of the month balances, and interest earned during the previous month to Oracle USSGL investment accounts and the investment transaction ledger. Once the reconciliation is complete, it is reviewed by another ARC accountant. If discrepancies exist with either reconciliation, research is conducted to determine the cause, adjust investments if necessary, and document corrective actions.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Provide ARC current investment guidance that dictates the type and amount of securities to be purchased and the amount of residual cash if any to be retained.
- Provide applicable legislation, and any subsequent legislation revisions, that authorizes the Program Agency to invest with the investment account set-up.
- Work with ARC to confirm significant investment and fund balance activity by e-mail when long-term investments are scheduled to be settled or settled in accordance with current investment guidance.
- Communicate to ARC any known delays to disbursement activity that may impact investments.
- Communicate to ARC any larger than normal disbursement activity that may impact investments.

Tests of Operating Effectiveness and Results of Testing

1. For a selection of customer agencies, inspected investment instructions and determined they were provided to ARC and defined the investment objectives for the agencies.
2. For a selection of investment purchases, inspected evidence and determined the investment purchases were reviewed and processed timely by ARC staff other than the individual who processed the investment purchase.
3. Observed the daily interface between InvestOne and Oracle and noted all investment activity in GAS securities were recorded in the general ledger.
4. For a selection of months for a selection customer agencies, inspected evidence of the investment reconciliations and determined all investment activity was reconciled, reviewed by ARC staff other than the individual who performed the reconciliation, and performed in a timely manner.
5. For a selection of new users granted access to FedInvest, inspected related access approval forms and determined access was appropriately approved and provisioned.
6. For a selection of days, inspected evidence of the daily reconciliation being performed comparing the investment account transactions within FedInvest to the dollar amounts recorded in Oracle and determined that reconciliations were performed, any discrepancies noted during the reconciliation were addressed and staff members other than the individuals who performed the reconciliations reviewed the reconciliations.

No exceptions noted.

Control Objective 14 – Supplier and Bank Records Changes

Controls provide reasonable assurance that changes to Supplier and Bank records are restricted to authorized individuals, and such changes are reviewed, approved, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures related to Supplier and Bank records changes for staff to follow.

Segregation of Duties – Changes to Supplier and Bank Records

User profiles set by Oracle system administrators, as authorized by the user's supervisor or manager, help ensure that only authorized employees are able to make changes to Supplier and Bank records. Authorized employees who have Supplier and Bank record change privileges do not have authorization to approve vendor payments in the accounting system allowing for proper segregation of duties.

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

- A source document from SAM or a document supplied by a vendor or customer, when SAM is not applicable (i.e., grants and loans, payroll database, and/or e-mail, etc.).
- Review by ARC staff other than the individual performing the task.

Review – Changes to Supplier and Bank Records

On a daily basis, a Financial Systems Analyst or an Accountant compares changes to Supplier and Bank records from the Oracle system to the change request documents and electronically signs the audit report indicating review. When it is determined that errors are made, the Financial Systems Analyst or Accountant provides a copy of the source document to a Systems Technician or another Financial Systems Analyst for correction and subsequent review.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Review active supplier reports provided by ARC and request to remove suppliers no longer needed in a timely manner.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for Supplier and Bank record changes and determined that the procedures were formally documented.
2. Inspected a list of Oracle users with role access to update, modify, or delete Supplier and Bank records, inquired of management, and determined users had the appropriate privileges.
3. Inspected a list of Oracle users with role access to process vendor payments and determined users had the appropriate privileges, and that no users with access to process vendor payments had access to update, modify, or delete Supplier and Bank records.

4. For a selection of changes to Supplier and Bank records, inspected the corresponding audit reports signed by the reviewing ARC staff and determined the Supplier and Bank 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 made by an authorized contracting officer who certifies the award is complete, accurate, and meets legal and regulatory requirements.

Description of Controls

The acquisition dollar threshold and type of acquisition determines the supporting documentation that is required to be retained in the acquisition file. The acquisition file documentation is reviewed by a warranted Contracting Officer prior to signing the award document. The Contracting Officer's signature on the award document certifies the award is complete and accurate and that the acquisition files meet legal and regulatory requirements.

The simplified acquisition files above the micro-purchase threshold are required to include a Vendor Matrix and an Award Summary, or all applicable information from the Vendor Matrix and the Award Summary may be combined and included in an Award Recommendation. Acquisitions above the simplified acquisition dollar threshold require an additional document to be completed called a Procurement Checklist.

Tests of Operating Effectiveness and Results of Testing

1. For a selection of acquisitions awarded, inspected evidence and determined that the award was signed by an authorized Contracting Officer to certify that the documents were complete and accurate and met Federal procurement and regulatory requirements.
2. For a selection of acquisitions awarded during the period, inspected evidence that the award had been sign by the Contracting Officer to certify that the documents are accurate and meet legal and regulatory requirements, and that the Contracting Officer who signed the acquisition was within their approval thresholds.

No exceptions noted.

Control Objective 16 – Sufficiently Funded Requisitions

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

Description of Controls

Contracting Officers are warranted by Treasury at specified dollar approval thresholds based on experience and training. The automated contract writing system (PRISM) contains award approval limits for each Contracting Officer at their respective dollar approval threshold prohibiting approval of awards at dollar amounts above their authorized level. PRISM contains configurable controls to prevent procurement awards made without sufficient funding provided by a funding document. Additionally, and in support of the DATA Act, PRISM's control features ensure that applicable awards are reported to the Federal Procurement Data System-Next Generation (FPDS-NG) and subsequently to USA Spending.

Tests of Operating Effectiveness and Results of Testing

1. Inspected award authorizations in PRISM and determined the warranted Contracting Officers were only able to approve awards within their specified dollar limits.
2. Observed an ARC staff member attempt to process a procurement award in PRISM for amount greater than the funding provided and noted the system prevented the award from being made.

No exceptions noted.

HUMAN RESOURCES PROCESSING CONTROLS

Control Objective 17 – Personnel Actions

Controls provide reasonable assurance that personnel actions are authorized, completely and accurately processed, and that any errors are identified and resolved.

Description of Controls[2]

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

ARC uses the Treasury Department's HRConnect as its human resources system for multiple federal agency customers. Its functions include personnel action and payroll document processing. Actions and documents processed in HRConnect interface with the NFC, and NFC ultimately sends payroll data back to ARC for an interface into Oracle.

New Employee Personnel Actions

To process a personnel action for an on-boarding employee, or to process an action for an employee that receives a promotion, reassignment or change to lower grade action through competitive procedures, an ESD Specialist authorizes, via digital PIV signature, a New Hire Checklist, in lieu of an SF-52. The ESD Specialist's digital signature serves as the legal authorization for the personnel action. A PPB HR Assistant then utilizes the New Hire Checklist, and other supporting documentation, to code and release the personnel action in HRConnect. The PPB HR Assistant verifies the action applied in NFC and a different PPB HR Assistant verifies the information in NFC is correct. The PPB HR Assistant also confirms the data in NFC matches the data in HRConnect by reviewing the Mismatch indicator in the employee's record in HRConnect. If the action does not apply or does not apply correctly in NFC, the PPB HR Assistant, along with assistance from the PPB HR Specialist, resolves any issues that stopped the action from applying or applying properly. After NFC's PAYE runs, the PPB HR Assistant who coded the action verifies that the employee was paid accurately, and all applicable deductions were made by verifying the information in PINQ (NFC's Payroll/Personnel Inquiry System). The SF-50 automatically flows via a data feed from NFC to the employee's Electronic Official Personnel Folder (eOPF).

In the event an error is found after PAYE runs, the PPB HR Assistant or PPB HR Specialist will initiate a History Correction Update Package (HCUP) to update erroneous data. The HCUP is reviewed and authorized by a different HR Specialist. After authorization, the HCUP is submitted to NFC. Once the HCUP has applied to the NFC database, the submitter reviews the data to verify accuracy before PAYE runs for that pay period.

Separating Employee Personnel Actions

Employee separations are grouped into five general categories: Resignations, Termination Appointment In (Transfers), other Terminations/Removals (non-Transfers), Retirements, and Deaths. Depending on the category, the personnel action is authorized by EBB, WRB, or PPB:

- For Retirement and Death actions, the supervisor of the retiring or deceased employee typically initiates the HRConnect action upon receipt of a confirmation e-mail from EBB. (Note, however, some customer agencies require that their local HR staff initiate Retirement and Death actions, or the employees initiate their own retirement action.)

---

[2] These controls cover all transactions delegated to ARC for process by customers.

Depending on level of experience, an EBB HR Specialist reviews, codes, and routes the action to PPB. If an EBB HR Specialist's work is still under review, the Specialist routes the action to an EBB Supervisor for review. Once reviewed, the EBB Supervisor forwards the personnel action to PPB.

- Removal and non-transfer Terminations (i.e., termination of probationary/trial employee) actions are submitted in HRConnect by a manager. A WRB ELR Specialist reviews, codes and approves the personnel action, and then forwards the personnel action to PPB. (Note that the ELR Specialist is responsible for coding the nature of action, legal authority, effective date, and remarks related directly to employee relations only; all other remarks are added to the action by PPB.)
- For all other separations, a PPB HR Assistant determines the type of separation and codes the personnel action for review and approval by a PPB HR Specialist.

After a separation is coded and approved, it is reviewed and released from HRConnect by a PPB HR Assistant. The PPB HR Assistant verifies the action applied in NFC and a different PPB HR Assistant verifies the information in NFC is correct. If the action does not apply or apply correctly in NFC, the PPB HR Assistant, along with assistance from the PPB HR Specialist, resolves any issues that stopped the action from applying or applying properly. After PAYE runs, the PPB HR Assistant who coded the action confirms that the employee was paid correctly by verifying the information in PINQ. The SF-50 automatically flows from NFC via a data feed to the employee's eOPF.

Maintenance Employee Personnel Actions

ARC HR processes various other personnel actions for employees, including, but not limited to career-ladder promotions, reassignments, change to lower grade, name changes, etc. from personnel actions submitted by a manager or the employee through HRConnect.

Manager submitted personnel actions are routed through an agency's internal approvals before routing to ARC HR. Depending on the type of personnel action, ARC HR staff in ESD, PPB, or WRB review the information, request any additional information needed, code and authorize the personnel action.

- Suspensions and Return to Duty (RTD)-Suspensions are reviewed, coded and approved by a WRB ELR Specialist. The ELR Specialist then forwards the personnel action to PPB. (Note that the ELR Specialist is responsible for coding the nature of action, legal authority, effective date, and remarks related directly to employee relations only; all other remarks would be added to the action by PPB.)
- Leave Without Pay (LWOP) and RTD actions related to a workers' compensation claim are reviewed, coded and approved by a WRB Workers' Compensation Specialist. The Specialist then forwards the personnel action to PPB. (Note that the Workers' Compensation Specialist is responsible for coding the nature of action, legal authority, effective date, and remarks related directly to employee relations only; all other remarks would be added to the action by PPB.)
- All personnel actions related to Pathways employees are reviewed and coded by a PPB HR Assistant. The PPB HR Assistant forwards the personnel action to an ESD Specialist for review and approval.
- All reorganizations are reviewed and coded by a PPB HR Specialist. The PPB HR Specialist forwards the personnel action to an ESD Specialist for review and approval.
- All other actions are reviewed and coded by a PPB HR Assistant. The PPB HR Assistant forwards the personnel action to an authorizing official, depending on the type of action, for review and approval.

After the personnel action is coded and approved, it is released from HRConnect by a PPB HR Assistant. The PPB HR Assistant verifies the action applied in NFC and a different PPB HR Assistant verifies the information in NFC is correct. If the action does not apply or apply correctly in NFC, the PPB HR Assistant, along with assistance from the PPB HR Specialist, resolves any issues that stopped the action from applying or applying properly. After PAYE runs, the PPB HR Assistant who coded the action confirms that the employee was paid correctly by verifying the information in PINQ.

Employee submitted personnel actions (such as name changes) bypass the customer agency review process and route directly to ARC HR. A PPB HR Assistant reviews the information, requests any additional information needed, and codes the personnel action. The PPB HR Assistant releases the action in HRConnect. The PPB HR Assistant verifies the action applied in NFC and a different PPB HR Assistant verifies the information in NFC is correct. If the action does not apply or apply correctly in NFC, the PPB HR Assistant, along with assistance from the PPB HR Specialist, resolves any issues that stopped the action from applying or applying properly. After PAYE runs, the PPB HR Assistant who coded the action confirms that the employee was paid correctly by verifying the information in PINQ.

Awards are routed through an agency's internal approvals before routing to ARC HR. No additional reviews or approvals are done by ARC HR. The PPB HR Assistant releases the action in HRConnect.

Federal Employees' Group Life Insurance (FEGLI)

All FEGLI elections are initiated via an SF-2817, Life Insurance Election form. An EBB HR Assistant (an EBB HR Specialist if the employee is a reemployed annuitant) verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. The EBB HR Assistant then manually inputs the form into HRConnect and verifies the change applied in NFC. A second EBB HR Assistant also verifies the document applied in NFC and that the information in NFC is correct. If a FEGLI election results from a qualifying life event, an EBB HR Assistant requests documentation to verify the employee's eligibility.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Ensure all personnel actions are submitted in HRConnect timely.
- Notify ARC timely regarding separating employees.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written policies and procedures for processing personnel actions and determined that the policies and procedures were formally documented.
2. For a selection of new employee personnel actions in HRConnect, inspected relevant documentation and determined that new employee personnel actions were documented, completed, authorized, and correctly applied.
3. Compared the Fiscal Service HR separation listing and the ARC HRConnect active employee listing and determined that there were no separated employees who retained access to HRConnect.

4. For a selection of separating employee personnel actions in HRConnect, inspected separation request documentation and determined the requested actions were reviewed and approved and carried out by the appropriate personnel.
5. For a selection of maintenance employee personnel action requests, for a selection of customer agencies, inspected documentation and determined that the requests were reviewed, approved, and correctly applied by the appropriate personnel.
6. For a selection of FEGLI elections, inspected the related Life Insurance Election forms and determined that eligibility was verified and certified by an EBB Specialist, and the action was correctly applied.

No exceptions noted.

Control Objective 18 – Payroll Documents

Controls provide reasonable assurance that payroll documents are completely and accurately processed, and that any errors are identified and resolved.

Description of Controls[3]

ARC has documented procedures for staff to follow for the processing of payroll documents that have been delegated to them by customers.

ARC uses the Treasury Department's HRConnect as its human resources system for multiple federal agency customers. Its functions include personnel action and payroll document processing. Actions and documents processed in HRConnect interface with the NFC, and NFC ultimately sends payroll data back to ARC for an interface into Oracle.

Payroll documents include direct deposit information for net pay and allotments, federal and state withholding, union dues, health insurance elections, TSP elections and lump sum payments for annual leave and compensatory time.

Employees are required to input changes to tax withholdings, health insurance, TSP contribution percentages, direct deposit and addresses using NFC's Employee Personal Page self-service option, whenever possible. Changes entered in this manner are processed automatically, bypassing ARC HR.

Federal Employees Health Benefits (FEHB) and TSP Contributions

FEHB and TSP elections (TSP catch-up contributions are also included in TSP elections) are employee-initiated via the appropriate form. An EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. The EBB HR Assistant then manually inputs the form into HRConnect and verifies the change applied in NFC. A second EBB HR Assistant also verifies the document applied in NFC and that the information in NFC is correct.

Lump Sum Payments for Unused Annual Leave and Compensatory Time

Employees receive payment for unused annual leave and compensatory time when they meet any of the following criteria:

- Separation from Federal service.
- Transfer to a Public International Organization.
- Military reservists who are activated to military duty and elect to receive a lump sum payment for annual leave, or have a balance of restored annual leave or compensatory time.
- Employee's compensatory time balance expired, depending on the employee's FLSA status and the agency's policy for paying FLSA Exempt employees.
- Employee converted to a senior level position, depending on the employee's FLSA status and the agency's policy for paying FLSA Exempt employees.

A PPB HR Specialist enters and releases the payroll document in HRConnect. After PAYE runs, the PPB HR Specialist verifies that the employee was paid for the hours.

---

[3] These controls cover all transactions delegated to ARC for process by customers.

<u>Payroll Documents</u>

Most changes in payroll information are completed by the employee using the self-service option in NFC's EPP. If the action does not apply in NFC due to an error, the submission will be present on a Suspense Inquiry System (SINQ) report. The report is monitored each pay period by PPB and EBB staff, as applicable. Each error is reviewed and resolved prior to PAYE running for the pay period.

In rare cases, employees submit requests for changes and/or deductions in writing to PPB. A PPB Contact Center Assistant reviews the request and contacts the employee if more information or additional verification is needed. The PPB Contact Center Assistant inputs and releases the request in HRConnect. The PPB Contact Center Assistant verifies the action applied in NFC and a different PPB Contact Center Assistant verifies the information in NFC is correct. After PAYE runs, the PPB Contact Center Assistant confirms that the employee was paid correctly by verifying the information in PINQ.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written policies and procedures for the processing of payroll documents and determined that procedures were formally documented.
2. For a selection of elections for FEHB, TSP, and TSP Catch-up Contributions for a selection of customer agencies, inspected the appropriate forms and determined the forms were verified and certified by an EBB Specialist, and the election was correctly applied.
3. For a selection of employees who received payment for unused annual leave or compensatory time for a selection of customer agencies, inspected relevant documentation and determined that approvals were obtained, criteria was met, and the employee was appropriately paid.
4. For a selection of written employee requests for payroll changes and/or deductions submitted to PPB, for a selection of customer agencies, inspected relevant documentation and determined the request was verified, and correctly applied.

No exceptions noted.

GENERAL COMPUTER CONTROLS

Control Objective 19 – 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 Fiscal Service 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, OBI, Discoverer, PRISM, webTA, ConcurGov, moveLINQ, IPP, OneStream, HRConnect, and Robotic Process Automation (RPA) have been documented. The logical access controls are based on Treasury and Fiscal Service 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, OBI and Discoverer

Access to Oracle, OBI and Discoverer are restricted to users with a valid logon identification (ID) and password. Oracle, OBI and Discoverer logons/sessions are encrypted to protect the information, making it unintelligible to all but the intended users. Sessions are protected using 128-bit or higher TLS encryption. Prospective Oracle, OBI and Discoverer 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 Fiscal Service and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in Oracle OBI, and/or Discoverer. 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 access is end-dated in the system to remove their access within 48 hours. Oracle end user's access is monitored and end dated after 90 days of inactivity by an RPA. System administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. Annually, the ARC generates a report listing system users for each customer agency for review. The Service Desk Branch updates the permissions for users based on the responses received from the customer agencies.

With Oracle R12, responsibilities are assigned to specific Multi-Org Access Control (MOAC) groups, in which case, the MOAC group determines which data can be accessed by users. Data entry is also restricted, allowing only values within the MOAC group to be selected for transaction processing. A MOAC group can be comprised of one operating unit (ledger) or multiple ones.

Only the SYSADMIN account controlled by Oracle Managed Cloud Services is assigned the System Administrator responsibility in the Oracle application. The OSD and PSB1 staff are assigned ARC Application Administrator responsibility in the Oracle application. The employees with the ARC Application 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 ARC Application 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 ARC Application Administrator from adding or removing any responsibilities from their own user ID.

The SDB/OSB/DSB managers can be assigned the ARC Application 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.

Administrative access to the underlying Oracle servers and databases is limited to Oracle Managed Cloud Services server and database administrators.

User IDs are assigned to internal and external users 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/OBI/Discoverer user's password must meet unique password configuration, password complexity and password expiration criteria to ensure strong password security.

Oracle/OBI/Discoverer access attempt logs are reviewed daily by the Service Desk Branch to identify if users attempted to unsuccessfully access the system five or more times in the day (15 or more times for group user accounts). When the maximum unsuccessful access attempts are 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. An RPA reviews the log and sends the e-mails out to the users.

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 or higher TLS 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 Fiscal Service 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 Oracle 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 access is end-dated in the system to remove their access. Oracle end user's access is monitored and end dated after 90 days of inactivity by an RPA. System administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. Annually, the ARC generates an OBI or Discoverer report listing users for each customer agency for review. Included for review are requisitioner and buyer approval limits by user. The Service Desk Branch 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

Control Objectives, Related Controls, and
Tests of Operating Effectiveness

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 SDB. The changes to functional access privileges are reviewed and compared to the changes to the OSD'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 OSD'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 Oracle Managed Cloud Services server and database administrators and specific OSD/SPSD employees.

User IDs for both internal and external users 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 Service Desk Branch to identify if users attempted to unsuccessfully access the system five or more times in the day (15 or more times for group user accounts). When the maximum unsuccessful access attempts are 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. An RPA reviews the log and sends the e-mails out to the users.

webTA[4]

Access to webTA is restricted to users with a valid logon ID and password or Single Sign On authentication. Access to webTA is provided using 128-bit or higher TLS 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; they are given access upon receipt of a personnel action. A PPB HR Administrator creates the user's profile based on information in the personnel action and assigns a user ID. An initial temporary password is provided to the new users by their timekeepers, by following the self-service password reset on the webTA login page, or by the user contacting the HR Systems Help Desk. 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.

Users that require elevated access (e.g., timekeeper, supervisor) are given that level of access 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 elevated access require a new access form to be submitted by the customer agency.

---

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

Upon receipt of an Administrative Resource Center System Access Form for End User Applications requesting the deletion of a webTA user, e-mail request from a supervisor or the customer agency's HR office, or a personnel action documenting a separated employee in HRConnect, an HR Administrator in the HR Systems Help Desk removes any elevated access. Upon receipt of a personnel action documenting a separated employee in HRConnect, an HR Administrator in PPB codes the exiting employee's timecard as "Final" and deactivates the employee's webTA access.

Annually, an HR Administrator sends out a list of timekeepers and supervisors to each customer agency for the agency to use in performing an annual 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). 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 ISS.

ConcurGov

Access to ConcurGov is restricted to users with a valid logon ID and password or Single Sign On authentication. All users must complete the registration process. After verifying that the traveler is not already in ConcurGov or set up in Oracle, TSD sends traveler a "ConcurGov New User Registration Worksheet" and "Direct Deposit Form" to complete and return via e-mail or fax. Budget Reviewers and Approving Officials must complete, sign, and submit an approved *ARC System Access Form* 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 Fiscal Service and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in ConcurGov. Changes to a user's identification (i.e., name change) or to the user's role in ConcurGov requires an *ARC System Access Form* to be resubmitted or an e-mail from the user copying his/her approving official or agency travel contact. An e-mail is forwarded to the user by the TSD helpdesk after the registration information is verified instructing the user to call the TSD helpdesk to activate their account. Users must establish their own unique ConcurGov password. A user's password must meet unique password configuration, password complexity, and password expiration criteria to ensure strong password security. Access privileges are granted in accordance with the concept of least privilege required.

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

- Federal Auditor – Invitational Travelers/Auditors and/or Exited Travelers (FA Role)
- Admin Level 5 – Customer Service Help Desk Tier 1, Designated TDSB staff (FATA 5)
- Admin Level 6 – Application Administrators; Customer Service Help Desk Tier 2, Designated TDSB staff (FATA 6)
- Admin Level 7 – Application Administrators; Customer Service Help Desk Tier 2, Designated TDSB staff (FATA 7)

Control Objectives, Related Controls, and Tests of Operating Effectiveness

- Admin Level 8 – Application Administrators; Designated TDSB staff (FATA 8)
- System Administrators (SAP Concur staff only) (FATA 9)
- Auto Approve (FSTA Role)
- Federal Supervisory Travel Approver (FSTA Role)
- No OBE (FSTA Role)
- No OBE Auto Approve (FSTA Role)
- Auto Approve - TGT, partial CFP, FHF, MCS, OSH (FT Role)
- Federal Traveler - All other Agencies (FT Role)
- No OBE- ADF, OTA, CSB (FT Role)
- No OBE Auto Approve (FT Role)
- Report User – Designated TDSB staff and users (e.g., customer travel contacts) given report access
- Technical (SAP Concur Use Only)

Upon TSD's receipt of an Exit Clearance form or e-mail request, a termination date is entered in the user's profile and ConcurGov access is terminated. On an annual basis, TSD staff creates reports of ConcurGov users and distributes the reports to customer agency Travel contacts for review and verification of the accounts.

moveLINQ

Access to the moveLINQ system is granted through three portals:

- The Employee Portal can be accessed from the internet by newly hired, currently employed and retired Federal Government employees of Treasury and Non-Treasury Federal customers.
  - New user accounts are created with the receipt of a "Request for Relocation" provided by the Customer Agency Contact. Access is removed once all relocation records have been deleted from the system.
  - Access is granted through the Fiscal Service Single Sign On (SSO) system.
    - This screen will accept
      - PIV/PIN
      - SecurID
      - ITIM UserID and Password.
    - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
    - The SSO system provides three records of identity, if those match what is in moveLINQ for the account user and if they have been configured for Employee portal access.
    - They will be able to see their own records ONLY as configured in their access account, once the documents have had workflow started.
    - Employee portal users do not have the roles with permissions or functions tied to them.
    - They can only apply their assigned status stamp to documents that have been electronically routed to them.

- The Agency Contact (aka Approval Portal users) can only be accessed by customer agency users while on white listed federal government networks either through direct connection or VPN.
  - New/modified/disabled user accounts are processed with the receipt of a "moveLINQ System Access Form" that has been signed by the customer user

acknowledging acceptance of the requirements to use the system. The document also has to be signed by the customer agency approving official, the moveLINQ Admin that added the user and the reviewing moveLINQ admin.
- o Access is granted through the Fiscal Service Single Sign On (SSO) system.
  - This screen will accept PIV/PIN only.
  - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
  - The SSO system provides three records of identity, if those match what is in moveLINQ for the account user and if they have been configured for Approval portal access, they will be able to see records that have been shared with them either through Organization access or through assigned workflow access.
  - They will only be able to view their assigned customer agency records that have been shared with them after workflow has been started.
  - Approval portal users do not have the roles with permissions or functions tied to them.
  - They can only apply their assigned status stamp to documents that have been electronically routed to them.

- The Expense Management Portal can only be accessed by Fiscal Service Employees either connected directly to the Fiscal Service network (wired or wireless on-premises) or through Fiscal Service VPN connection. .
  - o New/modified/disabled user accounts are processed with the receipt of a "moveLINQ System Access Form" that has been signed by the user acknowledging acceptance of the requirements to use the system. The document also has to be signed by a supervisor, the moveLINQ Admin that added the user, and the reviewing moveLINQ ISSO or SO.
  - o Access is granted through the Fiscal Service Single Sign On (SSO) system.
    - This screen will accept PIV/PIN only.
    - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
    - The SSO system provides three records of identity, if those match what is in moveLINQ for the account user and if they have been configured for Expense Management portal access, they will be able to see records that have been shared with them through Organization access.
    - Expense Management Users have roles with permissions assigned to them.
      - These user roles/permissions are granted based on the principle of separation of duties through assigned access authorizations and the least privilege principle.
  - o The following roles are configured within the moveLINQ system (sorted alphabetically):
    - Admin
    - Intern
    - Mgmt1
    - None
    - RC
    - RC_Tech
    - Specialist
    - Tax_Prep
    - Tech

Control Objectives, Related Controls, and Tests of Operating Effectiveness

- Viewer
- VIP Reviewer
- VIP_Accounting
- VIP_Accounting_SP

See Control Objective 21 for further discussion of the physical access control process.

<u>Invoice Processing Platform</u>

Access to IPP is restricted to users with a valid logon ID and password or SSO authentication. Internal and external users must complete, sign, and submit an approved *Administrative Resource Center Online Applications Access Request form*. Customer agency users must submit a Certificate of Completion for the On-line Invoice Approver Training located on their ARC customer webpage, unless they are on the list of attendees that completed the training given during their customer conversion to IPP. 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 Fiscal Service and ARC. The form defines the user's access specifications, which allow the user to perform his/her duties in IPP. The user receive an e-mail with a user id and one containing a temporary password from the Treasury UPS User Administration. Annually, FRB St. Louis sends a list of all IPP users in the Fiscal Service Admin Disburser Account for recertification. ARC reaches out to the customer agency IPP contact and returns the results to FRB St. Louis. In order to remove a user's IPP access, customer agencies submit a request for account termination. At that time, the IPP user's access is disabled in the system.

The IPP Fiscal Service Admin Disburser Account has user access levels that separate permissions into these categories from highest to lowest:

- Administrator:
  - Administrator
  - Administrator II
- Approver:
  - Approver
  - Approver CEA
  - Approver CEQ
  - Approver NSC
  - Approver OAS
  - Approver OMB
  - Approver OND
  - Approver OST
  - Approver OVP
  - Approver RVP
  - Approver SPE
  - Approver UST
  - Approver WHO
- Processor
- Viewer:
  - Viewer
  - APB Viewer
  - ARC Viewer
  - Customer Viewer

- Customer Report Viewer
- Viewer CEA
- Viewer CEQ
- Viewer NSC
- Viewer OAS
- Viewer OMB
- Viewer OND
- Viewer OST
- Viewer OVP
- Viewer RVP
- Viewer SPE
- Viewer UST
- Viewer WHO

Access is restricted in accordance with the concept of least privilege required.

Users must establish their own unique IPP password. A user's password must meet unique password configuration, password complexity and password expiration criteria to help ensure strong password security that follow the configuration requirements established by Fiscal Service IBM Security Identity Manager (ISIM).

OneStream

Access to OneStream is restricted to users with a valid logon ID and password. Prospective OneStream users must complete, sign, and submit an approved *Administrative Resource Center System Access Form for End User Application* to request access to OneStream. 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 Fiscal Service and ARC. The form defines the user's access specifications, which will allow the user to perform his/her duties in OneStream. Changes to existing user profiles require an e-mail to be sent to the Oracle 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 OneStream user access is end-dated in the system to remove their access. Annually, ARC generates a report listing system users for each customer agency for review as part of the annual recertification process. The Oracle Support Team updates the permissions for users based on the responses received from the customer agencies.

OneStream access is restricted using a series of cube views, roles, and workflows. User access is restricted based off the cube (cubes limit users' access to a specific customer's data) and roles assigned.

The System Administrator responsibility in OneStream is limited to certain OSD/SPSD employees requiring the access for the performance of job duties. Administrator duties include user setup and cube/role/workflow creation and assignment.

User IDs for OneStream are assigned by an ARC application 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 prior to establishing the user's password. Once the user logs into 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.

OneStream access attempt logs are reviewed daily by the Service Desk Branch to identify if users attempted to unsuccessfully access the system five or more times in the day. When five or more unsuccessful access attempts are 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.

HRConnect

Access to HRConnect is restricted to users with a valid login ID and password or Single Sign On authentication. All employees have access to their personnel data in HRConnect. Access forms are not required for standard employee, supervisor or proxy access. Employees are given access after processing of a personnel action and following the self-service registration on the HRConnect logon page. Supervisor access is automatically granted upon processing of a personnel action placing the employee in a supervisory position. Users that require elevated access (e.g., Admin, HR and PDS roles) are given that level of access following receipt of an *Administrative Resource Center System Access Form for End User Application* signed by the agency's authorized approver. 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 HRConnect. Changes to existing elevated access require a new access form to be submitted by the customer agency.

An employee's roles are automatically removed from HRConnect when he/she separates from the agency. Upon receipt of an *Administrative Resource Center System Access Form for End User Application* requesting removal of a user's HRConnect roles or e-mail request from the agency, the HR Systems Help Desk removes any elevated access from existing users.

Annually, an Analyst on the HR Systems Help Desk sends out a list of users with roles other than employee, manager, or proxy to each customer agency for the agency to use in performing an annual review of access. The HR Systems Help Desk updates the permissions for users based on the responses received from the customer agencies. Semiannually, an analyst on the HR Systems Help Desk performs a similar additional review for users with administrative roles.

Robotic Process Automation

Access to the Robotic Process Automation (RPA) is restricted to users that have the software installed on their PCs and that have access to a valid license key. A Service Request must be submitted within the Hewlett Packard Service Manager (HPSM) to initiate the installation of the RPA software and it must be approved by management within the Operations Support Division. Information Security Services (ISS) is responsible for installing the software for individual users. Additionally, a valid license key must be entered by each user in order to access the software. Service requests are entered to grant users access to the RPAdmin Active Directory (AD) group, which grants access to the restricted shared network drive location where the license keys necessary to access the RPAs are stored. Access to AD groups are reviewed annually.

Access and roles for the Production region of the KOFAX Management Console is restricted via Lightweight Directory Access Protocol (LDAP) groups. A Service Request must be submitted within HPSM to initiate adding a user to the applicable LDAP group, which must be approved by management within the Operations Support Division. Access to the needed LDAP groups is granted by ISS with an approved Service Request. In production, the administrative role is given to

authorized non-developers. This role allows users to upload RPAs, create schedules for RPAs, and execute RPA runs. This role also allows for configuration changes. Authorized developer users within the Digital Workforce Support Team (DWST) are granted a similar role in production, which is a view only role that does not allow for the upload, scheduling/execution of RPAs, or configuration changes.

Complementary Customer Agency Controls

Customer agencies should establish controls to:

- Review and approve listings of users with current Oracle, PRISM, webTA, ConcurGov, IPP, OneStream, and HRConnect access to ensure appropriateness and provide changes to ARC in a timely manner.
- Timely notify ARC regarding exiting employees.
- Notify ARC timely of any changes to HRConnect authorized approvers.
- Ensure all personnel actions are submitted in HRConnect timely.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for system access provisioning for Oracle, Discoverer/OBI, PRISM, webTA, ConcurGov, IPP, moveLINQ, OneStream, and HRConnect and determined procedures were documented.
2. Inspected both the Oracle user account management procedures and password procedures and determined the security policies and procedures were documented for Oracle.
3. Inspected both the PRISM user account management procedures and password procedures and determined the security policies and procedures were documented for PRISM.
4. Inspected both the webTA user account management procedures and password procedures and determined the security policies and procedures were documented for webTA.
5. Inspected both the ConcurGov user account management procedures and password procedures and determined the security policies and procedures were documented for ConcurGov.
6. Inspected both the moveLINQ user account management procedures and password procedures and determined the security policies and procedures were documented for moveLINQ.
7. Inspected both the IPP user account management procedures and password procedures and determined the security policies and procedures were documented for IPP.
8. Inspected both the Discoverer/OBI user account management procedures and password procedures and determined the security policies and procedures were documented for Discoverer/OBI.
9. Inspected the HRConnect user account management procedures and determined the security policies and procedures were documented for HRConnect.
10. Observed an Oracle logon session and noted Oracle users were required to have a valid login ID and password, and logins/sessions were encrypted with 256-bit TLS encryption.
11. For a selection of new Oracle users, inspected user access request forms and determined the forms were completed, access was authorized, and employees acknowledged that they understand the Privacy Act requirements.
12. For a selection of changes to Oracle user profiles, inspected authorizing documentation and determined updates to access rights were authorized.
13. Inspected a selection of requests for the termination of customer agency employees' Oracle access including evidence of when the accounts were end dated in Oracle and determined that the terminations of access were completed in a timely manner.
14. Inspected a selection of employee termination requests from customer agencies and an active Oracle user listing and determined that none of the terminated employees retained access to Oracle.

Control Objectives, Related Controls, and
Tests of Operating Effectiveness

15. Inspected the Fiscal Service HR separation listing and the Oracle user listing and determined no separated employees retained access to Oracle.
16. For a selection of days, inspected the daily Oracle inactivity reports and determined that the reports were reviewed, warning e-mails were sent to inactive users, and accounts inactive for more than 90 days were removed.
17. For a selection of end user account reviews for a selection of customer agencies, inspected evidence of the annual Oracle user access review and determined the lists were provided to customer agencies for review and changes provided by the customer agencies were applied.
18. Inspected a listing of user accounts and corresponding access privileges in Oracle and determined each user's access was restricted to distinct operating units or customer agency.
19. Inspected the user roles assigned to Oracle Application administrators and compared them to the BTD Allowable Responsibilities Table and determined the functional user permissions were restricted and commensurate with job responsibilities.
20. Observed an Oracle Application administrator attempt to add responsibilities to their user ID and determined the application automatically blocked the attempt to add responsibilities to their own user ID.
21. For a selection of occurrences, inspected documentation authorizing the use of temporary Admin Access and determined the access occurrences were documented, approved, and revoked when no longer needed.
22. Inspected the Oracle hosting contract and determined it stated access to the supporting operating system and database administrative accounts are limited to Oracle staff.
23. Inspected a listing of Oracle user accounts and determined accounts followed the naming convention.
24. Inspected Oracle profile options and ARC password standards and determined failed logins, password complexity, aging, generation, and length requirements were configured in accordance with the ARC password standards.
25. For a selection of Oracle application administrators and users, observed the password lifespan days established for the individual users and noted determined the observed settings were configured in accordance with the ARC password standards.
26. Inspected Oracle profile options and determined Oracle was configured to disconnect inactive sessions after 15 minutes.
27. For a selection of dates, inspected the Oracle violation logs and determined the violations logs were reviewed and potentially unauthorized activity was followed up.
28. Observed a PRISM logon session and noted user ID and passwords were required and PRISM logins/sessions were encrypted with 256-bit TLS encryption.
29. For a selection of new PRISM users, inspected user access request forms and determined the forms were completed and access was authorized.
30. For a selection of changes to PRISM user accounts, inspected authorizing documentation and determined updates to the accounts were authorized.
31. Inspected a selection of requests for the termination of customer agency employee's PRISM access and evidence of when the account was end dated in PRISM and determined requests for termination of access were completed in a timely manner.
32. For a selection of employee termination requests made from customer agencies, inspected the PRISM user listing determined that the employee did not retain access to PRISM after their termination date.
33. Inspected the Fiscal Service HR Separation listing and the PRISM user listing and determined no separated ARC employees retained access to PRISM.
34. For a selection of days, inspected the daily PRISM inactivity reports and determined that the reports were reviewed, warning e-mails were sent to inactive users, and accounts inactive for more than 90 days were removed.

35. For a selection of customer agencies, inspected evidence and determined that user lists were provided to customer agencies for review and access changes provided by the customer agencies were applied.
36. Observed the production PRISM system for a user and noted the system can be configured as defined in the New User Setup Policy and Procedure.
37. Inspected a selection of changes to PRISM functional access privileges and determined changes were reviewed and compared to the BTD's Team Responsibilities matrix, and were deemed appropriate.
38. Observed a PRISM Support Team member create a new account in PRISM and noted that upon first login, the user was immediately directed to reset their password.
39. Inspected a listing of PRISM user accounts and determined the accounts followed the naming convention.
40. Inspected PRISM configuration settings and determined PRISM logon/sessions were configured to time-out after 20 minutes of inactivity.
41. Inspected the PRISM password settings and determined failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.
42. For a selection of dates, inspected the PRISM violation logs and evidence of review and determined the violations logs were reviewed and violations were followed up.
43. Observed a user log into webTA and noted the connection to webTA was encrypted utilizing 128-bit TLS encryption.
44. Observed a webTA logon session and noted logins/sessions required a valid user name and password.
45. For a selection of changes to webTA users with elevated privileges, inspected user access request forms and determined the forms were completed and access was authorized.
46. Inspected a selection of webTA End User Application access removal requests and evidence of access removal and determined HR Administrators from the HR Systems Help Desk removed any elevated access.
47. Inspected the Fiscal Service HR separation listing with the webTA user listing and determined no separated employees retained access to webTA.
48. For a selection of customer agencies, inspected evidence of the annual user access review and determined that webTA user access lists were distributed to customer agencies for review and access changes identified by customer agencies were applied.
49. Inspected the Fiscal Service user privileges within webTA and determined users assigned the HR Administrator role were not also assigned the System Administrator role.
50. Inspected the Fiscal Service user privileges within webTA and determined users were assigned a role based on security configurations.
51. Inspected a listing of webTA user accounts with administrative access to the underlying webTA servers and databases and determined administrative access was limited to server and database administrators within ISS.
52. Observed a user logging into webTA for the first time and noted webTA automatically required users to create a new password after initial login.
53. Inspected the webTA password settings and determined failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.
54. Inspected webTA configuration settings and determined webTA sessions were configured to time-out if they remained inactive for 10 minutes.
55. Observed a user access the ConcurGov system and noted users needed to be authenticated prior to accessing the system.
56. For a selection of new ConcurGov users, inspected user access request forms or e-mails and determined the forms or e-mails were completed and access was authorized prior to being granted.

57. For a selection of changes to ConcurGov users, inspected the authorizing documentation and determined access changes were documented and authorized.
58. Inspected a selection of ConcurGov access removal requests and determined an Exit Clearance form or e-mail request was sent to note the user's access in ConcurGov was terminated.
59. For a selection of employee termination requests made from customer agencies, determined the employee did not retain access to ConcurGov after their termination date upon inspection of the ConcurGov user listing.
60. Inspected the Fiscal Service HR separation listing and ConcurGov user listing and determined separated employees did not retain access to ConcurGov.
61. For a selection of user reports distributed to customer agency Travel contacts for a selection of customer agencies, inspected evidence and determined each customer agency completed an annual user access review/verification and changes provided by the customer agencies were applied.
62. Inspected access levels within ConcurGov and determined access levels separated permissions from highest (admin) to lowest (report user).
63. Observed a user attempting to change their ConcurGov password using invalid settings and determined the system automatically prevented the use of passwords that did not meet the password configuration, complexity, and expiration requirements.
64. Observed a moveLINQ user login to the web based system and noted the system required the user to enter either a valid user ID and password, SecurID, or PIV/PIN.
65. Inspected documentation for a selection of added moveLINQ users and determined the requests were documented and approved.
66. Inspected a selection of moveLINQ termination requests and determined the removal of access was documented and performed, and compared the Fiscal Service HR separation listing with the moveLINQ user listing and determined there were no separated employees that retained access to moveLINQ.
67. Observed an Approval Portal user login to the moveLINQ and determined that they are required to authenticate either via PIV/PIN, that three records of identify are configured to match in SSO and moveLINQ, the user can only view their assigned customer agency records or apply their status stamp to documents routed to them, and the user does not have roles with assigned permissions or functions tied to them.
68. Inspected documentation for a selection of added moveLINQ users and determined the requests were documented and approved.
69. Observed a user login to the web based system expense management portal and noted that they are required to authenticate via PIV/PIN only and that three records of identify are configured to match in SSO and moveLINQ to allow access.
70. Inspected documented for a selection of added moveLINQ users and determined the requests were documented and approved.
71. Inspected access levels within moveLINQ and determined access levels separate permissions from highest to lowest.
72. Observed an IPP user login to the web based system and noted the system required the user to enter a valid user ID and password.
73. For a selection of customer agencies, inspected the annual account recertification supporting documentation and determined ARC contacted customer agencies and the results were returned to Federal Reserve Bank (FRB) St. Louis.
74. For a selection of new IPP accounts, inspected documentation and determined access requests were documented and approved prior to granting access.
75. Inspected the Fiscal Service HR separation listing and the IPP user listing and determined no separated employees retained access to IPP.
76. Observed a user attempt to change their IPP password using invalid settings and determined the system automatically prevented the use of passwords that do not meet the password configuration, complexity, and expiration requirements.

77. Inspected access levels within IPP and determined access levels separated permissions from highest (Administrator) to lowest (Viewer).
78. Observed an OneStream user login to the web based system and noted the system required the user to enter a valid user ID and password.
79. For a selection of new OneStream users, inspected corresponding user access request forms and determined the requests were documented and approved.
80. Inspected the Fiscal Service HR separation listing and the OneStream user listing and determined no separated employees retained access to OneStream.
81. For a selection of employee termination requests, inspected documentation and determined the employee did not retain access to OneStream after their termination date.
82. Inspected access levels within OneStream and determined access levels were restricted by cubes and workflows.
83. Inspected the listing of OneStream Administrators and the Fiscal Service personnel listing and determined that all administrators were OSD/SPSD employees.
84. Observed the password complexity configuration settings and determined that the system required strong passwords in accordance with ARC password standards.
85. For a selection of dates, inspected OneStream violation logs and determined the violation logs were reviewed and violations were followed up.
86. For a selection of customer agencies, inspected the annual account recertification supporting documentation and determined ARC contacted customer agencies and made related changes to access permissions in OneStream as necessary, based on their response.
87. For a selection of new or modified access changes to HRConnect users with elevated privileges, inspected user access request forms and determined they were completed and authorized.
88. Inspected a selection of HRConnect End User Application access removal requests and determined personnel in the HR systems Help Desk removed elevated privileges upon user separation.
89. Inspected the Fiscal Service HR separation listing and the HRConnect user listing and determined there were no separated employees who retained access to HRConnect.
90. For a selection of HRConnect user reports for a selection of customer agencies, inspected evidence of HRConnect User reports distributed to customer agencies and determined each customer agency was notified to complete an annual user access review, and ARC made the customer agency requested account changes where applicable.
91. Observed a user access HRConnect and determined that access was restricted to users with a valid login ID and password or Single Sign On with a valid PIV card.
92. For a selection of new RPAs implemented into production, inspected related security documentation and determined approval was obtained by the ISSO or System Owner of the application in which the RPA required access.
93. For a selection of new KOFAX user accounts, inspected documentation and determined access was approved.
94. Inspected recertification evidence for the RPA Active Directory group, and determined that users access was reviewed and any corrective actions noted were taken.

No exceptions noted.

Control Objective 20 – System Changes

Controls provide reasonable assurance that 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. ARC System Administrators are facilitators of the formal change management process via My Oracle Support, Oracle Managed Cloud Services' web-based service request system.

Oracle, OBI, Discoverer and PRISM

For Oracle, OBI, Discoverer and PRISM, ARC uses HPSM and My Oracle Support 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 Oracle, OBI, Discoverer and PRISM. Additionally, ARC processes customized application extension changes to Oracle. The ability to process and apply Oracle, OBI, Discoverer and PRISM changes is restricted to the database administrators under the coordination of Oracle Managed Cloud Services. Access to My Oracle support is monitored and reviewed biannually.

ARC Application 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. DSB staff develop customizations in separate development instances. OSB staff test changes by running test scripts and analyzing the results. Upon successful completion of testing, OSB staff approve the change request and forward it to the performer of the change, Oracle Managed Cloud Services database administrators. After the approved request has been completed, the performer updates the request in My Oracle Support accordingly, and the request is then closed.

For emergency changes to a production instance of Oracle, OBI, Discoverer or PRISM, ARC requires verbal approval from a designated on-call manager (for all production instances). ARC Application Administrators document the emergency change in My Oracle Support 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), ARC OSB and HROD 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 OSB staff forward a request for applying the new webTA release to production to HROD for approval. The ability to apply webTA releases is restricted to the database and application administrators under the authority of ISS. The new webTA release is not applied to production until it has been successfully tested and approved.

ConcurGov

ConcurGov is hosted and maintained by SAP Concur at their facility. The ETS vendor 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 the ETS vendors for changes to be included by the vendors in future scheduled release updates. TSD Analysts test all applicable ConcurGov changes in a ConcurGov acceptance test environment. If any of the changes included in a scheduled ConcurGov release update fail TSD's acceptance testing, the vendor may delay implementation of the release update. TSD has documented procedures for testing ConcurGov changes. Guidance is provided to customer agency contacts on any changes.

moveLINQ

moveLINQ is hosted by ISS and maintained at Fiscal Service. 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 and users test all moveLINQ changes in moveLINQ test environments. If any of the changes included in a scheduled moveLINQ release update fail the 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 Fiscal Service's HPSM to track changes to the system.

Invoice Processing Platform

IPP is a web-based system hosted by the FRB St. Louis. FRB St. Louis notifies all primary agency users in advance of any new IPP release and holds review/preview meetings to discuss all known changes as well as potential changes for the next release. During the "preview" section of the meeting, agencies can rank the proposed changes for the next release. In addition, FRB St. Louis publishes testing schedules and provides the agencies an opportunity to test the changes in a QA environment prior to deploying the code into IPP Production.

OneStream

OneStream is hosted and maintained within a non-public facing, private cloud environment. Updates and new system releases are provided on a six-month (semi-annual) basis and OneStream notifies ARC of these changes via e-mailed releases. Testing and application of system changes is a combined effort on the part of OSD, SPSD and ARAD. Functional testing is performed by ARAD to determine that the functional requirements are met, while OSD and SPSD performs security compliance testing, including testing of system and user access and role security. If testing from either the system administration or the functional requirements are not met, ARC may delay the implementation of the release until defects are addressed by the vendor. Existing test plans are available and updated periodically per release to match new releases and functionality on an ongoing basis. Guidance is provided to customer agency contacts on any changes.

HRConnect

HRConnect is hosted and maintained by the Department of the Treasury. The HRConnect Program Office informs HROD of scheduled updated system releases and the changes contained therein. HROD analysts coordinate user acceptance testing for applicable HRConnect changes in a

HRConnect test environment. HROD has documented procedures for testing HRConnect changes. Guidance is provided to customer contacts pertaining to significant changes.

Robotic Process Automation

Changes to RPAs are initiated by a Change Request Form submitted by the business area responsible for the process. DWST reviews these requests, and if approved, a JIRA ticket is created and assigned to an RPA developer.

Once the RPA developer completes the initial development, the RPA is tested in the non-production Acceptance region of the RPA Management Console. The developer then provides output materials and the test plan for Process Owner review. Once reviewed, Process Owner go live approval is obtained. The code then undergoes a final peer code review.

If the change is determined to have a security impact, a Security Impact Analysis portfolio will be completed. If necessary, process documentation outlining an overview of the change is submitted to the Security and Compliance Branch (SCB), who reviews and sends the portfolio to the Policy and Risk Management Branch (PRMB), which is a part of ISS, for a security analysis. Once approved by PRMB to proceed, an Independent Validation (IV) form is completed with supporting evidence including a System Security Plan update, peer code review, and Process Owner approval.

A non-developer resource within the DWST uploads the bot code to the production Management Console, schedules the RPA, and closes the JIRA ticket.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for application changes and determined the consistent use of the procedures by ARC staff provided reasonable assurance that system software and application changes are tested, approved, and documented in accordance with ARC policies and procedures.
2. Observed the HP Service Manager (HPSM) and noted the system is designed to retain necessary change management documentation and noted when the change to HPSM was made.
3. Inspected a selection of changes processed in HPSM/My Oracle Support and determined the changes were tested and approved prior to being implemented in the production environment.
4. Inspected the Oracle on Demand contract and determined it stated that changes to Oracle and PRISM are to be coordinated with Oracle on Demand database administrators.
5. Inspected evidence of access to My Oracle support being monitored and determined access was reviewed biannually.
6. For the one emergency change processed in My Oracle Support for Oracle, inspected evidence of the emergency change and determined that the approval was documented and ARC Application Administrators documented the change in My Oracle Support on the next business day.
7. Inspected the webTA system maintenance agreement and determined it contained system maintenance provisions and was current.
8. For a selection of webTA releases, inspected evidence and determined that the release was tested in a separate/non-production environment using testing scripts and was only released to production after the successful completion of customer acceptance testing by an authorized database administrator and appropriate approvals were obtained.
9. Inspected the ConcurGov system maintenance agreement and determined it contained system maintenance provisions and that it was current.
10. For a selection of ConcurGov changes, inspected documentation of testing and determined changes were tested prior to being implemented in the production environment.

11. For a selection of ConcurGov changes, inspected evidence of the change testing procedures provided by TSD and determined guidance was provided to customer contacts for applied changes.
12. Inspected the moveLINQ system maintenance agreement and determined it contained system maintenance provisions and that it was current.
13. For a selection of moveLINQ changes, inspected evidence and determined that the change was tested in a moveLINQ testing environment, and the change passed the testing prior to being applied in production.
14. Inspected the written procedures for testing and implementing moveLINQ changes and determined the procedures described the process for testing and implementing moveLINQ changes.
15. Inspected the OneStream system maintenance agreement and determined it contained system maintenance provisions and that it was current.
16. For a selection of OneStream changes, inspected evidence and determined that the changes were tested for both system administration and functional requirements prior to implementation.
17. For a selection of new RPAs implemented into production, inspected documentation and determined the RPA was appropriately tested and approved prior to production implementation.
18. KPMG was unable to inspect an example of RPA change documentation as there were no changes implemented into production during the scope period.

No exceptions noted.

Control Objective 21 – Non-interruptive System Service

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

Description of Controls

Fiscal Service has documented policies and procedures for controlling physical access to Fiscal Service 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.

Physical and environmental controls for the data centers that host Oracle, PRISM, ConcurGov, and IPP are not covered in this report.

The Fiscal Service's Asset Protection Division 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) immediately.

The webTA, and moveLINQ servers reside in ISS's data center. Physical access to the ISS data center is restricted to authorized users only. An employee needing access to the data center must have his/her Branch Manager request access for a one-day badge, which will give the employee access to the data center. The requests are made through HPSM, a workflow system that is used to approve data center access. After the Branch Manager completes and submits the HPSM request form for the appropriate ISS Resource area access level, requests are forwarded to ISS's data center managers for approval in the HPSM. If ISS approves the request and the appropriate training is completed by the employee, the Fiscal Service Asset Protection Division (APD), Physical Security Branch (PSB) grants access via PACS. Only designated 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 ISS 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 in order to be issued a 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 and employees 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.

ISS 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, ISS will, based on the individual's need for access, make a decision whether to request that APD remove their data center access or whether to provide authorization for their access.

From Fiscal Service's location, web sites, file transfer protocol (FTP) servers, web servers, and aspects of intrusion detection are monitored every ten minutes with a combination of software monitoring tools that generate alerts. The availability of network infrastructure, such as switches and firewalls, is monitored with a combination of software monitoring tools that generate alerts. ISS's data center is physically monitored by environmental monitoring software that 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 supply (UPS) systems 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. ISS 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, OBI and Discoverer

System operations manuals are provided to each employee assigned system maintenance responsibilities. The Oracle Support Team, within SDB, is available for users to call if they experience difficulties with the system. In addition, Oracle support personnel have access to internal application setup and security documentation, as well as various manuals and documentation produced by OSD/SPSD.

PRISM

PRISM user manuals are provided to end users. The PRISM Support Team within SDB is available for end users to call if they experience difficulties with the system, and PRISM application administrators have access to internal application setup and security documentation, as well as various manuals and documentation produced by OSD/SPSD.

webTA

webTA support personnel have access to online documentation produced by Kronos. The HR Systems Help Desk is available for users to call if they are experiencing difficulties with the system. OSB acts as a liaison between the HR Systems Help Desk and ISS to resolve system issues. Backups are executed on a nightly schedule on local instances per data center and stored within a SAN disk array (short term) then aged off into an onsite cloud (long term). A replication process occurs daily after following the nightly backup processing, which sends the backups to an alternate processing site. The onsite cloud is also replicated to all physical locations of cloud architecture as a tenant of cloud protocols.

See Control Objective 22 for further discussion of the backup process.

ConcurGov

ARC TSD staff investigates and attempts to resolve any system issues noticed by the ARC staff or reported to TSD by ConcurGov users. When possible, TSD staff resolves ConcurGov issues. If TSD staff cannot resolve an issue, the issue is escalated to SAP Concur. TSD notifies system users of the length of the expected outage or malfunction and notifies them again when the issue is resolved.

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 ISS 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.

Prior to May 9, 2020, ISS performed differential backups of the moveLINQ production database nightly and performed a full tape backup weekly. The monthly full backup tapes were sent to a long-term off-site facility for two years once the new high capacity tapes were full.

The moveLINQ system was migrated to the mLINQS Hosting Service on May 22, 2020. MHS hosts the moveLINQ system in accordance with the Fiscal Service contract for SaaS, within their contracted Microsoft Azure Government Cloud PaaS environment. For the database the contractor uses a point in time restore procedure that permits restoration of the application and data to a last known good configuration. Additionally, they maintain a rolling 35 days of the point in time restores and 8 weeks of weekly backups. For the app services, they manually save the "last known good" config and additionally backup the entire App Service nightly. Seven days of the nightly app service backups are available.

See Control Objective 22 for further discussion of the backup process.

Invoice Processing Platform

IPP is a web-based system hosted by the FRB St. Louis. FRB St. Louis has a customer service center for both agencies and suppliers including a help desk phone line and e-mail address. When IPP system issues arise, Fiscal Service sends an e-mail to the IPP Customer Support Center at FRB St. Louis for investigation and resolution.

OneStream

ARC monitors the connection to OneStream to ensure that the application is available. If connection to OneStream fails then a predetermined process of calling the system owners is started until someone within the program area is reached. System owners will contact the appropriate technical or functional area to address the issues and attempt to resolve. If required, the vendor will be contacted to provide additional support and diagnostics via their customer support portal and priority 1 ticket requests for emergencies.

HRConnect

The HR Systems Help Desk investigates and attempts to resolve any system issues noticed by ARC HR staff or reported by HRConnect users. When possible, the HR Systems Help Desk resolves HRConnect issues. If the HR Systems Help Desk cannot resolve an issue, the issue is escalated to the Treasury Tier 2 help desk. The HR Systems Help Desk notifies users of the length of the expected outage or malfunction and notifies them again when the issue is resolved.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for controlling physical access to Fiscal Service buildings and to the data center and determined the consistent use of the procedures provides reasonable assurance that interruptions due to operational failures are appropriately limited.
2. For a selection of new employees issued identification badges, inspected investigation summaries and determined a background check was completed for each individual and each employee had their finger prints on file.
3. For a selection of terminated Fiscal Service employees with access to Fiscal Service buildings located in Parkersburg, WV, inspected the PACS physical access listing and determined their building access had been removed in the PACS.
4. Observed a Fiscal Service individual and noted they displayed their identification badges at all times while inside the Fiscal Service Building.
5. For a selection of employees who were granted access to the ISS data center, but were not on the authorized access list, inspected evidence of the individual's Branch Manager access request for the employee to be issued a one-day badge and determined the request was a) tracked in HPSM, b) approved by ISS, and c) access was granted by a designated Asset Protection Division (APD), Physical Security Branch (PSB) specialist via PACS.
6. For a selection of months, inspected the access violation log and determined that logs were reviewed by ISS, all unauthorized access attempts were investigated, and a follow up with the individual's supervisor were completed.
7. For a selection of dates, inspected the ISS Visitor log and determined it was used to record visitor sign ins and outs, as well as visitor badge issuances.
8. For a selection of dates, inspected the daily shift logs and determined that daily inventories of vendor badges were performed and no missing badges were identified.
9. Inspected evidence of the annual review and recertification of individuals with access to the data center and determined the review and recertification was performed and unauthorized access identified through the review was removed.
10. Observed that HP Site Scope, Solarwinds, and Andover are monitoring ARC hosted applications, and noted ISS staff use them to monitor ARC hosted applications.
11. Observed various monitoring logs and determined a) they automatically generate alerts from HP's Site Scope; b) the application provides monitoring over websites, FTP servers, and intrusion detection software; and c) the logs and alerts are reviewed by ISS.
12. Observed the environmental monitoring software and noted such software was deployed and provided continuous checking and alarming capabilities for temperature changes, water, and humidity threats.
13. Observed sprinklers, hand-held fire extinguishers, air conditioning units and raised floors, and determined that such environmental protection mechanisms were installed in the ISS data center.
14. Observed deployed environmental controls and determined that they are present.
15. Inspected completed maintenance work orders and inspection reports for the UPS system and backup generator and determined the backup generator and UPS system were maintained.
16. Observed that redundant air conditioning (AC) units and noted the units were available and operational in the event of a main AC equipment failure.
17. Observed Oracle operations manuals and noted the manuals were supplied to each employee assigned system maintenance responsibilities.
18. Observed the internal application setup and security documentation and various manuals and documentation produced by Oracle Corporation and noted Oracle support personnel had access to such materials.

Control Objectives, Related Controls, and Tests of Operating Effectiveness

19. Inspected online support documentation for Oracle and determined users had access to the materials and the Oracle Support Team within SDB was available for users to call if they experienced difficulties with the system.
20. Observed internal application setup and security documentation, as well as various manuals and documentation produced by Compusearch, and noted PRISM application administrators had access to such materials.
21. Observed the PRISM user manuals and noted the manuals were available to end users.
22. Inspected online support documentation for PRISM and determined users had access to the materials and the Oracle Support Team within SDB was available for users to call if they experienced difficulties with the system.
23. Observed online documentation produced by Kronos and determined webTA support personnel had access to materials.
24. Inspected online support documentation for webTA and determined users had access to the materials and the HR Systems Help Desk was available for users to call if they experienced difficulties with the system.
25. Inspected the backup configurations for webTA and determined they were configured to complete a nightly differential backup.
26. Observed the backup configurations for a webTA server and determined that the daily replication process was not configured to send backups to an alternate processing site.
    Exception Noted: The backups were not configured to replicate to an alternate processing site since October 2019.
    Management Response: Management concurred with the exception and will implement corrective actions.
27. Inspected the backup log for webTA servers and determined differential backups were completed successfully.
28. Inspected the ConcurGov incident escalation procedures and determined the procedures were documented and available to support ARC staff personnel in investigating and attempting to resolve system issues.
29. Inspected documentation associated with a selected ConcurGov incident that TSD staff was unable to resolve and determined the issue was escalated to SAP Concur Technologies help desk for resolution.
30. Inspected ARC's maintenance agreement with moveLINQ vendor and determined it required the vendor to provide software and technical support for moveLINQ.
31. Inspected the RSB System Administrators escalation procedures and determined it stated that if a RSB Administrator cannot resolve an issue, the issue is escalated to mLINQs.
32. Inspected documentation associated with a selected moveLINQ incident that the RSB Administrators were unable to resolve and determined the issue was escalated to the mLINQs help desk for resolution.
33. Was unable to inspect an example of a moveLINQ tape in the Vendor's website site to verify it was sent off-site, as there was not a tape sent off-site during the examination period due to the transition of new tapes with increased storage capacity.
34. Inspected the backup configuration for moveLINQ and determined backup software was configured to complete both nightly differential and a weekly full backups.
35. Inspected the moveLINQ backup log which is retained for a month and determined scheduled backups were completed as required.
36. Inspected documentation associated with a selected IPP incident that Fiscal Service was unable to resolve and determined the issue was e-mailed to the IPP Customer Support Center at FRB St Louis for investigation and resolution.
37. For a selected IPP system issue that required Fiscal Service to e-mail the IPP Customer Service Center at FRB St Louis, inspected documentation for evidence of investigation and resolution by FRB St Louis and determined ARC tracked customer agency system issues with IPP.

38. Observed the HP Site scope tool and determined that it is used to monitor OneStream and alerts are set-up to notify personnel of system issues.

No exceptions noted, except as described above.

Control Objective 22 – Records Maintenance

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

Description of Controls

moveLINQ

MHS hosts the moveLINQ system in accordance with the Fiscal Service contract for SaaS, within their contracted Microsoft Azure Government Cloud PaaS environment. The contractor uses a point in time restore procedure that permits restoration of the application and data to a last known good configuration.

MHS maintains a rolling 35 days of the point in time restores and 8 weeks of weekly backups. For the app services we manually save the "last known good" config and additionally backup the entire app service nightly. Seven days of the nightly app service backups are available.

Network File Servers

When tapes are returned from the underground off-site storage facility, they are delivered to the Warehouse and Operations Center, located in Parkersburg, WV. Upon arrival Fiscal Service personnel verify the accuracy of the tapes on receipt.

On an annual basis, ISS performs a full physical inventory of all backup tapes that are in Fiscal Service's possession. Physical inventories are conducted at the 3rd Street Data Center in Parkersburg, West Virginia, the Warehouse and Operations Center, located in Parkersburg, WV, Kansas City Regional Operations Center (KROC) Data Center located in Kansas City, MO and at the underground offsite storage facility location.

Differential tape backups of network servers are created daily and retained for a period of five weeks in the backup library. On a weekly basis, ISS completes a full back up of all ARC shared network files to a data tape and they are retained for a two month period at the Warehouse and Operations Center, located in Parkersburg, WV. On a monthly basis, ISS completes a full backup of all ARC shared network files to a data tape and they are retained for a two year period at the underground offsite storage facility location.

Record Storage

Content Manager is an electronic recordkeeping repository application that meets the DoD5015.2 STD-certification 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 Content Manager. Fiscal Service's Records Management Section 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 metadata is recorded in Content Manager. Data records are stored in Content Manager 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

1. Inquired of management and was informed that during the examination period, ARC did not receive tapes from the vendor that were required for a system restore.
2. Inspected evidence of the annual full physical inventory of all backup tapes that were in Fiscal Service's possession and determined the inventory had been performed.
3. For a selection of network file servers used by ARC, inspected system-generated backup schedules and logs and determined daily differential and weekly full backups of the file servers were scheduled and successfully completed.
4. Observed the location of both hard and soft copy records and noted the records were stored in hardcopy and electronic folders respectively, and retained for a specified time period based off the latest document date.
5. For a selection of record boxes to be stored off-site, inspected each box's label and determined it contained a description of the contents of the box to include a unique box identification number, bar code, and the latest document date.
6. For a selection of record boxes to be stored off-site, inspected evidence and determined a description of each of the box's contents, latest document date, and approved retention authority had been entered in to Content Manager.
7. Observed the location of the active and inactive hard copy data records and noted the hard copy records were securely locked up after hours.

No exceptions noted.

MONITORING CONTROLS

Control Objective 23 – Monitoring Subservice Organizations

Controls provide reasonable assurance that SOC 1 reports or system verification letters provided by subservice organizations are reviewed and documented timely in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for staff to follow for reviewing SOC 1 reports and system verification letters.

ARC obtains the relevant SOC reports and documents the review of the report and if any control exceptions impact ARC's control environment. The complementary controls are reviewed and linked to controls in ARC's SOC report. The reviews are approved by management and documentation on the subservice organizations is made available to customer agencies. ARC contacts the subservice organization to obtain additional information for exceptions if applicable.

ARC obtains a system verification letter for the Fiscal Service subservice organizations that do not have a SOC 1 report. The system verification letter is reviewed and approved by ARC and made available to customer agencies.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for reviewing SOC 1 reports and system verification letters and determined the consistent use of the procedures provides reasonable assurance that SOC 1 reports and system verification letters are appropriately reviewed and approved.
2. Inspected SOC 1 report review memorandums and determined the reviews were documented and approved.
3. Inspected system verification letters and determined the reviews were documented and approved.

No exceptions noted.

V. OTHER INFORMATION PROVIDED BY THE ADMINISTRATIVE RESOURCE CENTER

CONTINGENCY PLANNING

System Back Up

The Oracle accounting system has a contingency plan managed by the ARC. The formal ARC Business Continuity Plan (BCP) was changed, new name being, OSS Business Continuity Plan, which was last updated in May 2016**.** All essential Oracle functions will be performed with the support of ARC employees. Full disaster recovery testing is performed on an annual basis in conjunction with Fiscal Service's ISS, Data Center's Disaster Recovery Plan (DRP). The Oracle primary database servers, located at Oracle Managed Cloud Services' primary site in Austin, TX, are replicated near real time using Data Guard to a contingency location. Oracle's Network File System (NFS) serves as the secondary back up of live data for the application. Data from the NFS is sent to tape back-up twice weekly and stored at an offsite location. These tapes serve as a tertiary back-up.

Prior to May 29, 2020, ISS performed differential backups of the moveLINQ production database nightly and performed a full tape backup weekly. The nightly backups were kept on-site for four weeks. The monthly full backup tapes were sent to a long-term off-site facility for two years. These backups ceased on May 29, 2020 after the system was moved to the MHS Cloud on May 22, 2020.

The moveLINQ system is tested annually as part of the Business Continuity Plan (BCP). Microsoft performs annual contingency testing of the platform. Annual BCP testing is performed which includes the Fiscal Service access to the moveLINQ system hosted within the MHS environment and the support tools hosted at Fiscal Service.

MHS is responsible for the system backups and data is maintained for six years.

SAP Concur, Inc. is responsible for system backup of ConcurGov and maintains data for six years.

IPP data is stored and backed-up on the storage area network (SAN) and replicates every minute between EROC (East Rutherford Operational Center) and Dallas. FRB St. Louis does a disaster recovery exercise for contingency planning, typically in August, to test the failover of IPP from their hosting facility in EROC to Dallas. The test ensures that the application successfully moved to Dallas, but does not require agencies to point to a different IP address in Dallas to submit a file due to its manually intensive nature.

Continuity of Operations

A fire alarm and sprinkler system that is managed, maintained, and tested by the building management protects ARC and ISS 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, except for the Data Center which utilizes a pre-action system.

In the event the main building becomes inoperable, network operations would be relocated to the KROC facility in accordance with the ISS data center's DRP. This facility employs a "warm site" strategy for recovery of network operations.

As part of the ARC BCP, should ARC facilities become unavailable, essential ARC personnel will relocate to established telework locations to reestablish their essential functions.

MANAGEMENT RESPONSE TO EXCEPTIONS IDENTIFIED IN THE REPORT

Control Objective 21 – Non-interruptive System Service

We have enabled the data replication for the impacted webTA server on July 12, 2020, and the backups are now sent to the alternate processing site. We are also developing a new policy and procedure to ensure that the control is implemented.

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig