Audit Report

OIG-23-037

FINANCIAL MANAGEMENT

Report on the Bureau of the Fiscal Service's Description of its Administrative Resource Center Shared Services System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2022 to June 30, 2023

September 29, 2023

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

**OFFICE OF
INSPECTOR GENERAL**

September 29, 2023

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

FROM: Ade O. Bankole /s/
                       Director, Financial Statement Audits

SUBJECT: Report on the Bureau of the Fiscal Service's Description of its
                       Administrative Resource Center Shared Services System and
                       the Suitability of the Design and Operating Effectiveness of its
                       Controls for the Period July 1, 2022 to June 30, 2023

We hereby transmit the attached subject report. Under a contract monitored by our office, KPMG LLP (KPMG), a certified independent public accounting firm, examined the Bureau of the Fiscal Service's description of its shared services system (the "system") titled "Management of Administrative Resource Center's (ARC) Description of its Shared Services System" throughout the period July 1, 2022 to June 30, 2023, for processing customer agencies' financial management, procurement, and human resource services transactions and general computer and monitoring controls and the suitability of the design and operating effectiveness of these controls. This report includes management's description of its shared services system, management's written assertion, and KPMG's independent service auditors' report. The contract required that the examination be performed in accordance with U.S. generally accepted government auditing standards and the attestation standards established by the American Institute of Certified Public Accountants.

In its examination, KPMG found in all material respects:

- the description fairly presents the system that was designed and implemented throughout the period July 1, 2022 to June 30, 2023;
- 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, 2022 to June 30, 2023, and subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2022 to June 30, 2023; and

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2022 to June 30, 2023 if complementary subservice organization and customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2022 to June 30, 2023.

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 auditors' report dated September 29, 2023, 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) 927-5329, or a member of your staff may contact Mark S. Levitt, Audit Manager, Financial Statement Audits, at (202) 927-5076.

Attachment

cc: Jeffrey J. Schramek
    Executive Director,
    Administrative Resource Center

Department of the Treasury
Bureau of the Fiscal Service

Administrative Resource Center Shared Services
Financial Management, Procurement, and Human Resources Transactions and
General Computer and Monitoring Controls

Report on the Description of the Administrative Resource Center Shared
Services System and the Suitability of the Design and Operating Effectiveness
of Its Controls (SOC 1® - Type 2 Report)
For the Period July 1, 2022 to June 30, 2023

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
ADMINISTRATIVE RESOURCE CENTER SHARED SERVICES

REPORT ON THE DESCRIPTION OF THE ADMINISTRATIVE RESOURCE CENTER SHARED SERVICES SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS

FOR THE PERIOD JULY 1, 2022 TO JUNE 30, 2023

Table of Contents

I. INDEPENDENT SERVICE AUDITORS' REPORT PROVIDED BY KPMG LLP

Independent Service Auditors' Report

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

Scope
We have examined management of the Bureau of the Fiscal Service's Administrative Resource Center (ARC) accompanying description of its shared services system for processing customer agencies' Financial Management, Procurement, and Human Resources Services transactions and General Computer and Monitoring Controls (the System) throughout the period July 1, 2022 to June 30, 2023 titled "Management of Administrative Resource Center's Description of its Shared Services System" (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 "Management of Administrative Resource Center's Assertion" (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 the 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 Management of Administrative Resource Center," is presented by management of ARC to provide additional information and is not a part of the Description of its System made available to customer agencies during the period July 1, 2022 to June 30, 2023. Information about ARC's contingency planning has not been subjected to the procedures applied in the examination of the Description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description of the 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, management of 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 Auditors' 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 and the standards applicable to attestation engagements contained in *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 the 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, 2022 to June 30, 2023. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

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 the 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 the Assertion:

  a. the Description fairly presents the System that was designed and implemented throughout the period July 1, 2022 to June 30, 2023;
  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, 2022 to June 30, 2023, and subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2022 to June 30, 2023; 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, 2022 to June 30, 2023 if complementary subservice organization and customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2022 to June 30, 2023.

Restricted Use
The purpose of this report, including the description of tests of controls and results thereof in Section IV "Management of Administrative Resource Center's Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Tests" is solely to provide information for management of Fiscal Service, customer agencies of Fiscal Service's ARC Shared Services during some or all of the period July 1, 2022 to June 30, 2023 and its 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 customer agencies themselves, when assessing the risks of material misstatement of customer agencies' financial statements, to support evaluations of the effect of Fiscal Service's ARC Shared Services' controls on customer agencies' financial statements. Accordingly, this report is not suitable for any other purpose.

KPMG LLP

September 29, 2023
McLean, Virginia

II. MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER'S ASSERTION

September 29, 2023

Administrative Resource Center's Assertion

We have prepared the accompanying description of Bureau of the Fiscal Service's (Fiscal Service) Administrative Resource Center (ARC)'s Shared Services System for Financial Management, Procurement, and Human Resources Services transactions and General Computer and Monitoring Controls system (the System) for processing customer agencies' transactions throughout the period July 1, 2022 to June 30, 2023 titled "Management of Administrative Resource Center's Description of the Administrative Resource Center Shared Services System" (the Description) for customer agencies' of the System during some or all of the period July 1, 2022 to June 30, 2023 and their 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 organizations and customer agencies of the System themselves, when assessing the risks of material misstatement of user entities' financial statements.

ARC uses subservice organizations for some of its application processing. 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 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 organizations.

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 the System made available to customer agencies of the System during some or all of the period July 1, 2022 to June 30, 2023 for processing their transactions as it relates to 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 of the System 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 of the System;

        (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 other information prepared for customer agencies;

(4) how the System captures and addresses 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, 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 agency controls and complementary subservice organization controls assumed in the design of the service organization's controls; and

(8) other aspects of our control environment, risk assessment process, information and communication (including the related business processes), control activities, and monitoring activities that are relevant to the 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, Procurement, and Human Resource 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, 2022 to June 30, 2023 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, 2022 to June 30, 2023. 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 management of ARC;

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,

Paula Corbin.
Acting - Deputy Commissioner,
Administrative Resource Center

**III. MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER'S
DESCRIPTION OF ITS SHARED SERVICES SYSTEM**

OVERVIEW OF OPERATIONS

The Administrative Resource Center (ARC) is an organizational unit of the Bureau of the Fiscal Service (Fiscal Service). Beginning with Fiscal Year (FY) 2023, ARC was reorganized to become a discrete organizational unit within the Fiscal Service. With this reorganization, all 6 divisions of the Office of Shared Services and 9 divisions from Fiscal Accounting were transferred to ARC. ARC 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 and Vendors Branch (APVB)	Accounting
	Document Processing
	Reporting
	1099 Reporting
	Supplier Table Update and Maintenance
Accounts Receivable Branch (ARB)	Accounting
	Document Processing
	Reporting
	Debt Collection
	Treasury Report on Receivables Reporting
Agency Intragov Processing Branch (AIPB)	Intragovernmental Business
	Document Processing
Agency Intragov Reports and Projects Branch (AIRPB)	Intragovernmental Business
	Reporting

Transaction Management Division (TMD)	Services Provided
Payroll and Cards Branch (PCB)	Accounting
	Record and Reconcile Payroll
	Purchase Card Processing
Grants and Loans Branch (GLB)	Accounting
	Document Processing
	Reporting
	Grant, Foreign Transaction, and Loan Activity
Special Services Branch (SSB)	Accounting
	Document Processing
	Reporting
	Debt Collection
	Treasury Report on Receivable Reporting

Funds Management Division (FMD)	Services Provided
Funds Management Branch (FMB)	Document Processing
	Reporting

	Investment Activities
Agency Cash Branch (ACB)	Provides Cash Related Services
	Disbursements to Non-federal Entities
	Check Scanning
	Fund Balance with Treasury Reconciliation
	Accounting
Budget Execution Branch (BEB)	Accounting
	Reporting
	Budget

Agency Reporting and Analysis Division (ARAD)	**Services Provided**
Reporting and Analysis Branch 1 (RAB1)	Accounting
	Reporting, Analysis, and Audit Support
Reporting and Analysis Branch 2 (RAB2)	Accounting
	Reporting, Analysis, and Audit Support
Reporting and Analysis Branch 3 (RAB3)	Accounting
	Reporting, Analysis, and Audit Support

Operations Support Division (OSD)	**Services Provided**
Procurement and Accounting Support Branch (PASB)	Operate and Maintain Financial Management Systems
Reporting and Technology Support Branch (RTSB)	Operate and Maintain Financial Management Systems

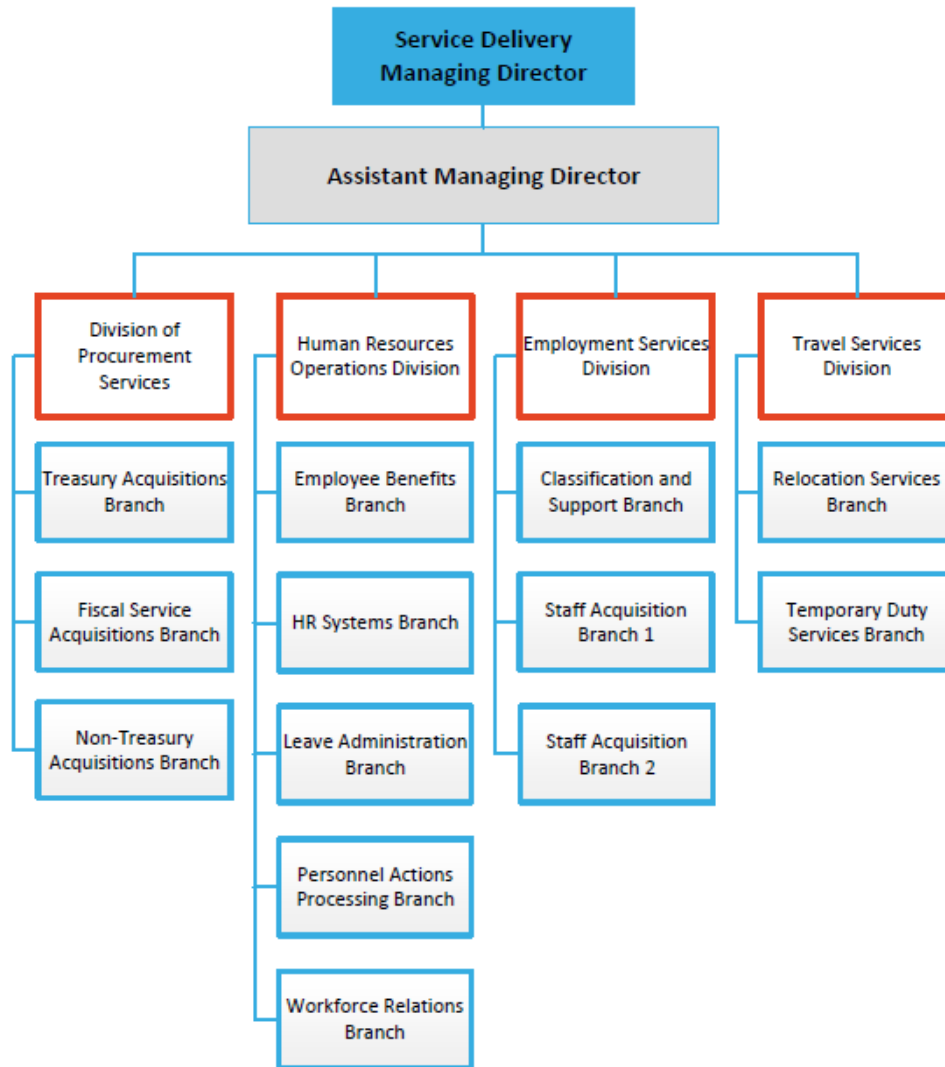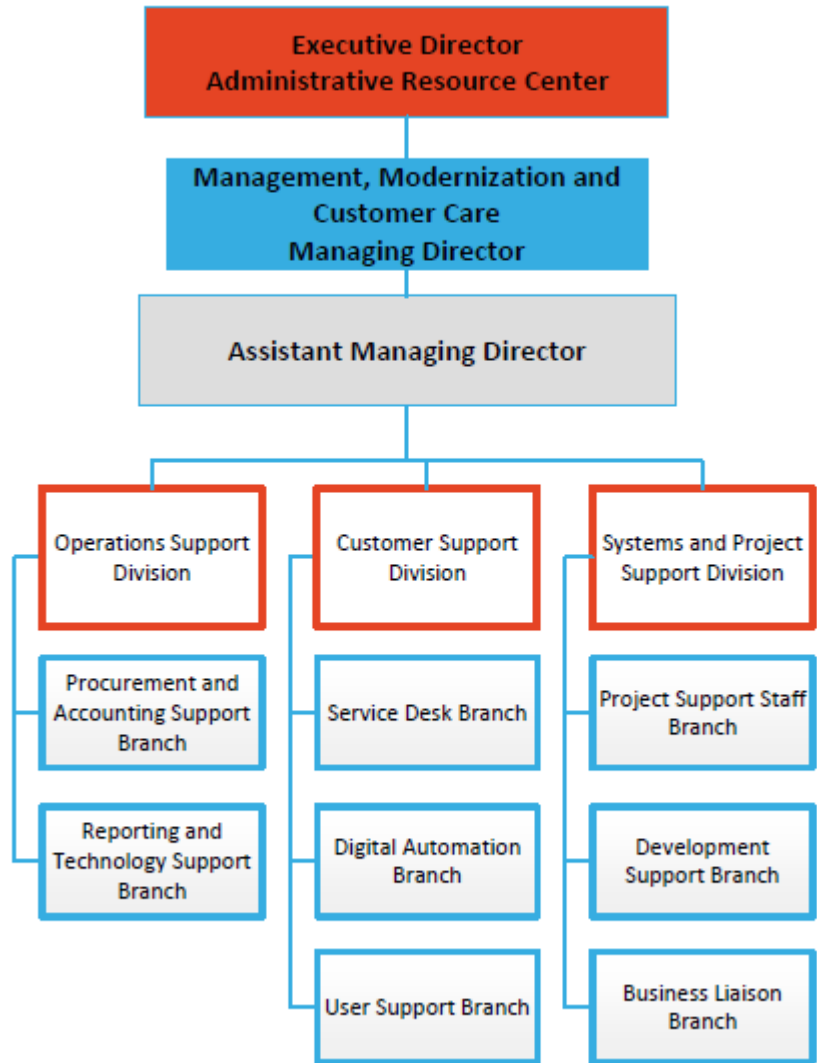| **Customer Support Division (CSD)**	**Services Provided**
Service Desk Branch (SDB)	Financial Management System Support and Training
Digital Automation Branch (DAB)	Develop and Maintain Robotic Process Automation
User Support Branch (USB)	Financial Management System Support and Training

Systems and Project Support Division (SPSD)	**Services Provided**
Project Support Staff Branch (PSSB)	Application Development, Analysis, and Project Management
Development Support Branch (DSB)	Application Development, Analysis, and Project Management
Business Liaison Branch (BLB)	Internal Project Support

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

Human Resources Operations Division (HROD)	**Services Provided**
Employee Benefits Branch (EBB)	Processes and Monitors Personnel Benefit Actions

HR Systems Branch (HRSB)   HR Business System Support

Leave Administration Branch (LAB)   Processes and Monitors Time and Attendance Records

Personnel Actions Processing Branch (PAPB)   Processes and Monitors Personnel Payroll Transactions

Workforce Relations Branch (WRB)   Processes and Monitors Personnel Actions

Employment Services Division (ESD)	**Services Provided**
Classification and Support Branch (CSB)	Position Classification
Staff Acquisition Branch 1 (SAB1)	Staff Acquisition
Staff Acquisition Branch 2 (SAB2)	Staff Acquisition

Travel Services Division (TSD)	**Services Provided**
Relocation Services Branch (RSB)	Relocation
Temporary Duty Services Branch (TDSB)	Temporary Duty

These services are provided by the divisions as shown in the following organizational charts below:

Management of Administrative
Resource Center's Description
of its Shared Services System

Executive Director
Administrative Resource Center

Management, Modernization and Customer Care
Managing Director

Assistant Managing Director

Operations Support Division
- Procurement and Accounting Support Branch
- Reporting and Technology Support Branch

Customer Support Division
- Service Desk Branch
- Digital Automation Branch
- User Support Branch

Systems and Project Support Division
- Project Support Staff Branch
- Development Support Branch
- Business Liaison Branch

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 help 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 awards, training orders or interagency agreements. Recording the obligations in Oracle sets aside funds to help 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 receive 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 Oracle. 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 award. In the second method, invoices are submitted directly to ARC to be manually processed (non-IPP). ARC has controls 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 help 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 help 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 Fund Transfer (EFT) Act 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 Department of the Treasury (Treasury) for payment using Treasury's Secure Payment System (SPS). In addition, ARC processes most intragovernmental payments using Fiscal Service'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 made.

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 with Oracle. 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 Oracle.

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 Treasury'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 help ensure transactions are posted to the appropriate accounts.

ARC works with customer agencies to develop and implement processes to help 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 Oracle 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, Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS), Treasury Report on 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 helps ensure that proprietary and budgetary general ledger account relationships are maintained and accurate, and corrects any discrepancies.

System Platform Services

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 system changes. To this end, ARC maintains

responsibility for System Integration Testing (SIT), providing customers an opportunity to perform User Acceptance Testing (UAT), and approving production changes.

Procurement Services

Procurement Services consist of the following:

- Awarding of acquisitions 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 Procurement Request Information System Management (PRISM).

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 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.

Human Resources Services

The Human Resources Operations Division (HROD) provides payroll and personnel actions processing, using the Treasury HRConnect or National Finance Center's (NFC) Entry, Processing, Inquiry and Correction System (EPIC). 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, liaison, or employee will initiate the transaction and an Employee Benefits Branch (EBB) HR specialist will code the transaction (some actions require an EBB supervisor to approve). Once it is approved, the action is sent to the Personnel Actions Processing Branch (PAPB) to process and release the transaction. For removals and non-transfer terminations (i.e., termination of probationary/trial employee), actions are submitted in HRConnect by a manager. A Workforce Relations Branch (WRB) Employee and Labor Relations (ELR) Specialist reviews, codes, and approves the personnel action, and then forwards the personnel action to PAPB. For all other separations a PAPB HR Assistant determines the type of separation and codes the personnel action for review and approval by a PAPB 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 Employment Services Division (ESD), PAPB or WRB review the information, request any additional information needed

and code and authorize the personnel action. After the personnel action is coded and approved, it is released from HRConnect by a PAPB HR Assistant. The PAPB HR Assistant verifies the action was applied in the NFC and a different PAPB 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 PAPB HR Assistant reviews the information, requests any additional information needed, and codes the personnel action. The PAPB HR Assistant releases the action in HRConnect. The PAPB HR Assistant verifies the action applied in NFC, and a different PAPB HR Assistant verifies the information in NFC is correct.

All Federal Employees' Group Life Insurance (FEGLI) elections are initiated via a SF-2817, Life Insurance Election form received within the United States of America Staffing (USA Staffing) Onboarding system or outside the system (fax, email, United States Postal Service (USPS), etc.). An EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. If a FEGLI election results from a qualifying life event (QLE), an EBB HR Assistant requests documentation to verify eligibility to make a change due to the QLE. For the forms received outside of the Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the Onboarding system, the election electronically transmits to HRConnect, where the HR Assistant releases the election to NFC. For all forms, the EBB HR Assistant 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.

Federal Employees Health Benefits (FEHB) and Thrift Savings Plan (TSP) elections are employee-initiated via the appropriate form received within the USA Staffing Onboarding system, outside the system (fax, email, USPS, etc.) or via Employee Personal Page (EPP). When elections are submitted outside of EPP, an EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. For FEHB elections that are a result of a QLE, an EBB HR Assistant requests documentation to verify eligibility to make a change due to the QLE. For any dependent being added to an FEHB plan, an EBB HR Assistant obtains documentation to verify family member eligibility and notes it on the form. For the forms received outside of the Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the Onboarding system, the election electronically transmits to HRConnect, where the HR Assistant releases the election to NFC. For all forms submitted outside of EPP, the EBB HR Assistant 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 are met. A Leave Administration Branch (LAB) HR Specialist enters and releases the payroll document in EPIC. After NFC's Payroll Computation System (PAYE) runs, the LAB HR Specialist verifies that the employee was paid for the hours.

Payroll documents for new hires are submitted to PAPB within the USA Staffing Onboarding system, as part of the on-boarding process. The forms electronically transmit to HRConnect, where a PAPB HR Assistant reviews and releases the payroll documents to NFC. The PAPB HR Assistant verifies the payroll documents applied in NFC and a different PAPB HR Assistant verifies the information in NFC is correct. If the payroll documents do not apply or apply incorrectly in NFC, the PAPB HR Assistant, along with assistance from a PAPB HR Specialist, resolve any issues.

After PAYE runs, the PAPB HR Assistant who entered the payroll documents confirms that the employee was paid correctly.

Most changes in payroll information are completed by the employee using the self-service option in NFC's EPP. In rare cases, employees submit requests for payroll document changes and/or deductions in writing to PAPB. A PAPB Processing Call Center Assistant reviews the request and contacts the employee if more information or additional verification is needed. The PAPB Processing Call 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 PAPB Processing Call Center Assistant verifies the action applied in NFC and a different PAPB Processing Call Center Assistant verifies the information in NFC is correct. Employees can also submit requests for changes and/or deductions through NFC's 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.

Travel Services

The Travel Services Division (TSD) provides relocation services and temporary duty services, which consist of the following:

Relocation Services consist of the following:

- Operating and maintaining moveLINQ, a government relocation expense management system in compliance with the Federal Travel Regulations (FTR), Department of State Standardized Regulations (DSSR), and Joint Travel Regulations (JTR) 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.
- Providing application administration.
- Providing customer service.
- Providing application 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 an interface with Oracle.
- Providing 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 submitted to the traveler and/or Approving Official for review and approval via the Portal, as appropriate. ARC processes payments and the approved documents are interfaced and reconciled to Oracle daily for customer agencies.

Temporary Duty services consist of the following:

- Operating and maintaining the ETS systems (ConcurGov) in compliance with the FTR for all 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 with 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 documents are interfaced with Oracle immediately upon approval, providing the document has sufficient funding and valid accounting. Each received authorization and voucher is reconciled to Oracle daily. ConcurGov contains system audits that prohibit documents that do not meet certain FTR or contain the required accounting information from being approved and thereby interfacing to Oracle.

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

Control Environment

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

ARC holds management meetings on a regular basis to discuss special processing requests, operational performance, and the development and maintenance of projects in process. Documented 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 personnel when they are hired and every three to five years. The confidentiality of customer agency information is stressed during the new employee orientation program and is emphasized in the personnel manual issued to each employee. ARC provides a mandatory orientation program to all full time employees and encourages employees to attend other formal outside training. Training available to employees with related work responsibilities includes, but is not limited to: Prompt Pay and Voucher Examination, Appropriation Law, Federal Acquisition Regulations, FTR, Reconciling with and Reporting to Treasury, Federal Accounting Fundamentals, USSGL Practical Applications, Budgeting and Accounting – Making the Connection and Computer Security Awareness Training.

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

ARC has placed into operation a risk assessment process to identify and manage risks that could affect ARC's ability to provide reliable services to the 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

ARC management monitors the quality of internal control performance as a normal part of their activities. Management inquires of staff and/or review data to help 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 management within ARC's Agency Reporting and Analysis Division reviews reconciliations from Oracle subledger 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. 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 ARC systems that do not receive a SOC 1 report, system verification letters are prepared to document the information security controls that are implemented. ARC will contact the subservice organization to obtain additional information for exceptions if applicable.

INFORMATION AND COMMUNICATION

Information Systems

ARC performs application administration for the following applications: PRISM, ConcurGov, moveLINQ, and IPP which are all feeder systems into Oracle. Oracle Managed Cloud Services (OMCS) hosts Oracle, OBI, and PRISM; SAP Concur hosts ConcurGov; the Federal Reserve Bank of St. Louis hosts IPP; mLINQS Hosting Service (MHS) hosts moveLINQ within their contracted Microsoft Azure Cloud Government Cloud platform; Microsoft Azure Government hosts OneStream XF; Salesforce hosts oneARC within their contracted Amazon Web Services (AWS) GovCloud+ platform; and ARC hosts webTA.

Oracle Federal Financials (Oracle), Oracle Business Intelligence (OBI)

OMCS operates Oracle R12 and Oracle databases in an Oracle Cloud Infrastructure system environment. Oracle uses a two-tier web-based infrastructure with a front-end Internet user interface and a database residing inside a secure network. Access to the front-end user interface is controlled by a secure Lan2Lan (l2l) tunnel by the Bureau of Fiscal Service. All tunnel connectivity is controlled by Bureau of the Fiscal Service administrators and is only opened to approved customer assigned network ranges. Functions of Oracle include budget execution, federal report generation, general ledger, purchasing, accounts payable, accounts receivable, project accounting, fixed assets, and manufacturing. ARC currently uses Oracle Business Intelligence (OBI) as a report writer package. The package provides users with the ability to create their own ad-hoc reports for query purposes. It is an intuitive ad-hoc query, reporting, analysis, and Web-publishing tool that empowers business users at all levels of the organization to gain immediate access to the Oracle operational database. The information from OBI is obtained directly from the Oracle tables.

PRISM

OMCS, which operates PRISM, uses the Windows Server 2016 operating system. PRISM uses an Oracle 19c database running in a Cloud Infrastructure 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 OMCS 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

Fiscal Service's IPP electronic invoice processing solution (mandated by the OMB Electronic Invoicing Mandate) is a web-based electronic invoicing and payment information system. Awards 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 with Fiscal Service's National Payment Center of Excellence (NPCE), which provides payment services for federal agency sites. IPP users consist of invoice approvers, viewers and administrators.

webTA

Ultimate Kronos Group's (UKG) webTA is the time and attendance system for a majority of their 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 in order to be interfaced with Oracle. webTA uses an Oracle database, which runs on the ARC subnet and accesses data in the ARC demilitarized zone (DMZ) using Red Hat Linux, an Apache web server, and a Tomcat application server. 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.

ConcurGov

SAP Concur's travel system ConcurGov is the system selected by the Treasury as its E-Gov Travel solution. 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 help 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 travel (TDY) authorizations, vouchers, local vouchers and miscellaneous employee reimbursements. Approved documents interface with Oracle for obligation or payment during a real time interface process. ConcurGov users consist of travelers, document preparers, budget reviewers, Approving Officials and administrators. TSD Analysts test all applicable ConcurGov changes in a ConcurGov acceptance test environment.

moveLINQ

The mLINQS relocation expense management system, moveLINQ, fulfills the relocation management program, payment system and reporting requirements. moveLINQ is used to support and enable agencies' administration of their travel programs such as E-Gov Travel Service. moveLINQ is a Federal Travel Regulation 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 with 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 Fiscal Service system is hosted separate from other mLINQS customers. MHS maintains a rolling 35 days of the point in time restores and 8 weeks of weekly backups. For the application services, ARC manually saves the "last known good" configuration files and performs a nightly backup of the entire application service. Seven days of the nightly application service backups are available.

Robotic Process Automation

The Kofax[1] robotic process automation (RPA) creates and deploys software robots (or bots) to automate repetitive tasks and manual processes. Currently, RPAs are used in Control Objectives 2 and 18. ARC's RPAs are developed and managed by the Digital Automation Branch (DAB). Access to the Kofax RPA software and the bot code network drive directory is restricted to authorized users by use of Enterprise Service Management (ESM/ServiceNow) tickets before access is granted. ESM/ServiceNow 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 three separate environments: integration, acceptance test, and the production environment. The integration environment is only used for software upgrades. The acceptance 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 DAB uploads the RPA code in the production Kofax RPA Management Console and then closes the JIRA ticket.

OneStream XF

OneStream XF is a corporate performance management tool. The application accesses the database 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 TLS encrypted connection. OneStream XF is configured to consolidate financial data and automate workflows for financial reconciliations and financial statement reporting processes.

oneARC

The Salesforce enterprise system is a Customer Relationship Management system that allows customers to provide customized support to their customers and manage customer accounts, cases, and interactions via phone, e-mail, mobile, messaging, and social media channels. Questions and comments from social media channels can become part of a case queue, and customers can easily collaborate using mobile devices. Information from online profiles can be used to deliver customized responses. Salesforce applications can be fully integrated with back-office applications.

ARC has configured a Salesforce GovCloud+ instance to handle Budgetary, Purchasing, and Accounts Payable Financial Management requests from customer agency contacts. The request values and approvals stored in the Salesforce instance for each request type include the requester, a request approver if needed, applicable notes on request, and documents which ARC employees worked on the case record.

oneARC is the mechanism by which customers request Financial Management transactions. It contains workflows that route the work to the correct assignment group in ARC instead of the customers having to send emails to a group mailbox.

---

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

Communication

ARC has implemented various methods of communication to help ensure that all employees understand their individual roles and responsibilities. These methods include orientation and training programs for newly hired employees, and use of e-mail 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 ARC's employee training and career development programs, internal training classes, and professional conferences.

Control Objectives and Related Controls

ARC'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 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 the overall internal control for each ARC customer agency. 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, considering 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:

- Approve and return relocation travel documents to RSB for processing in moveLINQ in a timely manner.
- 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.
- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.
- Review and communicate customer agency required levels of budget and expenditure controls to ARC.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Send approved requests to record manual obligations to ARC in a timely manner.
- Approve invoices for payment and send approved invoices to ARC in a timely manner.
- Approve travel vouchers and accurately enter the vouchers into ConcurGov in the proper period.
- 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.
- Maintain and communicate to ARC a list of individuals and applicable authority limits authorized to request non-referencing payments and expense corrections.
- 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.
- Ensure relocation documents are authorized and completely and accurately processed in their agency financial system in a timely manner.
- Properly allocate SmartPay charges and obtain Approving Official certification prior to auto-close.
- Provide post payment approval for SmartPay auto-closed invoices.
- Review the financial reports provided by ARC to help ensure that disbursement transactions are complete and accurate.
- Plan and monitor cash flow related to reimbursable authority to prevent overspending of cash.
- Ensure that the Chief Financial Officer (CFO) certifies that the TROR and Debt Collection Activities report submitted to the Treasury is accurate and consistent with agency accounting systems.
- Review unfilled customer orders, receivable and advance reports for completeness, accuracy, and validity.

- Send approved and accurate documentation of unfilled customer orders, receivables, and cash receipts transactions to ARC in the proper period.
- Provide assistance, when requested, to determine a check's purpose and validity prior to deposit.
- Review and confirm the leave accrual schedule annually.
- Review the financial reports provided by ARC to help ensure that monthly payroll and leave accruals are complete and accurate.
- Review and confirm ARC customer agency specific payroll disbursement procedures on an annual basis.
- Review the financial reports provided by ARC to help ensure that payroll disbursements are complete and accurate.
- Verify that payroll processed by third-party providers is complete and accurate.
- Review and approve, prior to submission, the financial reports prepared by ARC to help ensure that reports prepared for external use are complete, accurate, and submitted in a timely manner.
- Ensure that the variance analyses are reviewed and approved by Treasury and the Department of Homeland Security's (DHS) CFO or designee in support of financial reports' completeness, accuracy and timely submission for external use.
- Approve and send revenue and expense accruals to ARC in a timely manner.
- Review open accrual reports for completeness, accuracy, and validity.
- Review the financial reports provided by ARC to help ensure that accruals are complete and accurate.
- Review and approve, prior to submission, the financial reports prepared by ARC to help ensure that all reports prepared for external use are complete, accurate, and submitted in a timely manner.
- Review and provide authorization of all DATA Act files prior to submission.
- Provide certification of GTAS to ARC prior to system certification.
- Review and approve the annual submission of the TROR and Debt Collection Activities report.
- Communicate OMB apportionment status to ARC.
- Monitor usage of budget authority during periods of operation under a Continuing Resolution to help ensure that OMB directed apportionment limits are not exceeded.
- Review the financial reports provided by ARC to help ensure that budget entries are complete and accurate.
- Send approved budget plans to ARC in a timely manner.
- Routinely review authorizations within oneARC to confirm that only authorized users are submitting budget template requests on behalf of the agency.
- Maintain and communicate to ARC a list of individuals authorized to submit manual journal entries that are initiated by the customer agency.
- Send valid and approved requests to record manual journal entries to ARC in a timely manner if they are initiated by the customer agency.
- Communicate to ARC any known delays to receipt or disbursement activity that may impact investments.
- Communicate to ARC any larger than normal receipt or disbursement activity that may impact investments.
- Provide applicable legislation, and any subsequent legislation revisions, that authorizes the customer agency to invest with the investment account set-up.
- 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.
- 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.

- Review active supplier reports provided by ARC and request to remove suppliers no longer needed in a timely manner.
- Help ensure all personnel actions are submitted in HRConnect timely.
- Notify ARC timely regarding separating employees.
- Notify ARC timely of any changes to HRConnect authorized approvers.
- Review and approve listings of users with current Oracle, OBI, PRISM, webTA, ConcurGov, IPP, OneStream XF, and HRConnect access to help ensure appropriateness and provide changes to ARC in a timely manner.
- Routinely review approvers within oneARC to confirm that only authorized users and responsibilities are executing actions and approvals.

Specific CCACs are provided in Control Objectives 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, and 18 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 administers the business applications described below that provide government wide transactions and produce reports and outputs that are relevant to customer agencies' internal control over financial reporting.

Central Accounting Reporting System (CARS) –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 performs reconciliations between the account summary and transaction reports.

Secure Payment System – ARC processes payments for invoices within SPS.

Collections Information Repository (CIR) and IPAC – Receivables and any cash differences (collections and disbursements) are identified between these two applications.

Treasury Report on Receivables (TROR) and Debt Collection Activities, Cross Servicing Next Generation (CSNG) System–TROR is the primary means for providing data on the status of non-tax debt portfolio. Debts are transferred for collection to Debt Management Services (DMS) via CSNG.

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 215s, 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 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 subsystem of the Debt Information Management System (DIMS). InvestOne is used to record and report investment activity and balances reported by FMB. The InvestOne accounting system is licensed by FIS Capital Markets US LLC. The investment activity 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 – Invoices are electronically routed for approval and payment within IPP.

Department of the Treasury

Treasury administers the business applications described below that provide reports and outputs that are relevant to customer agencies' internal control over financial reporting.

TIER – For ARC's Treasury 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 bureaus and other reporting entities within the Treasury and in a standardized format. Data submitted to TIER 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.

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

HRConnect – The human resources management system owned and administered by the Treasury designed 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 NFC'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 and is responsible for the backup of data.

Oracle Corporation

Oracle Managed Cloud Services – Provides the computer processing, infrastructure and support for Oracle, OBI, and PRISM. OMCS staff serve as the database and operating system administrators and provides backup and recovery services for Oracle and PRISM. ARC retains application administration responsibilities.

OneStream XF

OneStream XF – OneStream XF allows for financial data to be consolidated and workflows to be automated pertaining to financial reconciliations and financial statement reporting.

United States Department of Agriculture

National Finance Center (NFC) – NFC processes payroll and personnel actions, initiated in front-end systems (HRConnect and EPIC) by ARC personnel. The actions are then sent to NFC's Payroll/Personnel System (PPS). PPS includes the processing of personnel actions, awards, allotments, performance appraisals, health and life insurance, 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. These files are for recording payroll disbursements.

mLINQS, LLC

moveLINQ – Relocation expense management system. MHS applies updates and provides system administration, while ARC provides the 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.

Salesforce

oneARC – The oneARC system was developed with internal and contractor resources to provide ARC with an automated authorization and case management system to track customer requests for the Budget lifecycle. oneARC is hosted by Salesforce within their contracted AWS GovCloud+ platform.

Office of Personnel Management (OPM)

USA Staffing Onboarding – ARC uses USA Staffing Onboarding, OPM's system for the end-to-end talent acquisition process, as the means for receiving information from a new hire. USA Staffing Onboarding allows new hires to electronically submit health and life insurance forms, and payroll documents (e.g., tax forms and direct deposit information) to ARC.

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, considering 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.

Bureau of the 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 – Budget, and Control Objective 12 – Federal Investments

- Responsible for restricting logical access, including privileged user accounts, to services and other hardware devices used to host, manage and support CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA.
- Responsible for granting, reviewing, and removing user access to CARS, SPS, CIR, 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, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA.
- Responsible for maintaining physical access and environment controls for CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA.
- Responsible for performing data back-ups for CARS, SPS, CIR, TROR, CSNG, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA.
- Responsible for maintaining business process controls for input, processing, and output of information for CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA.

Department of the 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 16 – Personnel Actions, and Control Objective 17 – Payroll Documents

- Responsible for restricting logical access, including privileged user accounts, to services and other hardware devices used to host, manage and support TIER, FARS, and HRConnect.
- Responsible for granting, reviewing, and removing user access to TIER, FARS, and HRConnect.
- Responsible for performing patching to the operating system and database and application changes to TIER, FARS, and HRConnect.

- Responsible for maintaining physical access and environment controls for TIER, FARS, and HRConnect.
- Responsible for performing data back-ups for TIER, FARS, and HRConnect.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information for TIER, FARS, and HRConnect.

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 restricting logical access, including privileged user accounts, to services and other hardware devices used to host, manage and support 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 identifying and implementing 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.

OneStream

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

- Responsible for the implementation of logical access security software, infrastructure, and architectures to OneStream XF.
- Responsible for authorizing access for new internal and external users and to remove credentials when access is no longer authorized in OneStream XF.
- Responsible for the identification and authentication of internal and external users when accessing system components in OneStream XF.
- 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 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 and remediation of vulnerabilities, as well as reporting to appropriate personnel.
- Responsible for performing patching to the operating system and database and application changes to OneStream XF.
- Responsible for performing data back-ups.

United States Department of Agriculture

Control Objective 5 – Payroll and Leave Accruals, Control Objective 6 – Payroll Disbursements Control Objective 16 – Personnel Actions, and Control Objective 17 – 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.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information.

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.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information

mLINQS, LLC

Control Objective 1 – Obligations and Control Objective 2 – Disbursements

- 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.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information.

Salesforce

Control Objective 10 – Budget

- Responsible for restricting logical access, including privileged user accounts, to services and other hardware devices used to host, manage and support in oneARC.
- Responsible for performing patching to the operating system and database and application changes to oneARC.
- Responsible for maintaining physical access and environment controls for oneARC.
- Responsible for performing data back-ups for oneARC.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information.

Office of Personnel Management (OPM)

USA Staffing Onboarding

Control Objective 16 – Personnel Actions and Control Objective 17 – Payroll Documents

- 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.
- Responsible for maintaining business process controls associated with the complete, accurate, timely and authorized input, processing, and output of information.

IV. MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND KPMG LLP's TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

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 specified 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 .36 of Attestation Standards - Clarification and Recodification (AT-C) section 205, *Assertion Based Examination Engagements* (American Institute of Certified Public Accountants, 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.

40   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

FINANCIAL MANAGEMENT PROCESSING CONTROLS

Control Objective 1 – Obligations

Controls provide reasonable assurance that obligations are authorized, complete, accurate, timely processed, and 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 obligations.

<u>PRISM System Interface</u>

An obligation is created when a customer agency enters into a legally-binding contract with a vendor for goods or services. The obligation is entered into Oracle 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. PRISM has built-in controls that validate information provided by the customer agency and help ensure proper authorization is granted prior to the interface with Oracle. 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 help 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 releases require an analyst intervention, the analyst will be required to notate why the action was performed. Every business day separate analysts are responsible for executing and reviewing a report to identify all PRISM documents that were released the previous business day. Each document 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 analysts review a report created to recognize all newly created or modified obligations, within the previous five days, to verify documents have interfaced correctly to Oracle and represent the intended award amounts. Conversely, the same report identifies all Oracle obligations modified in the previous five days and verifies those amounts reconcile to PRISM. Obligation mismatches are independently reviewed by an analyst and action taken accordingly where necessary and

reconciliation actions are notated in the report. The action taken to complete the 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 send 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 help ensure submissions match authorization authority and adequate accounting information has been received, and manually enters the obligation into Oracle. Some obligations are submitted through the oneARC portal and the technicians input them into Oracle. Obligations posted in Oracle are available for both ARC and customer agency review through ad hoc OBI reports.

Temporary Duty Travel System Interface

ARC and customer agency travelers enter travel authorizations into ConcurGov and electronically route them to Approving Officials for review and approval. ConcurGov is a web-based, self-service travel system that utilizes a fully-automated booking process. ConcurGov uses system processes and audits to help ensure compliance to the FTR. ConcurGov is used to prepare, examine, route, approve and record travel authorizations and vouchers. Approving Officials electronically stamp the authorization with a status of "approved." ConcurGov prevents a user from self-approving travel authorizations unless they have authorized access.

SAP Concur's Enterprise Application Integration sends approved travel authorization data into Oracle and Oracle records the obligation, provided the accounting string for the obligation transaction is valid and funds are available.

Accepted files are loaded into Oracle as obligations in the general ledger. An OBI report is generated and reviewed to identify and correct data interface errors and exceptions between ConcurGov and Oracle. Transactions with errors are reviewed and manually entered into the financial system. Approved authorizations in ConcurGov are reconciled daily by ARC Travel Services with an OBI report to help ensure that all ConcurGov authorizations have been interfaced and processed into Oracle.

Relocation Travel System Interface.

The RSB personnel enter PCS travel authorizations into moveLINQ and electronically route them to Approving Officials for review and approval. Approving Officials 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."

Non-payment customer agencies receive a daily reconciliation report containing approved documents which have been electronically routed to their agency officials.

Payment customer agencies approved documents are interfaced daily via batch process to Oracle which records an obligation in the general ledger. In order to ensure that all moveLINQ authorizations have been interfaced and processed in Oracle an accounting technician performs a daily reconciliation that compares reports from both systems.

42   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

<u>Budget Execution System Controls</u>

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) are 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 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 documents 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.

43   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of obligations and determined the procedures were 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 Oracle.
3. Observed the PRISM Support Team Staff monitor the "Pending Financial Approval (Award)" and "Disapproved during Pending Financial Approval" reports and noted the reports were monitored, no backlogs existed, and no interface errors were identified.
4. For a selection of days, inspected that the report used to identify all PRISM documents released the previous business day and determined that they were reviewed and actions taken on any variances noted were reviewed by a supervisor.
5. For a selection of days, inspected that the report used to identify Oracle and determined that the obligation mismatches were reviewed and that actions were taken for documents identified on the report
6. For a selection of manually entered obligations and customer agencies, inspected the 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 that approved travel authorizations interfaced with Oracle and that Oracle recorded the obligation to the general ledger.
8. For a selection of days and customer agencies, inspected the ConcurGov to Oracle interface reconciliations and determined daily reconciliations were performed, any data interface errors or exceptions identified were corrected, any rejected transactions were manually entered into the Concur, and all approved travel authorizations were interfaced and processed by Oracle.
9. Observed a ConcurGov user who was 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 with Oracle.
10. Observed the daily moveLINQ interface and noted that approved relocation authorizations were interfaced with 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 and approved by the customer agency.
13. Observed an ARC user attempt to enter a transaction identification number that already existed and noted that Oracle issued an error message alerting the user of the duplication and automatically rejected the entry of a duplicate transaction number.

No exceptions noted.

44   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 2 – Disbursements

Controls provide reasonable assurance that non-payroll disbursements are complete, accurate, timely processed, and 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 award.

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 (FRB) of St. Louis 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 awards loaded for each supplier are also tied to the collector account. This limits the awards the vendor can view and invoice against. The current IPP configuration requires all invoices reference an approved award.

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

If the vendor submits the invoice through IPP it is automatically routed to the invoice approver designated on the award. This designation is made by the Contracting Officer on the award, which is interfaced with Oracle and then IPP. Awards 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 and they cannot route invoices to other users for approval. Only IPP invoices that were approved by the invoice approver or Contracting Officer for the award are interfaced with 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 Unique Entity Identifier (UEI) number (formerly the Data Universal Number System (DUNS) number) is assigned to the award at time of award. The banking information for the assigned UEI number is interfaced from System for Award Management (SAM) to Oracle.

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

45   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Non-IPP Customer Agency Invoice Approvals

Non-IPP invoices are either sent to ARC or to the customer agency. For 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 award 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.

Oracle controls set at the user identification and/or vendor level help 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 an accountant prior to disbursement.

A GLB accountant performs a 100% review of all foreign payments 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 help 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.

SmartPay Customer Agency Approvals

ARC processes disbursements for invoices that have been authorized by an Approving Official/Designee. When the approval window closes in the SmartPay 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

ARC and customer agency travelers enter travel vouchers into ConcurGov and electronically route them to Approving Officials for review and approval. ConcurGov is a web-based, self-service travel system that utilizes a fully-automated booking process. ConcurGov uses system processes and audits to help ensure compliance to the FTR. ConcurGov is used to prepare, examine, route, approve and record travel authorizations and vouchers. Approving Officials electronically stamp the voucher with a status of "approved." ConcurGov prevents a user from self-approving travel vouchers.

SAP Concur's Enterprise Application Integration sends approved travel voucher data into Oracle and Oracle records the disbursement provided the accounting string for the disbursement transaction is valid and funds are available.

Accepted files are loaded into Oracle as disbursements in the general ledger. An OBI Status Report is generated and reviewed to identify and correct data interface errors and exceptions between ConcurGov and Oracle. Transactions with errors are reviewed and manually entered into the financial system. Approved vouchers in ConcurGov are reconciled daily by an ARC Travel

46   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Services with an OBI report to help ensure that all ConcurGov vouchers have been interfaced and processed into Oracle.

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. This includes supplier household goods and other third party invoices, employee advances, and employee relocation travel reimbursements.

All third party invoices are examined by ARC to help ensure they are a complete and valid invoice. In addition, invoices are matched to the obligating documents and are certified by invoice approvers where applicable. The invoice approver certifies that the invoice is in accordance with the terms of the order. Employees and Agency Officials 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".

Non-payment customers receive a daily reconciliation report containing approved documents which have been electronically routed to their agency officials.

Approved documents for payment customers are interfaced daily via batch processing to Oracle which records a disbursement in the general ledger. Approved vouchers in moveLINQ are reconciled daily by an Accounting Technician with an Oracle generated report to help ensure that all moveLINQ vouchers have been processed in Oracle.

Oracle controls set at the user identification and/or vendor level help ensure that payment of 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.

ARC transmits EFT and check payment files to the Treasury for payment using SPS.

IPP Review

All invoices processed by IPP are subject to post payment audit. ARC reviews 10% of all invoices processed by IPP for each customer agency 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 award 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 award 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 help 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. Oracle user access profiles restrict accounting technicians' ability to process documents that require review and approval an accountant and help ensure proper segregation of duties is maintained. A 100% post payment audit review is conducted monthly on all invoices resulting in a payment of greater than $2,500 that was both processed and approved by the same individual.

47   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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. 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; and 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 a 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 SPS. An ARC Data Entry Operator (DEO) submits bulk files created in Oracle via drop zones to Fiscal Service's National Payment Center of Excellence. 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 certified in SPS to the payment files generated by Oracle to help ensure all approved invoices due for payment have been certified in SPS. 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 Oracle. 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 of SmartPay Activity

ARC accountants perform reconciliations of SmartPay 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:

48   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

- 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 cash disbursements by performing a month-to-date reconciliation of Treasury's cash disbursement activity in CARS 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 Oracle 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 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 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) are 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 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.

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.

49   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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

- Review the financial reports provided by ARC to help 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 documents to RSB for processing in moveLINQ in a timely manner.
- Ensure relocation documents are authorized and completely and accurately processed in their agency financial system 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 SmartPay charges and obtain Approving Official certification prior to auto-close.
- Provide post payment approval for SmartPay 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.
- Plan and monitor cash flow related to reimbursable authority to prevent overspending of cash.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing of disbursements and determined the procedures were 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 that the invoices successfully interfaced with Oracle and that new purchase orders for IPP vendors were successfully interfaced with IPP.
5. Observed the daily ConcurGov interface and reconciliation and noted that approved travel disbursements were interfaced with Oracle and that Oracle recorded the disbursements to the general ledger.
6. For a selection of days and customer agencies, inspected ConcurGov voucher reconciliations and determined that 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 that the system automatically prevented the approval. action.
8. Observed moveLINQ relocation vouchers interface with Oracle and noted that the approved vouchers interfaced via automated batch process.
9. For a selection of days, inspected moveLINQ vouchers and determined that the vouchers were reconciled by an Accounting Technician with an Oracle generated report.
10. Observed an accountant process an invoice over $2,500 and noted that 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 ARC's review of invoices of non-IPP invoices less than $2,500, and determined that the review performed was subject to random sampling by a lead accounting technician or an accountant for post payment review.
12. For a selection of months, inspected evidence of the 100% post audit management monthly review of invoices greater than $2,500 that had been processed and approved by the same individual, and determined all the invoices were reviewed by a supervisor.
13. For a selection of months and customer agencies, inspected ARC's review of 10% of all processed invoices by IPP and determined that the review was performed appropriately and discrepancies were resolved.
14. For a selection of weeks and customer agencies, inspected ARC's audit worksheets and determined that the quality sampling was performed, that audit worksheets were completed for selected vouchers and reviewed, and that any errors were followed-up on.
15. For a selection of months and customer agencies, inspected ARC's audit worksheets and determined that the statistical sampling was performed, that audit worksheets were completed for selected vouchers and reviewed, and that any errors were followed-up on.
16. For a selection of days, inspected the reconciliation performed by the ARC SPS certifying officer and determined that the number and dollar amount of payments reconciled from the SPS generated payment schedule to the payment files generated by Oracle, 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 stated otherwise).
18. For a selection of late payments, inspected invoices processed 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, reperformed the calculation of interest owed and determined Oracle calculated the Prompt Payment interest accurately.
20. For a selection of months and customer agencies, inspected the reconciliation of SmartPay activity and determined that the reconciliations were performed, reviewed, and that any differences were resolved.
21. For a selection of months and customer agencies, inspected reconciliations and determined that accountants performed reconciliations of the CARS Account Statements and Undisbursed Appropriation Account Ledger Reconciliations and that supervisory reviews were completed.

51   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

22. For a selection of customer agencies, inspected their budget execution settings in Oracle and determined that the settings were input in Oracle by USB staff, reviewed by a supervisor for completeness and accuracy, and annually reviewed with the customer agency.
23. For a selection of quarters and non-Treasury customer agencies, inspected the Intra-governmental Certified Explanation of Balances completed by ARC accountants and determined a) reconciliations of fiduciary 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 and Treasury customer agencies, inspected the non-fiduciary transaction confirmations completed by ARC accountants and determined that reconciliations of transactions and balances with trading partners were completed, that any necessary adjustments were identified and recorded, and that elimination reporting was completed using the TIER reporting process.
25. Observed an ARC user attempt to enter a transaction identification number that already existed 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.

52   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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

Controls provide reasonable assurance that unfilled customer orders, receivables, and cash receipts are complete, accurate, timely processed, and 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 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 cash receipts by performing a month-to-date reconciliation of Treasury's cash receipt activity in CARS to the Oracle 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

53   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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 a customer 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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.
- Plan and monitor cash flow related to reimbursable authority to prevent overspending of cash.
- Ensure that the Chief Financial Officer 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, cash receipts, and receivables and determined the procedures were documented.
2. For a selection of unfilled customer orders, inspected customer agency approvals and determined the unfilled customer orders were only processed by ARC after being approved by the customer agencies.
3. For a selection of receivables, inspected customer agency approvals and determined the receivables were only processed by ARC after being approved by the customer agencies.

54   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

4. For a selection of cash receipts, inspected customer agency approvals and determined the cash receipts were only processed by ARC after being approved by the customer agencies.
5. For a selection of months and customer agencies, inspected reconciliations and determined that accountants performed reconciliations of the CARS Account Statements and Undisbursed Appropriation Account Ledger Reconciliations and that supervisory reviews were completed.
6. For a selection of quarters and customer agencies, inspected the TROR reports completed by ARC accountants and determined that: 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 and non-Treasury customer agencies, inspected the Intra-governmental Certified Explanation of Balances completed by ARC accountants and determined: a) reconciliations of fiduciary 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 and Treasury customer agencies, inspected the non-fiduciary transaction confirmations completed by ARC accountants and determined that reconciliation of transactions and balances with trading partners was completed, that any necessary adjustments were identified and recorded, and that 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 issued an error message alerting the user of the duplication and automatically rejected the entry.

No exceptions noted.

55   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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 either picked up by ARC designated accounting technicians at the mailroom or sent to the A3F mail drop by the mail deliverer and signed for by an ARC designated accounting technician if delivery confirmation was requested. The ARC designated accounting technician (who does not have Oracle access to post accounts receivable transactions) receives, opens, and logs all checks received in 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 entering the date in the "Date Received" 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 FRB Cleveland 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

56   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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 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 did not have Oracle 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 to OTCnet and determined the total checks were posted completely and accurately to Oracle.
6. Inspected a selection of check deposits and determined they were deposited and recorded in Oracle by an ARC staff member other than the individual who processed the deposit.

No exceptions noted.

57   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 5 – Payroll and Leave Accruals

Controls provide reasonable assurance that payroll and leave accruals are complete, accurate, timely processed, and documented in accordance with ARC policies and procedures.

Description of Controls

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

System Calculation of Accruals

Monthly payroll accruals are recorded and reviewed on a monthly basis by a payroll accountant and reversed in the subsequent accounting period. The monthly payroll accruals are subsequently reviewed and approved by a supervisor. The payroll accrual is a prorated calculation performed by Oracle. To make its calculation, Oracle 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, and quarterly) and reversed prior to recording the next scheduled leave accrual. The leave accrual calculation is performed by Oracle based on data provided by the customer agency's payroll service provider. To make its calculation the Oracle requires a payroll accountant to enter specific parameters (e.g., pay period and pay year).

Complementary Customer Agency Controls

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

- Review the financial reports provided by ARC to help ensure that monthly payroll and leave accruals are complete and accurate.
- Review and confirm the 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 documented for the processing of payroll and leave accruals.
2. For a selection of months, inspected a selection of customer agencies' monthly payroll accrual reports and determined that the customer agencies' monthly payroll accruals were documented, entered timely and accurately, and reviewed monthly by an ARC accountant.
3. For a selection of months, inspected a selection of customer agencies' leave accruals and determined the leave accruals were documented, entered timely and accurately, and reviewed monthly by an ARC accountant.

No exceptions noted.

58   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 6 – Payroll Disbursements

Controls provide reasonable assurance that payroll disbursement data (disbursed by a third-party) are complete, accurate, timely processed, and 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 detail payroll data to Oracle and summary journal entries to the general ledger. The payroll accountant reviews a report and corrects all of the transactions that did not properly interface with the system. The payroll accountant contacts the customer agency 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 cannot 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 and supervisors review a reconciliation of payroll disbursements recorded in Oracle and payroll disbursements as reflected in Treasury's cash systems. The payroll accountant investigates and resolve 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance to:

- Verify that payroll processed by third-party providers is complete and accurate.
- Review the financial reports provided by ARC to help ensure that payroll disbursements are complete and accurate.
- Review and confirm ARC customer agency 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 documented for the processing of payroll disbursements.
2. For a selection of pay periods and customer agencies, inspected interface errors reports and determined during the interface, that input files were checked for errors and errors were corrected.

Management of Administrative Resource Center's Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Tests

3. For a selection of months and customer agencies, inspected reconciliations of the payroll disbursements recorded in Oracle to the payroll disbursements as reflected in Treasury's cash systems and determined that: 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.

60   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 7 – USSGL

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

<u>Description of Controls</u>

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

<u>Transaction Set-up Controls</u>

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), the ARC USSGL Team will communicate the appropriate changes to ARC Oracle system administrators to help ensure the accounting transaction posting models are revised.

<u>General Ledger Account Reconciliations</u>

Accountants perform general ledger account reconciliations (utilizing Oracle, Excel, or other source files as subledger) on balance sheet accounts to help 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 help 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.

<u>GTAS Edit Checks</u>

ARC submits the GTAS files for its non-Treasury customers, except for the DHS, 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 based on USSGL attributes 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 rejects any Treasury Appropriation Fund Symbol (TAFS) that fails the validations or edit checks. ARC investigates and resolves any TAFS failed by the GTAS system.

61　　*Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Treasury Information Executive Repository Validation Checks

For Treasury and DHS customer agencies, GTAS reporting requirements are met using TIER. TIER is a Treasury and DHS 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 Changes in Net Position (SCNP)* 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 Budgetary Resources (SBR)* 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 XF tables to determine compliance with the TFM reporting requirements. ARC investigates and resolve any differences between TFM crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Treasury and DHS 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 the 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 Treasury and DHS 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 *SCNP* during the third and fourth quarters for review by a supervisor and submission to OMB. During the fourth quarter the *SBR* and *SCA* are also included in the supervisor review and submission to OMB. For customer agencies using OneStream XF, there are additional checks to compare the OneStream XF trial balance to the Oracle trial balance and GTAS balances.

Financial Statement Variance Analysis

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

For non-Treasury and non-DHS customer agencies, accountants prepare a third and fourth 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance to:

- Review and approve, prior to submission, the financial reports prepared by ARC to help ensure that reports prepared for external use are complete, accurate, and submitted in a timely manner.
- Ensure that the variance analyses are reviewed and approved by Treasury and DHS's CFO or designee in support of financial reports' completeness, accuracy and timely submission for external use.

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 documented.
2. Observed the processing of a transaction to an inappropriate USSGL account and noted the Oracle cross-validation rules rejected the transaction.
3. Inquired of management and inspected a list of users with access to change posting models and determined that user access to make changes to models was restricted based on valid job responsibilities.
4. For a selection of newly established posting models, inspected ARC supervisory approvals of the new posting models and TFM/USSGL guidance and determined the new posting models were authorized and were in agreement with TFM/USSGL guidance.
5. Inspected ARC's confirmation of the annual review of USSGL account titles and descriptions and determined the supervisory accountant performed the annual review of USSGL account titles and descriptions.
6. For a selection of months and customer agencies, inspected the budgetary-to- proprietary account relationship reconciliations completed by ARC accountants and determined that: the 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 noted Oracle executed edit checks on the data based on USSGL attributes 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 performed USSGL validations and no failures were identified.
9. For a selection of months and 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 and 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 and customer agencies, inspected the reconciliations of the financial statements prepared by ARC to the general ledger and determined that the reconciliations were performed and reviewed by a supervisor and that any differences noted are resolved.

12. For a selection of quarters and customer agencies, inspected the financial statement variance analyses and determined that they were reviewed by ARC supervisory accountants and approved by the bureau CFOs or designees prior to being submitted to the Department.

No exceptions noted.

64   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 8 – Period-End Accruals

Controls provide reasonable assurance that the period-end accruals are complete, accurate, timely processed, and documented in accordance with ARC policies and procedures.

Description of Controls

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

Revenue and Expense Accruals

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.

Non-Invoice Accruals

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.

General Ledger to Subledger Reconciliation

On a monthly basis, ARC accountants prepare a reconciliation of revenue and expense accrual balances in the general ledger to the subledger detail, which is reviewed by a supervisor. For customers using OneStream XF, the general ledger to subledger reconciliations are automated. Accountants reconcile only billed revenue accruals since unbilled revenue accruals are recorded directly in the general ledger. Any differences identified are corrected by an accounting technician or accountant in the subsequent accounting period.

Budget Execution System Controls

Customer agencies can establish and monitor both legally established and internally developed budget plans in Oracle to help 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) are 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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 help 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 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 documentation of revenue and expense accruals and determined the accounting technicians followed the instructions provided from the customer agencies and the Oracle entries were reviewed and approved by supervisory accountants and processed timely.
3. For a selection of customer agencies, inspected manual journal entry templates of the year-end payroll accrual data loaded into Oracle and determined the entries were imported successfully, reviewed, and posted to the general ledger.
4. For a selection of quarters and customer agencies, inspected manual journal entry templates of the non batch leave accrual data loaded into Oracle and determined the entries were reviewed and approved by a supervisory accountant.
5. For a selection of months and customer agencies, inspected the reconciliation of revenue and expense accrual balances in the general ledger to the subledger detail and determined that any

66   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

differences noted were corrected by an accounting technician or accountant in a subsequent accounting period and that they were reviewed by a supervisor.

6. For a selection of customer agencies, inspected their budget execution settings in Oracle and determined the settings were input in Oracle by USB staff, reviewed by a supervisor for completeness and accuracy, and 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.

67   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 9 – Governmentwide Reporting

Controls provide reasonable assurance that Governmentwide reporting is complete, accurate, timely processed, 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

GTAS is a web-based system for use in the Governmentwide reporting 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 DHS, supervisory accountants review all submissions prepared by accountants and review all data to help ensure 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 DHS customer agency is required to submit financial accounting and budgetary data each month to TIER, DHS's data warehouse, within DHS'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 help 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 customer agencies following Treasury guidelines. Independent accountants or analysts review all reports.

Financial Statement Crosswalks

ARC accountants prepare a *BS, SNC, and SCNP* 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 *SBR and SCA* (when applicable) for all customer agencies. ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream XF table to help ensure compliance with the reporting requirements. ARC investigates and resolve any differences between TFM crosswalks and ARC's internally prepared financial statements.

Financial Statement Review

For Treasury and DHS 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.

68   *Management of Administrative Resource
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests*

The *SBR 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 *SCNP* during the third and fourth quarters for review by a supervisor and submission to OMB. During the fourth quarter the SBR and SCA may also be included in the supervisor review and submission to OMB. For customers using OneStream XF, there are additional checks to compare the OneStream XF trial balance to the Oracle trial balance and GTAS balances.

Financial Statement Variance Analysis

For both Treasury and DHS customer agencies, ARC 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 DHS bureau variance is also approved by the DHS's CFO or designee.

For non-Treasury and non-DHS customer agencies, ARC accountants prepare a third and fourth 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 requests 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 monthly basis. For those customer agencies, three files are submitted to the governmentwide DATA Act Broker system (Broker) on a monthly basis. The Broker has validation checks with the GTAS submissions. The accountants review the reports produced by the Broker to verify that all three files have been successfully reconciled and passed all validation checks. Upon completion of the accountants' review, a monthly reconciliation package is sent to the customer agency for review and approval. Upon receipt of the customer agency monthly attestation, ARC updates the status of the monthly DATA Act Files submission to "Published" on behalf of the customer agency. On a quarterly basis, the customer agency provides certification approval for all three monthly DATA Act submissions. ARC updates the status of the three monthly DATA Act File submissions to "Certified" on behalf of the customer agency.

69   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Complementary Customer Agency Controls

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

- Review and approve the annual submission of the TROR and Debt Collection Activities report.
- Provide certification of GTAS to ARC prior to system certification.
- Ensure that the CFO certify that the TROR and Debt Collection Activities report submitted to the Treasury is accurate and consistent with agency accounting systems.
- Ensure that the variance analyses are reviewed and approved by Treasury and DHS's CFO or designee in support of financial reports' completeness, accuracy and timely submission for external use.
- Review and provide authorization of DATA Act files prior to submission.

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 quarters and customer agencies, inspected the quarterly GTAS submissions and determined selected submissions were reviewed and certified.
3. For a selection of months and 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 and customer agencies, inspected the corresponding supervisory accountant review of the Prompt Payment reports and determined they were reviewed before submission.
5. For a selection of quarters and customer agencies, inspected the reconciliation of customer agencies' financial statements prepared by Treasury 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 and customer agencies, inspected the financial statement variance analyses and determined they were reviewed by an ARC supervisory accountant prior to being submitted to the Department.
7. For a selection of quarters and customer agencies, inspected the TROR and Debt Collection Activities Reports and determined the reports were reviewed by an ARC supervisory accountant.
8. For a selection of quarters and customer agencies, inspected results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements and determined such comparisons were performed and ARC investigated and resolved any differences.
9. For a selection of quarters and 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 and Treasury customers, inspected supporting documentation and determined the customers' monthly DATA Act submissions were appropriately completed, reviewed, and timely submitted in TIER as required.

70   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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

No exceptions noted.

71   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 10 – Budget

Controls provide reasonable assurance that budget entries are complete, accurate, timely processed, and documented 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) are 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.

72   *Management of Administrative Resource
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests*

<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 help 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 cash disbursements by performing a month-to-date reconciliation of Treasury's cash disbursement activity in CARS to the Oracle 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 Oracle by an accounting technician or another accountant who neither prepared nor reviewed the FBWT reconciliation.

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

- Review the financial reports provided by ARC to help 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 help ensure that OMB directed apportionment limits are not exceeded.

- Routinely review authorizations within oneARC to confirm that only authorized users are submitting budget template requests on behalf of the agency.
- Plan and monitor cash flow related to reimbursable authority to prevent overspending of cash.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for the processing budget entries and determined that the procedures were documented.
2. For a selection of customer agencies, inspected their budget plan execution settings in Oracle settings and determined that the settings were input in Oracle by USB staff, reviewed by a supervisor for completeness and accuracy, and annually reviewed with the customer agency.
3. For a selection of months and 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.
4. For a selection of months and customer agencies, inspected reconciliations of CARS Account Statement balances to general ledger FBWT balances and determined accountants performed the reconciliations, the reviews were completed by staff other than the individuals who performed the reconciliations, and differences were resolved.
5. 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.

74   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 11 – Manual Journal Entries

Controls provide reasonable assurance that manual journal entries are authorized, completely and accurately posted, and documented in accordance with ARC policies and procedures.

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 XF determines whether or not the user can prepare and/or approve a manual journal entry. OneStream XF system controls require all manual JEs are approved by a supervisor. Once a user has entered a journal entry in OneStream XF 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 XF 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 XF manual JEs. OneStream XF 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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 documented.
2. Inspected the list of Oracle users with the ability to create manual JEs and determined that they were assigned a supervisor in Oracle and were subject to the automated approval workflow.

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

No exceptions noted.

Control Objective 12 – Federal Investments

Controls provide reasonable assurance that federal investments in Government Account Series (GAS) securities are authorized, complete, accurate, timely processed, and 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 identification (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 USSGL accounts are reconciled between Oracle and FedInvest to help 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 a supervisory ARC accountant. If discrepancies exist with either reconciliation, research is conducted to determine the cause, adjust investments if necessary, and document corrective actions.

77   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Complementary Customer Agency Controls

Customer agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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 customer 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 receipt or disbursement activity that may impact investments.
- Communicate to ARC any larger than normal receipt or 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 documented, provided to ARC and defined the investment objectives for the agencies.
2. For a selection of investment purchases, inspected investment purchase review documentation and determined the investment purchases were reviewed and processed timely by ARC staff other than the individual who processed the investment purchase.
3. For a selection of days, inspected reconciliations of investment account transactions within InvestOne to the general ledger dollar amounts recorded in Oracle and determined the investment activity in GAS securities from InvestOne was recorded in the Oracle general ledger and the amounts reconciled between the two systems.
4. For a selection of months and customer agencies, inspected the investment reconciliations and determined 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 the FedInvest user access listing and related access request forms and determined the forms were completed, access was authorized, and authorized access matched that which was configured in FedInvest.
6. For a selection of days, inspected the daily reconciliation of 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.

78   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 13 – Supplier and Bank Records Changes

Controls provide reasonable assurance that changes to supplier and bank records are authorized, complete, accurate, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures related to supplier and bank record 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 Oracle 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 agency auditors should determine whether customer agencies have established controls to provide reasonable assurance 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 documented.
2. Inspected a list of Oracle users with role access to update, modify, or delete Supplier and Bank records and their corresponding job titles, and determined users had the appropriate privileges as they were commensurate with their roles and responsibilities.
3. Inspected a list of Oracle users with role access to process vendor payments and determined that no users have access to both process vendor payments and update, modify, or delete Supplier and Bank records.

79   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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 14 – Acquisitions and Contracts

Controls provide reasonable assurance that acquisitions are made by an authorized contracting officer who certifies the award is complete, accurate, and documented in accordance with ARC policies and procedures.

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 the award document, vendor matrix, award summary, and procurement checklist, and determined that the award was signed by an authorized Contracting Officer to certify that the documents were complete and accurate, met procurement and regulatory requirements, and was within their approval threshold.

No exceptions noted.

81   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 15 – Sufficiently Funded Requisitions

Controls provide reasonable assurance that award requisitions are approved and supported by sufficient funding.

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 from being made without sufficient funding. Additionally, in support of the DATA Act, PRISM's control features help 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 procurement award from being made.

No exceptions noted.

82   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

HUMAN RESOURCES PROCESSING CONTROLS

Control Objective 16 – 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

ARC has documented procedures for staff to follow for the processing of personnel actions that have been delegated to them by the customer agencies.

HRConnect is a 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 with 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. An EBB Specialist reviews the hire to determine eligibility for Retirement, Federal Employees Health Benefits (FEHB) and Federal Employees' Group Life Insurance (FEGLI), and provides the information via PAPB's database or the USA Staffing Onboarding system. A PAPB HR Assistant then utilizes the New Hire Checklist, and other supporting documentation, to code and release the personnel action in HRConnect. The PAPB HR Assistant verifies the action applied in NFC and a different PAPB HR Assistant verifies the information in NFC is correct. The PAPB 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 PAPB HR Assistant, along with assistance from the PAPB HR Specialist, resolve any issues that stopped the action from applying or applying properly. After NFC's PAYE runs, the PAPB 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 PAPB HR Assistant or PAPB 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 PAPB:

83   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

- 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.) Depending on level of experience, an EBB HR Specialist reviews, codes, and routes the action to PAPB. 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 PAPB.
- Removal and non-transfer Termination (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 PAPB. (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 PAPB.)
- For all other separations, a PAPB HR Assistant determines the type of separation and codes the personnel action for review and approval by a PAPB HR Specialist.

After a separation is coded and approved, it is reviewed and released from HRConnect by a PAPB HR Assistant. The PAPB HR Assistant verifies the action applied in NFC and a different PAPB HR Assistant verifies the information in NFC is correct. If the action does not apply or apply correctly in NFC, the PAPB HR Assistant, along with assistance from the PAPB HR Specialist, resolve any issues that stopped the action from applying or applying properly. After PAYE runs, the PAPB 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 a customer agency's internal approvals before routing to ARC HR. Depending on the type of personnel action, ARC HR staff in ESD, PAPB, 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 PAPB. (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 PAPB.)
- Leave Without Pay (LWOP) and RTD actions related to a workers' compensation claim are reviewed, coded, and approved by a LAB Workers' Compensation Specialist. The Specialist then forwards the personnel action to PAPB. (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 are added to the action by PAPB.)
- All personnel actions related to Pathways employees are reviewed and coded by a PAPB HR Assistant. The PAPB HR Assistant forwards the personnel action to an ESD Specialist for final review and approval.

Management of Administrative Resource Center's Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Tests

- All reorganizations are reviewed and coded by a PAPB HR Specialist. The PAPB HR Specialist forwards the personnel action to an ESD Specialist for review and approval.
- All other actions are reviewed and coded by a PAPB HR Assistant. The PAPB HR Assistant forwards the personnel action to an authorizing official, depending on the type of action, for final review and approval.

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

Most awards are routed through an agency's internal approvals and then released directly to NFC using HRConnect's award bypass functionality. No additional reviews or approvals are done by ARC HR. However, there are some customer agencies that provide their performance (ratings based) awards to ARC HR on spreadsheets to be uploaded directly into HRConnect by a PAPB HR Specialist. After the spreadsheet has processed the HR Specialist performs spot checks to help ensure the spreadsheet processed correctly.

FEGLI

All FEGLI elections are initiated via a SF-2817, Life Insurance Election form received within the USA Staffing Onboarding system or outside the system (fax, email, USPS, etc.). An EBB HR Assistant (an EBB HR Specialist if the employee is reemployed annuitant) verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. If a FEGLI election results from a qualifying life event (QLE), an EBB HR Assistant requests documentation to verify the employee's eligibility. For the forms received outside of the Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the Onboarding system, the election electronically transmits to HRConnect. For all forms the EBB HR Assistant 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.

Complementary Customer Agency Controls

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

- Help 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 documented.
2. For a selection of new employee personnel actions in HRConnect, inspected relevant documentation and determined that new employee personnel actions were documented, reviewed, authorized, and correctly applied.
3. Inspected 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, 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.

86   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 17 – 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

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

HRConnect is a human resources system for multiple federal agency customer agencies. 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 with Oracle.

Payroll documents include direct deposit information for net pay and allotments, federal and state withholding, union dues, health insurance elections, Thrift Savings Plan (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.

FEHB and TSP Contributions

FEHB and TSP elections are employee-initiated via the appropriate form or via EPP. When elections are received via a form, an EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist. For FEHB elections that are a result of an initial enrollment opportunity or QLE that contain dependents, an EBB HR Assistant requests documentation to verify eligibility. For any dependent being added to an FEHB plan, an EBB HR Assistant obtains verification documentation and notes it on the form. 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. (Note: Payment is optional. If the employee elects payment, it is made through NFC's Special Payroll Processing System (SPPS)).
- 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.

87   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

A LAB HR Specialist enters and releases the payroll document in EPIC. After PAYE runs, the LAB HR Specialist verifies that the employee was paid for the unused leave or compensatory time.

All Other Payroll Documents

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 PAPB and EBB staff, as applicable. Each error is reviewed and resolved prior to PAYE running for the pay period.

Payroll documents for new hires are submitted in writing to PAPB, as part of the on-boarding process. A PAPB HR Assistant inputs and releases the payroll documents in HRConnect. The PAPB HR Assistant verifies the payroll documents applied in NFC and a different PAPB HR Assistant verifies the information in NFC is correct. If the payroll documents do not apply or apply incorrectly in NFC, the PAPB HR Assistant, along with assistance from a PAPB HR Specialist, resolve any issues. After PAYE runs, the PAPB HR Assistant who processed the payroll documents confirms that the employee was paid correctly by verifying the information in PINQ.

In rare cases, current employees submit requests for changes and/or deductions in writing to PAPB. A PAPB Processing Call Center Assistant reviews the request and contacts the employee if more information or additional verification is needed. The PAPB Processing Call Center Assistant inputs and releases the request in HRConnect. The PAPB Processing Call Center Assistant verifies the action applied in NFC and a different PAPB Processing Call Center Assistant verifies the information in NFC is correct. After PAYE runs, the PAPB Processing Call 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 documented.
2. For a selection of FEHB and TSP elections and customer agencies, inspected the FEHB and TSP election forms and determined the forms were verified, reviewed, and certified by an EBB Specialist and that 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 the approval forms, payment reports, timecards, and verification payments and determined that approvals were obtained, criteria were met, and the employee was appropriately paid.
4. For a selection of written employee requests for payroll changes and/or deductions submitted to PAPB for a selection of customer agencies, inspected approval forms, payment reports, timecards, and verification payments and determined the request was verified and correctly applied.

No exceptions noted.

88   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

GENERAL COMPUTER CONTROLS

Control Objective 18 – 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, PRISM, webTA, ConcurGov, moveLINQ, IPP, OneStream XF, 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 and OBI

Access to Oracle and OBI are restricted to users through the use of multifactor authentication (MFA). MFA is accomplished utilizing PIV credentials or ID.me. Oracle and OBI 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 and OBI 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 and/or OBI. 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 users' access is monitored and end dated after 90 days of inactivity by an RPA. ARC Oracle system administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. Annually, 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. For OBI, data access is restricted by assignment of Role Groups to determine the type of data (Financial, PRISM, Payroll) and Virtual Private Network (VPN) Groups to limit the type of data specific to the end user.

Only the SYSADMIN account controlled by OMCS is assigned the system administrator responsibility in the Oracle application. The Customer Support Division (CSD), Operation Support

89   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Division (OSD) and Systems and Project Support Division (SPSD) employees are assigned ARC Oracle application administrator responsibility in the Oracle application. The employees with the ARC Oracle 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 subsequently approved by a supervisor or manager. Additionally, the individuals with ARC Oracle 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 ARC Oracle application administrator from adding or removing any responsibilities from their own user ID.

The SDB/Procurement and Accounting Support Branch (PASB)/Reporting and Technology Support Branch (RTSB)/DSB managers can be assigned the ARC Oracle 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 OMCS server and database administrators.

User IDs are assigned to internal and external users by an ARC Oracle system administrator. To access the application, users must authenticate their session utilizing MFA.

PRISM

Access to PRISM is restricted to users through the use of MFA. MFA is accomplished utilizing Common Approach to Identity Assurance (CAIA) that includes: PIV credentials, derived PIV, Login.gov, or ID.me. 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 users' access is monitored and end dated after 90 days of inactivity by an RPA. ARC PRISM system administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. Annually, ARC generates an OBI 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 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.

90   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

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 CSD'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 CSD'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 OMCS server and database administrators and specific CSD/OSD/SPSD employees.

User IDs for both internal and external users are assigned by an ARC PRISM system administrator. To access the application, users must authenticate their session utilizing MFA.

webTA[2]

Access to webTA was restricted to users through a valid login ID and password or MFA until March 2023 at which time only MFA is permitted. MFA is accomplished utilizing Common Approach to Identity Assurance (CAIA) that includes: PIV credentials, derived PIV, Login.gov, or ID.me. 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 LAB HR administrator creates the user's profile based on information in the personnel action.

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.

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 LAB codes the exiting employee's timecard as "Final" and deactivates the employee's webTA access.

Annually, an HR administrator in the HR Systems Help Desk 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 helps to ensure that these employees who do not currently validate or approve time on a regular basis still require their role as a timekeeper or supervisor.

---

[2] The scope of the description of webTA controls applies only to full service webTA customer agencies.

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 MFA. MFA is accomplished utilizing PIV credentials. 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 Supplier Entry 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. 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 help ensure strong password security. Access privileges are granted in accordance with the concept of least privilege required.

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.

ConcurGov has separate permissions that are assigned to users that enforce separation of duties.

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 customer agencies.
  - 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 Common Approach to Identify Assurance (CAIA) system
    - The logon screen will accept
      - PIV credentials

92   *Management of Administrative Resource
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests*

- ID.me
  - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
  - The CAIA system provides three records of identity, if those match what is in moveLINQ for the account user; they have been configured for Employee portal access.
  - Users 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.
  - Users 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 agency 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 administrator that added the user and the reviewing moveLINQ administrator.
  - Access is granted through the Fiscal Service CAIA system.
    - The logon screen will accept PIV credentials only.
    - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
    - The CAIA system provides three records of identity, if those match what is in moveLINQ for the account user; 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. Access to records is controlled through organization access and/or workflows assigned.
    - 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.
  - 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 administrator that added the user, and the reviewing moveLINQ Branch Manager or System Owner (SO).
  - Access is granted through the Fiscal Service CAIA system.
    - The logon screen will accept PIV credentials only.
    - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.

93   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

- The CAIA system provides three records of identity, if those matches what is in moveLINQ for the account user; 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.

Invoice Processing Platform

Access to IPP is restricted to users with a valid logon ID and password or MFA. MFA is accomplished utilizing PIV credentials. Internal and external users must complete, sign, and submit an approved Administrative Resource Center System Access Form for End User Applications. Customer agency users with the role of approver 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 access form is either signed by or approved via email by one of the customer agency authorized system access approvers listed on the customer agency Delegation of Authority form. Once the IPP access account is created, the user receives one e-mail with a user ID and another 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 to confirm the ongoing appropriateness of the customer agency's IPP users. Then ARC certifies the results in the Shared Document with Secured Access (SDSA) that is operated by FRB St. Louis. Lastly, ARC returns the certified 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 and access is restricted in accordance with the concept of least privilege required:

- Administrator
- Approver
- Processor
- Viewer

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

OneStream XF

Access to OneStream XF was restricted to users with a valid logon ID and password until MFA was implemented at the end of June 2023. MFA is accomplished utilizing PIV credentials or ID.me. Prospective OneStream XF users must complete, sign, and submit an approved Administrative Resource Center System Access Form for End User Applications to request access to OneStream

XF. 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 XF. 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 XF user access is end-dated in the system to remove their access within 48 hours. OneStream XF end users' access is monitored, and end dated after 60 days of inactivity by an RPA. ARC OneStream XF system administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. Annually, 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.

OneStream XF 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 agency's data) and roles assigned.

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

The SDB/USB/RTSB/PSS managers can be assigned the system administrator responsibility in situations where the manager deems the access is required. This responsibility is granted on a temporary basis with the proper request and approval and will be end-dated once the access is no longer necessary.

User IDs for OneStream XF are assigned by an ARC OneStream XF 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 help ensure strong password security.

OneStream XF 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. An RPA reviews the log and sends the e-mails out to the users.

HRConnect

Users access HRConnect via MFA. MFA is accomplished utilizing PIV credentials or login.gov. 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. 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

95   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

access specifications, which will allow the user to perform his/her duties in HRConnect. Changes to existing elevated access requires 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 Applications 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.

Semi-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. The analyst on the HR Systems Help Desk also performs a similar semi-annual review for users with administrative roles.

USA Staffing Onboarding

Access to USA Staffing Onboarding is restricted to users through the use of MFA. MFA is accomplished utilizing PIV credentials. USA Staffing Onboarding employees are given access when they accept the tentative job offer. Users that require elevated access (e.g., admin, and HR 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 USA Staffing Onboarding. Changes to existing elevated access requires a new access form to be submitted by the customer agency.

Semi-annually, an analyst on the HR Systems Help Desk sends out a list of users with elevated roles 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. In order to remove a user's USA Staffing Onboarding access, customer agencies submit a request for account termination. At that time, the USA Staffing Onboarding user's access is disabled in the system.

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 ESM/ServiceNow to initiate the installation of the RPA software and it must be approved by management within the CSD. 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 in turn grants access to the restricted shared network drive location where the license keys necessary to access the RPAs are stored. Access to AD groups is reviewed annually.

Access and roles for the Production region of the KOFAX Management Console is restricted via LDAP groups. A Service Request must be submitted within ESM/ServiceNow to initiate adding a user to the applicable LDAP group, which must be approved by management within the CSD. 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 DAB are granted a similar role in

96   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

production, which is a view only role that does not allow for the upload, scheduling/execution of RPAs, or configuration changes.

When a DAB employee separates from the branch, access termination is initiated. Service Requests must be submitted within the ESM/ServiceNow to initiate the uninstallation of the RPA software, removal of the user from the RPAdmin Active Directory (AD) group, and removal of the user from the applicable RPA LDAP group. Each ticket must be approved by management within the CSD. ISS is responsible for uninstalling the software for individual users, removing users from the RPAdmin AD group, and removing users from the applicable RPA LDAP group with an approved Service Request. Quarterly a review of the access to the KOFAX Management Console and LDAP is performed.

oneARC

Access to oneARC is restricted to users utilizing MFA. MFA is accomplished utilizing PIV credentials, login.gov or ID.me. All logons/sessions are encrypted to protect the information, making it unintelligible to all but the intended users. New oneARC users must complete, sign, and submit an approved Administrative Resource Center System Access Form for End User Applications to request access to oneARC. 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 oneARC. Changes to existing user profiles can be achieved in two ways. An e-mail can be sent to the oneARC notifications mailbox by an authorized individual requesting the change and defining what access should be added/deleted/changed. The second method is that the exact same points of contact at each agency can use the Self Service authorizations mechanism that is built inside oneARC. In order to remove a user's access there are also multiple ways this can be accomplished. First, removing an employee's PIV card will restrict access. Second, customer agencies submit a request for account termination. At that time, the user's access is terminated in the system by a oneARC administrator. Third, using the Self Service Authorizations mechanism in oneARC, authorization officials at each customer agency can remove the ability for a user to submit requests.

OneARC uses an Agile project development approach for its configuration management. This means that the oneARC team has the ability to load batches of new users and permissions for existing users (internal and external) for each new module during Go Live. The load sheets are prepared by comparing current Delegation of Authority listings and email submissions to the responsible group mailbox for the workflow oneARC is automating. These load sheets are prepared from lists provided from the accounting area. Customer agencies or internal management then do a complete review of all users (previously loaded ones, and new ones) that may need access. Once they are approved by the customer agencies or internal management for that area they are then loaded into oneARC. If a user is not on this list they must complete the System Access Form mentioned above. Each new user is assigned to a customer agency and provided access to one of three roles as determined by the customer agency authorizing official. The three roles are User, Executive, or Manager.

Once a user is created, a customer agency authorizing official provides the necessary authorizations for the employee to submit requests. Authorization officials at each agency are identified during the project phases tied to each area. Authorization officials are not able to approve their own access (so each agency has a minimum of two authorization officials). Internal employees' access is tied to a permission set that allows them to work customer cases. To modify an internal user's access,

97   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

FS Form 5409 form must be filled out. User modifications occur via the same methods above: Self Service Authorizations, emails from the Authorization officials, and FS Form 5409 forms.

Reports on authorizations are available upon demand to the appropriate customer points of contact. An admin can also run reports on agency authorizations, including when they were submitted and approved. All administrator actions can be exported as necessary.

Complementary Customer Agency Controls

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

- Review and approve listings of users with current Oracle, OBI, PRISM, webTA, ConcurGov, IPP, OneStream XF, and HRConnect access to help ensure appropriateness and provide changes to ARC in a timely manner.
- Notify ARC timely regarding separating employees.
- Notify ARC timely of any changes to HRConnect authorized approvers.
- Help ensure all personnel actions are submitted in HRConnect timely.
- Routinely review approvers within oneARC to confirm that only authorized users and responsibilities are executing actions and approvals.

Tests of Operating Effectiveness and Results of Testing

1. Inspected written procedures for system access additions and terminations for Oracle, OBI, PRISM, webTA, ConcurGov, IPP, moveLINQ, OneStream XF, HRConnect, USA Staffing, and oneARC and determined procedures were documented.
2. Inspected the Oracle user account management procedures and determined procedures were documented for Oracle.
3. Inspected the PRISM user account management procedures and determined procedures were documented for PRISM.
4. Inspected both the webTA user account management procedures and password procedures and determined procedures were documented for webTA.
5. Inspected both the ConcurGov user account management procedures and password procedures and determined procedures were documented for ConcurGov.
6. Inspected the moveLINQ user account management procedures and determined procedures were documented for moveLINQ.
7. Inspected both the IPP user account management procedures and password procedures and determined procedures were documented for IPP.
8. Inspected both the OBI user account management procedures and password procedures and determined procedures were documented for OBI.
9. Inspected the HRConnect user account management procedures and determined procedures were documented for HRConnect.
10. Inspected both the OneStream XF user account management procedures and password procedures and determined procedures were documented for OneStream XF.
11. Inspected the oneARC user account management procedures and determined procedures were documented for oneARC.
12. Inspected the USA Staffing Onboarding user account management procedures and determined procedures were documented for USA Staffing Onboarding.
13. Observed an Oracle logon session and noted that users were required to have a valid logon ID and password and that logins/sessions were secured using TLS 1.2, AES with 128 bit encryption (High), and ECDH with 256 bit exchange.

98   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

14. For a selection of new Oracle users, inspected user access request forms and determined that the forms were completed, access was authorized, and employees acknowledged that they understood the Privacy Act requirements.
15. For a selection of changes to Oracle user profiles, inspected authorizing documentation and determined updates to access rights were authorized.
16. For a selection of requests for the termination of customer agency employees' Oracle access, inspected the Oracle Terminations listing and access removal requests and determined that the requests for the termination of access were completed and removal of access was performed in a timely manner.
17. 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.
18. Inspected the Fiscal Service HR separation listing and the Oracle user listing and determined no separated employees retained access to Oracle.
19. For a selection of days, inspected the daily Oracle inactivity reports and determined the report was reviewed and users who were inactive for over 90 days were end-dated.
20. For a selection of user account reviews for customer agencies, inspected the customer agencies' annual Oracle user access review and the system-generated user access list and determined the user access lists were provided to customer agencies for review and changes provided by the customer agencies were applied.
21. 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 the customer agency.
22. 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.
23. Observed an ARC Oracle application administrator attempt to add responsibilities to his/her user ID and noted that the application automatically blocked the attempt to add responsibilities to the user's ID.
24. For a selection of instances in which temporary administrator access was granted, inspected corresponding authorization forms/documentation and the Oracle Administrators listing, and determined such instances were documented, approved, and revoked when no longer needed.
25. Inspected the Oracle hosting contract and determined it stated access to the supporting operating system and database administrative accounts was limited to Oracle staff.
26. Inspected a listing of Oracle user accounts and determined accounts followed a defined naming convention.
27. Observed a PRISM logon session and determined valid credentials were required and those logins/sessions were encrypted with TLS 1.2, ECDHE_RSA with P-256, and AES 128 GCM.4.
28. For a selection of new PRISM users, inspected user access request forms and determined the forms were completed, access was authorized, and authorized access matched that which was configured in PRISM.
29. For a selection of changes to PRISM user accounts, inspected authorizing documentation and determined updates to the accounts were authorized and authorized access matched that which was configured in PRISM.
30. Inspected a selection of requests for the termination of customer agency employee's PRISM access to determine whether the requests for the termination of access were completed in a timely manner to remove the access.

    Exception Noted: One of 25 users selected for testing did not have his/her PRISM access terminated timely. The user's access was not removed until five days after they transferred positions.

    Management Response: Management concurred with the exception and will implement corrective actions.

99   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

31. 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.
32. Inspected the Fiscal Service HR Separation listing and the PRISM user listing and determined no separated ARC employees retained access to PRISM.
33. For a selection of days inspected the daily PRISM inactivity reports and determined the report was reviewed and users who were inactive for over 90 days were end-dated.
34. For a selection of user account reviews and customer agencies, inspected the customer agencies' annual PRISM user access review and the system-generated user access list and determined the user access lists were provided to customer agencies for review and changes provided by the customer agencies were applied.
35. Observed the production PRISM system for a selected user and noted that access was limited to assigned operating units based on their Site ID.
36. For a selection of changes to PRISM functional access privileges, inspected email access requests and determined changes were reviewed and compared to the BTD's Team Responsibilities matrix, and were deemed appropriate.
37. Inspected a listing of PRISM user accounts and determined the accounts followed a defined naming convention.
38. Observed a user log into webTA and noted the connection to webTA was encrypted utilizing TLS 1.2 and AES 256 bit encryption.
39. Observed a webTA logon session and noted logins/sessions required valid credentials.
40. For a selection of changes to webTA users with elevated privileges, inspected user access request forms and determined the forms were completed, access was authorized, and authorized access matched that which was configured in webTA.
41. Inspected a selection of webTA End User Application access removal requests for access removal and compared removal requests to the webTA separation listing and determined HR administrators from the HR Systems Help Desk removed any elevated access in a timely manner.
42. Inspected the Fiscal Service HR separation listing with the webTA user listing and determined no separated employees retained access to webTA.
43. For a selection of customer agencies, inspected annual user access review and determined that webTA user access lists were distributed to customer agencies for review documentation and access changes identified by customer agencies were applied.
44. Inspected the Fiscal Service user privileges within webTA and determined users assigned the HR administrator role were not also assigned the system administrator role.
45. Inspected a listing of webTA user accounts with administrative access to the underlying webTA servers and organizational chart and databases and determined administrative access was limited to server and database administrators within ISS.
46. Observed a user logging into webTA for the first time and noted webTA automatically required users to create a new password after initial login.
47. Inspected the webTA password settings and determined settings related failed logins, password complexity, aging, generation, and length requirements were configured in accordance with ARC password standards.
48. Inspected webTA configuration settings and determined webTA sessions were configured to time-out if they remained inactive for 10 minutes.
49. Observed a user access the ConcurGov system and noted the user had to be authenticated prior to accessing the system.
50. 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.

100   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

51. For a selection of changes to ConcurGov users, inspected the authorizing documentation and the ConcurGov Access Listing and determined access changes were documented, access was authorized, and authorized access matched that which was configured in ConcurGov.
52. 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.
53. For a selection of ConcurGov employee termination requests made from customer agencies, inspected the ConcurGov Terminations listing and access removal requests and determined the employee did not retain access to ConcurGov after their termination date.
54. Inspected the Fiscal Service HR separation listing and ConcurGov user listing and determined separated employees did not retain access to ConcurGov.
55. For a selection of user account reviews for customer agencies, inspected the corresponding ConcurGov user access review and the system-generated user access listing and determined the user access lists were provided to customer agencies for review and changes provided by the customer agencies were applied.
56. Inspected access levels within ConcurGov and determined access levels separated permissions from highest (administrator) to lowest (report user).
57. Observed a user attempt to change his/her 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.
58. Observed an Employee Portal user login to moveLINQ and determined that the user was required to authenticate either via PIV/CAC, ID.me, or Login.Gov, that three records of identity were configured to match in CAIA and moveLINQ, that the user could view his/her own records and only apply his/her assigned stamp to documents routed to the user, and that the user did not have roles with assigned permissions or functions tied to them.
59. Inspected documentation for a selection of added moveLINQ users and determined the requests were documented, approved, and access was configured as authorized.
60. 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.
61. Observed an Approval Portal user login to moveLINQ and noted that the user could only authenticate via PIV/CAC, only view his/her assigned customer agency records or apply status stamp to documents routed to them, and did not have roles with assigned permissions or functions tied to the user.
62. Observed a user login to the web based system expense management portal and noted that the user was required to authenticate via PIV/CAC only and that three records of identity are configured to match in CAIA and moveLINQ to allow access.
63. Inspected a system-generated moveLINQ user and role listing and determined roles were designed and provisioned in accordance with a least-privilege security approach.
64. 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 or authenticate using SSO.
65. For a selection of customer agencies, inspected the annual account recertification supporting documentation and determined ARC contacted customer agencies to initiate the recertifications, and results were returned to FRB St. Louis so that access changes could be applied as necessary.
66. For a selection of new IPP accounts, inspected documentation and determined access requests were documented, approved, and access was configured as authorized.
67. Inspected the Fiscal Service HR separation listing and the IPP user listing and determined no separated employees retained access to IPP.
68. Inspected system-generated IPP user and role listing and determined roles were designed and provisioned in accordance with a least-privilege security approach.

69. Observed a user attempt to change his/her IPP password using invalid settings and noted that the system automatically prevented the use of passwords that did not meet the password configuration, complexity, and expiration requirements.
70. Observed an OneStream XF user login to the web based system and noted the system required the user to enter a valid user ID and password. After migration to SSO, in June 2023, observed a Onestream XF user log in and noted the system required the user to authenticate using SSO.
71. For a selection of new OneStream XF users, inspected corresponding user access request forms and determined the requests were documented, approved, and access was configured as authorized.
72. Inspected the Fiscal Service HR separation listing and the OneStream XF user listing and determined no separated employees retained access to OneStream XF.
73. For a selection of employee termination requests, inspected email requests and inactivity reports and determined the employee did not retain access to OneStream XF after their termination date.
74. Inspected access levels within OneStream XF and determined access levels were restricted by cubes and workflows.
75. Inspected the listing of OneStream XF administrators and the Fiscal Service personnel listing and determined that all administrators were OSD/SPSD employees.
76. Observed the OneStream XF password complexity configuration settings and noted that the system required strong passwords in accordance with ARC password standards.
77. For a selection of dates, inspected OneStream XF violation logs and determined the violation logs were reviewed and violations were followed up.
78. Inspected the HUD annual account recertification and the system-generated user access list and determined ARC contacted HUD to initiate the recertification and made related changes to access permissions in OneStream XF as necessary, based on the customer agency' response.
79. For a selection of new or modified access changes to HRConnect users with elevated privileges, inspected user access request forms and determined the requests were documented, approved, and access was configured as authorized.
80. For a selection of HRConnect End User Application termination requests, inspected the HR Connect Terminations listing and access removal requests and determined personnel in the HR systems Help Desk removed elevated privileges upon user separation.
81. Inspected the Fiscal Service HR separation listing and the HRConnect user listing and determined there were no separated employees who retained access to HRConnect.
82. For a selection of customer agencies, inspected the customer agencies annual HR Connect user access review and associated system-generated access lists and determined the lists were provided to customer agencies for review and changes provided by the customer agencies were applied.
83. Observed a user access HRConnect and noted that access was restricted to users with a valid login ID and password or SSO with a valid PIV card.
84. For a selection of new KOFAX users, inspected the year over year active KOFAX user listing and determined that no new KOFAX user account provisioned access within FY23.
85. Inspected the annual recertification for the RPA AD group and determined that user access was reviewed and no instances of inappropriate access were identified.
86. Inspected the Fiscal Service HR separation listing and the active KOFAX user listing and determined there were no separated employees who retained access to RPA software.
87. For a selection of new oneARC users, inspected corresponding user access request forms and determined access was documented, approved, and access was configured as authorized.
88. Observed a user access oneARC and determined the user was required to authenticate via SSO.
89. For a selection of changes to oneARC users, inspected authorizing documentation and determined updates to access rights were configured as authorized.

Management of Administrative Resource Center's Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Tests

90. For a selection of oneARC access removals, inspected the oneARC Terminations listing, access request forms and email requests, and determined termination of oneARC access was completed and access was removed.
91. Inspected the Fiscal Service HR separation listing and the active oneARC user listing to determine whether terminated users retained access to oneARC.
92. Inquired of ARC Management and was informed that oneARC access review policy and procedure were not developed, documented, disseminated.

    Exception Noted: oneARC user access review was not documented in accordance with ARC's policies and procedures.

    Management Response: Management concurred with the exception and will implement corrective actions.
93. Observed a user access USA Staffing and noted that users are required to authenticate to USA Staffing via PIV/CAC or Login.Gov.
94. For a selection of new or modified access changes to USA Staffing Onboarding users with elevated privileges, inspected user access request forms, and determined access was documented, approved, and access was configured as authorized.
95. For a selection of customer agencies, inspected the semi-annual account recertification and user access list and determined ARC contacted customer agencies to initiate the recertifications and made related changes to access permissions in USA Staffing Onboarding as necessary, based on customer agencies' responses.
96. For a selection of employee termination requests, inspected USA Staffing Onboarding Account records and determined the retired users did not retain access to USA Staffing Onboarding after their termination date.

No exceptions noted, except as indicated above.

103   *Management of Administrative Resource
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests*

Control Objective 19 – Application Changes

Controls provide reasonable assurance that changes to the applications are authorized, tested, approved, and documented in accordance with ARC policies and procedures.

Description of Controls

ARC has documented procedures for testing, approving, and documenting changes.

Oracle, OBI, and PRISM

Key steps for each change, including the initial request, approval, and implementation into production is documented in ESM/ServiceNow, JIRA, and My Oracle Support for Oracle, OBI, and PRISM.

ARC processes standard software releases (i.e., patches) for Oracle, OBI, and PRISM. Oracle Managed Cloud Services provide notification to ARC of standard software releases, along with associated Release Notes outlining changes. Additionally, ARC processes customized application extension changes to Oracle. The ability to process and apply Oracle, OBI, and PRISM changes is restricted to the database administrators under the coordination of OMCS. 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 a separate development instance. OSD staff test changes by running test scripts and analyzing the results in a separate test environment. Upon successful completion of testing, OSD staff approve the change request and forward it to the performer of the change, OMCS 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, 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's webTA maintenance agreement with immixTechnology expired in March 2023 at which time a new maintenance agreement was obtained with Lentech, a vendor for UKG'S 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 UKG, ARC RTSB and HROD staff test the new release in a separate test instance by running test scripts and analyzing the results. The ability to apply webTA releases is restricted to the database and webTA application administrators under the authority of ISS. The new webTA release is not applied to production until it has been successfully tested and approved.

Management of Administrative Resource Center's Control Objectives and Related Controls, and KPMG LLP's Tests of Operating Effectiveness and Results of Tests

OneStream XF

ARC uses ESM/ServiceNow, OneStream Support, JIRA, and a Change Control Log to document key steps for each change: including the initial request, approval, and implementation into production.

ARC processes standard software releases (both Minor and Major). Releases identified as Major must be FedRamp Approved prior to being applied in a test environment. Additionally, ARC processes customized migration files for setup changes. The ability to process and apply changes is restricted to the application administrators.

When a new OneStream XF release is received, OneStream Support provides notification to ARC along with associated Release Notes outlining changes. ARC RTSB, PSS and ARAD staff test the new release in a separate test environment by running test scripts and analyzing the results. The ability to apply OneStream XF releases is restricted to the application administrators. The new OneStream XF release is not applied to production until it has been successfully tested and approved.

ARC ARAD Super Users serve as the primary initiators of migration change requests. The following is indicated in the request: Change ID number, service ticket number, description of change, global indicator, migration from environment/application, migration to environment/application, primary POC, supervisory approval. Migration changes are developed in a separate development environment with staff from ARC RTSB and ARAD running test scripts and analyzing the results. Upon successful completion of testing, ARC RTSB perform a backup of Production prior to moving the approved migration file to Production. After the approved request has been completed, all parties are notified and associated service ticket is closed.

Robotic Process Automation

Changes to RPAs are initiated by a Change Request Form submitted by the business area responsible for the process (Process Owner). DAB 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 of the change, the RPA is tested in the non-production Acceptance region of the RPA Management Console. The developer then provides RPA output materials for Process Owner review. If satisfactory, the code then undergoes a final peer code review. Once the code reviewed, the Process Owner's test plan and go live approval is obtained.

If the change is determined to have a security impact, the existing Security Impact Analysis (SIA) portfolio is updated and routed to the Information System Security Officer (ISSO) and System Owner for review and approval. When an RPA change request creates a new business process, the ISSO also sends the SIA portfolio to the Policy and Risk Management Branch (PRMB), which is a part of ISS, for a security analysis. Once the SIA is approved by the ISSO/System Owner and PRMB (when applicable), an Independent Validation (IV) form is completed with supporting evidence including a System Security Plan update, peer code review, and Process Owner approval.

Once the IV form is signed by both the ISSO and System Owner, a non-developer resource within the DAB uploads the bot code to the production Management Console, schedules the RPA, and closes the JIRA ticket.

<u>oneARC</u>

Requests for changes to oneARC workflows are submitted by the business area responsible for the process. The oneARC Product Owner reviews the change request and, if the requested is approved, a JIRA ticket is created and assigned to a Salesforce developer.

Once the developer completes the initial development, the change is tested in the non-production region of oneARC. The developer then provides output materials and the test plan for Process Owner review. Once reviewed, the Process Owner provides the "go live". The code then undergoes any necessary UAT testing.

A non-developer resource within the oneARC administration team uploads the packaged change to the production region. The Product Owner then approves the closure of the JIRA ticket.

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

1. Inspected written procedures for application changes and determined such procedures were documented.
2. Observed ESM/ServiceNow and noted the system is configured to retain necessary change management documentation when changes are made.
3. For a selection of changes processed in ESM/ServiceNow and My Oracle Support, inspected corresponding ESM/ServiceNow tickets 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 ARC's biannual review of access to My Oracle support and determined access was reviewed and no instances of inappropriate access were identified as a result of the review.
6. For a selection of emergency changes processed in My Oracle Support for Oracle and PRISM, inspected corresponding ESM/ServiceNow tickets and determined the emergency changes were approved by an ARC Oracle or PRISM application administrator in My Oracle Support the next business day.
7. Inspected the webTA system maintenance agreement and determined it contained system maintenance provisions and was current.
8. Inspected change management records associated with a selection of webTA releases and determined that the releases were tested in a separate non-production environment using testing scripts and were only released to production after the successful completion of customer acceptance testing by an authorized database administrator and appropriate approvals were obtained.
9. Inspected change management records associated with a selection of OneStream XF releases and determined that releases were tested in a separate non-production environment using testing scripts and were only released to production after successful testing by an authorized application administrator and appropriate approvals were obtained.
10. For a selection of new RPAs implemented into production, inspected change documentation and determined the RPAs were tested and approved prior to production implementation.
11. For a selection of RPA changes, inspected change documentation and determined the changes were tested and approved prior to being implemented to production.
12. For a selection of oneARC workflow changes, inspected change documentation and determined that the changes were tested and approved prior to being implemented to production.

No exceptions noted.

106   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Control Objective 20 – Non-interruptive System Service

Controls provide reasonable assurance that the data center used to host webTA servers is restricted to authorized users and that identified system issues are investigated and resolved and/or escalated for resolution.

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, OBI, ConcurGov, IPP, OneStream XF, HRConnect, and oneARC are not covered in this report.

The Fiscal Service Asset Protection Division (APD) issues employee badges, after performing security background checks and fingerprinting.

Employees are always required to have badges available upon request.

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

The webTA 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 ESM/ServiceNow, a workflow system that is used to approve data center access. After the Branch Manager completes and submits the ESM/ServiceNow request form for the appropriate ISS Resource area access level, it is forwarded to ISS's data center managers for approval in the ESM/ServiceNow. If ISS approves the request and the appropriate training is completed by the employee, the Physical Security Branch (PSB) within APD 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 and OBI

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 CSD/OSD/SPSD.

ARC monitors the connection to Oracle and OBI to help ensure that the application is available. If the connection to Oracle and OBI 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 the connection issue. 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.

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 CSD/OSD/SPSD.

ARC monitors the connection to PRISM to help ensure that the application is available. If the connection to PRISM 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 the connection issue. 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.

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. RTSB acts as a liaison between the HR Systems Help Desk and ISS to resolve system issues.

108   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

Backups are executed hourly on local and recovery servers at each data center and stored within a redundant disk array (short term). Data is placed on tape store for archival purposes.

ConcurGov

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

moveLINQ application administrators investigate any system issues reported to them by moveLINQ users or discovered by them during the performance of normal duties as assigned. When possible, moveLINQ application administrators resolve moveLINQ issues. If the administrator cannot resolve an issue, the issue is escalated to mLINQS, the vendor. The moveLINQ administrator notifies the users of the length of the expected problem and notifies them again when the issue is resolved.

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, ARC sends an e-mail to the IPP Customer Support Center at FRB St. Louis for investigation and resolution.

OneStream XF

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, the Oracle Support Team staff have access to the internal system setup and security documentation as well as various manuals and documentation produced and maintained by OSD.

ARC monitors the connection to OneStream XF to help ensure that the application is available. If the connection to OneStream XF 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 the connection issue. 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 resolve 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.

oneARC

oneARC user manuals are available for all end users to download from the Help Section within oneARC. The oneARC Support Team within RTSB is available for end users to call if they experience difficulties with the system, and oneARC application administrators have access to internal application setup, authorization information, as well as various manuals and documentation produced by OSD.

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 they were documented.
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 an individual attempt to access the Fiscal Services Building and noted he/she displayed his/her identification badges while inside the facility.
5. For a selection of employees granted one-day badges to the ISS data center, inspected the access request approvals from the individual's branch manager and determined the request was a) tracked in ESM/ServiceNow, and b) approved by ISS, and c) 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 to determine whether logs were reviewed by ISS, all unauthorized access attempts were investigated, and a follow up with the individual's supervisor was completed.
   > Exception Noted: For one of two months selected, the access violation log review was not performed timely.
   > Management's Response: Management concurred with the exception and will implement corrective actions.
7. For a selection of dates, inspected the ISS visitor log and determined that data centers required visitors to sign in prior to being issued a visitor badge, and sign out at the completion of their data center visit.
8. For a selection of dates, inspected the daily shift logs and determined an inventory of daily badges was performed.
9. Inspected the annual review and recertification of individuals with access to the data center and access requests from ISS and determined that the review/recertification was performed and unauthorized access found was identified and removed.
10. Observed that HP Site Scope and noted such tools were implemented for use by ISS staff to monitor ARC hosted applications.
11. Observed various monitoring logs and noted that a) they automatically generated alerts from HP's Site Scope; b) the application provided monitoring over websites, FTP servers, and intrusion detection software; and c) the logs and alerts were reviewed by ISS.
12. Observed the Andover monitoring application and noted the application was installed and used to monitor ISS data center environmental conditions.
13. Observed the ISS data center and noted sprinklers, hand-held fire extinguishers, and raised floors were present.
14. Inspected completed maintenance work orders and inspection reports for the uninterruptible power supply (UPS) and the emergency power generator and determined the generator and UPS were maintained.

110   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

15. Inspected the redundant air conditioning (AC) units and determined they were available and in operation in the event of a main AC equipment failure.
16. Observed Oracle operations manuals and determined the manuals are supplied to each employee assigned system maintenance responsibilities.
17. Observed the internal application setup and security documentation and various manuals and documentation produced by Oracle Corporation and determined they were documented and made available to Oracle support personnel.
18. Observed online support documentation for Oracle and determined the Oracle Support Team was available for users to call if they were experiencing difficulties with the system.
19. Observed internal application setup and security documentation and determined PRISM application administrators have adequate access to materials.
20. Observed PRISM user manuals and determined the manuals are supplied to end users.
21. Inspected online support documentation for PRISM and determined users have adequate access to the materials and determined the PRISM Support Team, within SDB, is available for users to call if they are experiencing difficulties with the system.
22. Observed online documentation produced by Kronos and noted webTA support personnel have adequate access to materials.
23. Inspected listing of webTA issues escalated to the HR Help desk and determined issues were documented and resolved.
24. Inspected the ConcurGov incident escalation procedures and determined the incident escalation procedures were documented and available to support ARC staff personnel in investigating and attempting to resolve any system issues.
25. For a selection of issues escalated to Concur, inspected escalated issue tickets and determined the issues were documented and resolved.
26. Inspected ARC's maintenance agreement with moveLINQ and determined that it required moveLINQ to provide software and technical support for moveLINQ.
27. Inspected RSB system administrator's escalation procedures and determined they stated that if an RSB administrator cannot resolve an issue, the issue is escalated to mLINQ.
28. For a selection of moveLINQ incidents that the RSB Administrator was unable to resolve, inspected emails requesting support and determined the issues were escalated to the mLINQ help desk for resolution.
29. For a selection of escalated IPP system issues that Fiscal Service was unable to resolve, inspected emails requesting support and determined the issues were escalated to the IPP Customer Support Center at FRB for investigation and resolution by FRB.
30. Observed the HP Site scope tool and determined that it was used to monitor OneStream and alerts were set-up to notify personnel of system issues.
31. Observed internal application setup and authorization information, as well as various manuals and documentation produced by OSD and noted oneARC application administrators have adequate access to materials.
32. Observed oneARC Help Section and noted user manuals were available for all end users to download.
33. Observed online support documentation for oneARC and determined the oneARC Support Team was available for users to call if they were experiencing difficulties with the system.

No exceptions noted, except as indicated above.

Control Objective 21 – Backups

Controls provide reasonable assurance that relevant data is backed up, available for restoration, and in accordance with ARC policies and procedures.

Description of Controls

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 that are located at the underground offsite storage facility location. Media inventories are maintained via the tape libraries at the 3rd Street Data Center located in Parkersburg, WV and the Kansas City Regional Operational Center (KROC) Data Center located in Kansas City, MO.

Differential backups of Network File Shares are created daily and retained for a period of 90 days. Differential backups are replicated to the alternate Fiscal Service Data Center daily. Daily differential backups are also tiered after 7 days to our immutable storage, the IBM Cloud Object Storage (ICOS). It will remain on the ICOS for the remainder of the 90 day retention period. The ICOS is distributed across three Fiscal Service physical locations.

Tests of Operating Effectiveness and Results of Testing

1. KPMG was not able to determine the operating effectiveness of the Tape Receiving control and verify the accuracy of tapes received, as tapes are only sent back to Fiscal Service if a significant issue were to arise, and KPMG was informed none arose during the testing period.
2. Inspected evidence of the annual physical inventory of all backup tapes that are in Fiscal Service's possession and determined the inventory was performed.
3. For a selected network file server used by ARC, inspected system-generated backup schedules and logs and determined that daily differential backups and weekly full backups of the file server were scheduled and successfully completed.
4. Inspected the backup configurations for webTA and determined they were configured to complete a nightly differential backup.
5. Observed the backup configurations for a webTA server and determined that the daily replication process was configured to send backups to an alternate processing site.
6. Inspected the backup log for webTA servers and determined differential backups were completed successfully.

No exceptions noted.

MONITORING CONTROLS

Control Objective 22 – 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, 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 they were documented.
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.

113   *Management of Administrative Resource*
Center's Control Objectives and Related Controls, and KPMG LLP's
Tests of Operating Effectiveness and Results of Tests

V. OTHER INFORMATION PROVIDED BY THE MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER

CONTINGENCY PLANNING

System Back Up

The Oracle accounting system has a contingency plan managed by ARC, which was last updated in May 2023. 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 OMCS' primary site on the east coast, are replicated near real time using Data Guard to a contingency location in the western United States.

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 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 East Rutherford Operational Center (EROC) and Dallas. FRB St. Louis performs 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 help ensure that the application was 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

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.

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/