



# Audit Report



OIG-26-001

## 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, 2024 to June 30, 2025**

November 25, 2025

Office of Inspector General  
Department of the Treasury

**This Page Intentionally Left Blank**



OFFICE OF  
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

November 25, 2025

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

**FROM:** Shiela Michel /s/  
Acting 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, 2024 to June 30, 2025

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, 2024 to June 30, 2025, 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, 2024 to June 30, 2025;
- 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, 2024 to June 30, 2025, and subservice organizations and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2024 to June 30, 2025; and

- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2024 to June 30, 2025 if complementary subservice organization controls and complementary customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2024 to June 30, 2025.

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 the Bureau of the 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 November 25, 2025, 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) 927-5407.

Attachment

cc: Jeffrey J. Schramek  
Deputy Commissioner,  
Financial Integrity and Shared Services

**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, 2024 to June 30, 2025**

**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, 2024 TO JUNE 30, 2025**

**Table of Contents**

<u>Section</u>	<u>Description</u>	<u>Page</u>
<b>I.</b>	<b>INDEPENDENT SERVICE AUDITORS’ REPORT PROVIDED BY KPMG LLP .....</b>	<b>1</b>
<b>II.</b>	<b>MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER’S ASSERTION.....</b>	<b>5</b>
<b>III.</b>	<b>MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER’S DESCRIPTION OF ITS SHARED SERVICES SYSTEM.....</b>	<b>8</b>
	OVERVIEW OF OPERATIONS .....	9
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, AND MONITORING .....	22
	Control Environment.....	22
	Risk Assessment.....	22
	Monitoring.....	22
	Monitoring Subservice Organizations.....	23
	INFORMATION AND COMMUNICATION .....	24
	Information Systems.....	24
	Communication .....	27
	CONTROL OBJECTIVES AND RELATED CONTROLS .....	28
	COMPLEMENTARY CUSTOMER AGENCY CONTROLS .....	75
	SUBSERVICE ORGANIZATIONS .....	78
	COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS.....	81
<b>IV.</b>	<b>MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER’S CONTROL OBJECTIVES AND RELATED CONTROLS, AND KPMG LLP’S TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS .....</b>	<b>86</b>
	FINANCIAL MANAGEMENT PROCESSING CONTROLS.....	88
	Control Objective 1 – Obligations.....	88
	Control Objective 2 – Disbursements.....	91
	Control Objective 3 – Unfilled Customer Orders, Receivables, and Cash Receipts.....	98
	Control Objective 4 – Deposits .....	101
	Control Objective 5 – Payroll and Leave Accruals .....	103
	Control Objective 6 – Payroll Disbursements .....	104
	Control Objective 7 – USSGL.....	106
	Control Objective 8 – Period-End Accruals .....	111
	Control Objective 9 – Governmentwide Reporting.....	113

Control Objective 10 – Budget.....	118
Control Objective 11 – Manual Journal Entries.....	120
Control Objective 12 – Federal Investments.....	121
Control Objective 13 – Supplier and Bank Records Changes.....	123
<b>PROCUREMENT PROCESSING CONTROLS .....</b>	<b>125</b>
Control Objective 14 – Acquisitions and Contracts.....	125
Control Objective 15 – Sufficiently Funded Requisitions.....	126
<b>HUMAN RESOURCES PROCESSING CONTROLS.....</b>	<b>127</b>
Control Objective 16 – Personnel Actions.....	127
Control Objective 17 – Payroll Documents.....	133
<b>GENERAL COMPUTER CONTROLS .....</b>	<b>136</b>
Control Objective 18 – System Access.....	136
Control Objective 19 – Application Changes.....	164
Control Objective 20 – Data Center Physical Access and Environmental Controls.....	170
Control Objective 21 – Computer Operations.....	175
Control Objective 22 – Backups.....	177
<b>V. OTHER INFORMATION PROVIDED BY THE MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER .....</b>	<b>178</b>
Continuity of Operations.....	179

**I. INDEPENDENT SERVICE AUDITORS' REPORT PROVIDED BY KPMG LLP**



KPMG LLP  
Suite 12000  
1801 K Street, NW  
Washington, DC 20006

## Independent Service Auditors' Report

Deputy Inspector General, Department of the Treasury  
Deputy Commissioner of Administrative Resource Center:

### *Scope*

We have examined management of Bureau of the Fiscal Service's Administrative Resource Center's (ARC) accompanying description of its shared service system (the System) for processing customer agencies' transactions throughout the period July 1, 2024 to June 30, 2025 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" (the Assertion). The controls and control objectives included in the Description are those that management of ARC believes are likely to be relevant to customer agencies' internal control over financial reporting, and the Description does not include those aspects of 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. Information about ARC's contingency planning has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the Description and, accordingly, we express no opinion on it.

ARC uses the 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 organization(s). 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 the 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 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 operated effectively to achieve the related control objectives stated in the Description throughout the period July 1, 2024 to June 30, 2025. 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
- 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:

- the Description fairly presents the System that was designed and implemented throughout the period July 1, 2024 to June 30, 2025;
- 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, 2024 to June 30, 2025, and subservice organization(s) and customer agencies applied the complementary controls assumed in the design of ARC's controls throughout the period July 1, 2024 to June 30, 2025; and
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period July 1, 2024 to June 30, 2025 if complementary subservice organization controls and complementary customer agency controls, assumed in the design of ARC's controls, operated effectively throughout the period July 1, 2024 to June 30, 2025.

### *Restricted Use*

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of ARC, customer agencies of ARC's System during some or all of the period July 1, 2024 to June 30, 2025, 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 customer agencies themselves, when assessing the risks of material misstatement of customer agencies' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

*KPMG LLP*

Washington DC  
November 25, 2025

**II. MANAGEMENT OF ADMINISTRATIVE RESOURCE CENTER'S  
ASSERTION**



DEPARTMENT OF THE TREASURY  
BUREAU OF THE FISCAL SERVICE  
WASHINGTON, DC 20227

November 25, 2025

**Administrative Resource Center's Assertion**

We have prepared the accompanying description of Bureau of the Fiscal Service's Administrative Resource Center's (ARC)'s shared service system (the System) for processing customer agencies' transactions throughout the period July 1, 2024 to June 30, 2025 titled "Management of Administrative Resource Center's Description of its Shared Services System" (the Description) for customer agencies of the System during some or all of the period July 1, 2024 to June 30, 2025, 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 customer agencies' financial statements.

ARC uses the 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 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, 2024 to June 30, 2025 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;
  - (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 System 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 operated effectively throughout the period July 1, 2024 to June 30, 2025 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, 2024 to June 30, 2025. 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,



---

Jeffrey J. Schramek  
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 a unit within the Bureau of the Fiscal Service (Fiscal Service), operating as a distinct entity within the Fiscal Service. Since its inclusion in the Treasury Franchise Fund (TFF) in August 1998—established under Public Law 104-208 and later solidified by Public Law 108-447—ARC has provided administrative services, including financial management, human resources, travel, and procurement. These services are offered on a competitive, full-cost, fee-for-service basis. ARC’s mission is to deliver responsive, customer focused, cost-effective administrative support to customer agencies.

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

<b>Agency Payable and Receivable Division (APRD)</b>	<b>Services Provided</b>
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
Agency Cash Branch (ACB)	Provides Cash Related Services Disbursements to Non-federal Entities Check Scanning Fund Balance with Treasury Reconciliation Accounting
<b>Transaction Management Division (TMD)</b>	<b>Services Provided</b>
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
Funds Management Branch (FMB)	Document Processing Reporting Investment Activities
<b>Agency Reporting and Analysis Division (ARAD)</b>	<b>Services Provided</b>
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
Budget Execution Branch (BEB)	Accounting Reporting Budget
<b>Division of Procurement Services (DPS)</b>	<b>Services Provided</b>
Treasury Acquisitions Branch (TAB)	Procurement
Fiscal Service Acquisitions Branch (FSAB)	Procurement
Non-Treasury Acquisitions Branch (NTAB)	Procurement
<b>Human Resources Operations Division (HROD)</b>	<b>Services Provided</b>
Employee Benefits Branch (EBB)	Processes and Monitors Personnel Benefit Actions
Leave and 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
<b>Employment Services Division (ESD)</b>	<b>Services Provided</b>
Classification and Support Branch (CSB)	Position Classification
Staff Acquisition Branch 1 (SAB1)	Staff Acquisition
Staff Acquisition Branch 2 (SAB2)	Staff Acquisition
<b>Human Resources Systems Division</b>	<b>Services Provided</b>
Help Desk and Reports Branch (HDRB)	HR Systems Support and HR Reports
Systems Support Branch (SSB)	HR Systems Support and Training
<b>Travel Services Division (TSD)</b>	<b>Services Provided</b>
Relocation Services Branch (RSB)	Relocation
Temporary Services Branch (TSB)	Temporary Duty
<b>Customer Support Division (CSD)</b>	<b>Services Provided</b>
Service Desk Branch (SDB)	Financial Management System Support
User Support Branch (USB)	Financial Management System Support and Training
Digital Automation Branch (DAB)	Develop and Maintain Robotic Process Automation
Procurement and Accounting Support Branch (PASB)	Operate and Maintain Financial Management Systems
<b>Systems and Projects Division (SPSD)</b>	<b>Services Provided</b>
Project Support Staff Branch (PSSB)	Application Development, Analysis, and Project Management

Development Support Branch (DSB)

Reporting and Technology  
Support Branch (RTSB)

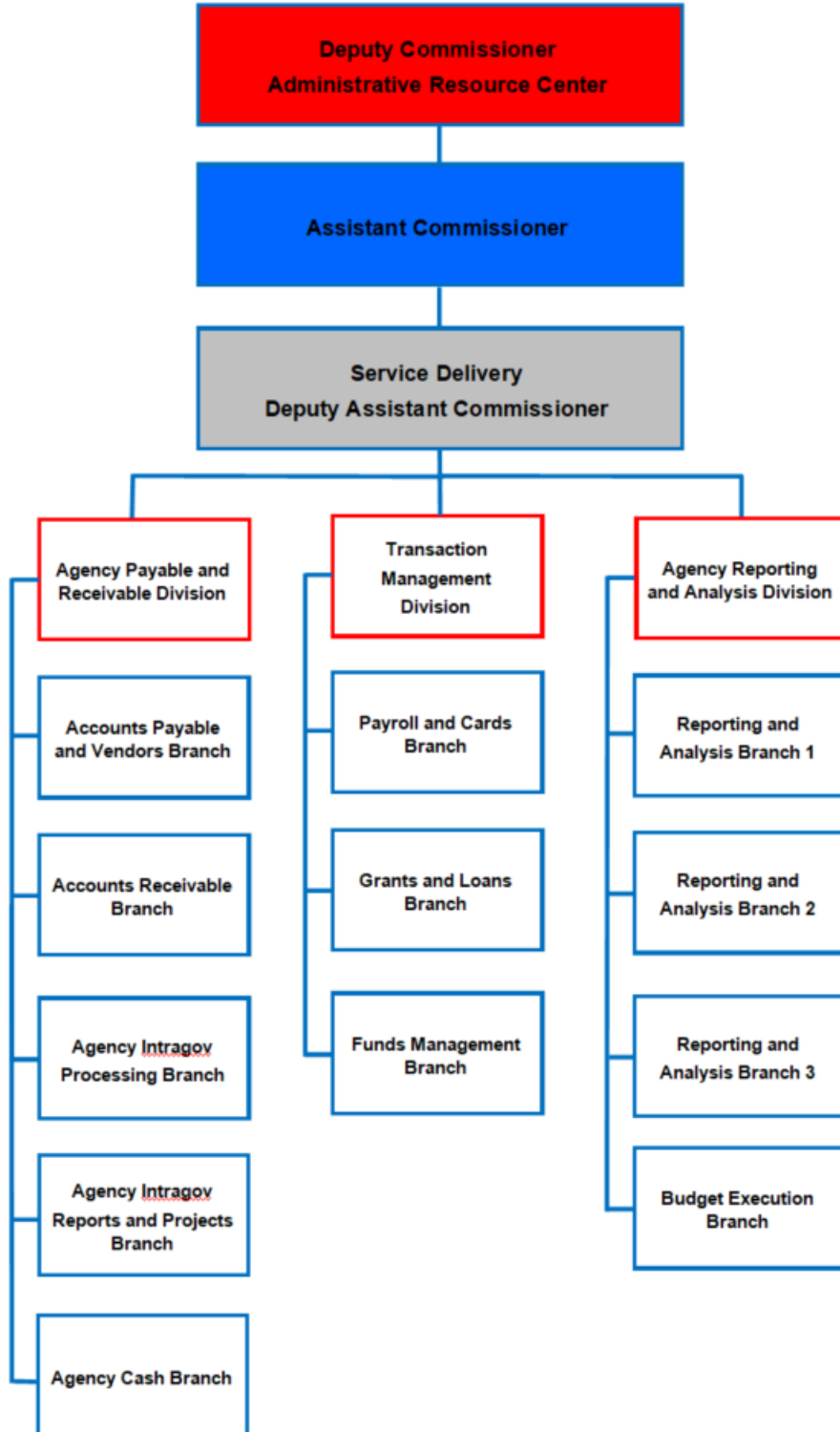
Business Liaison Branch (BLB)

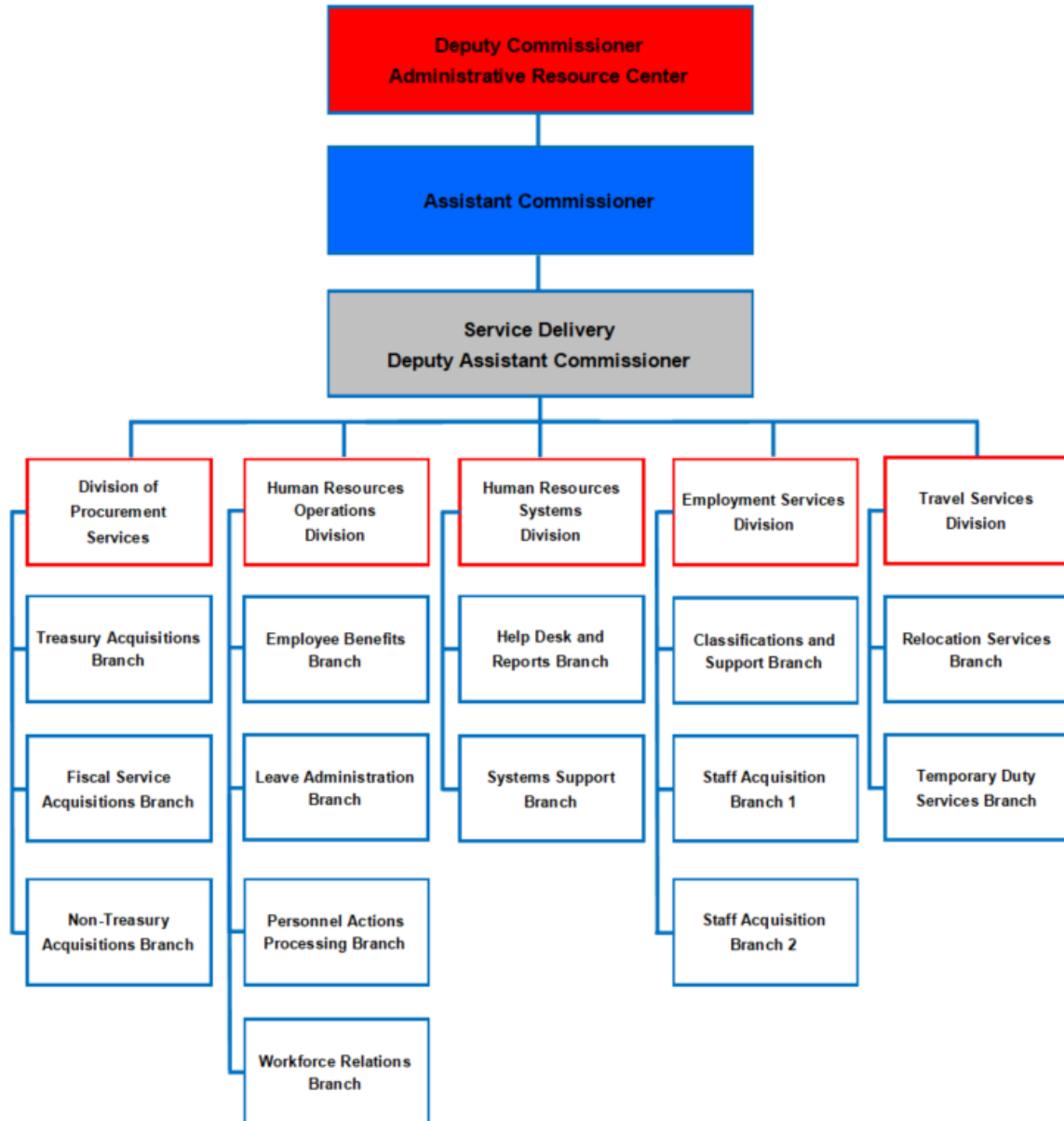
Application Development, Analysis, and Project  
Management

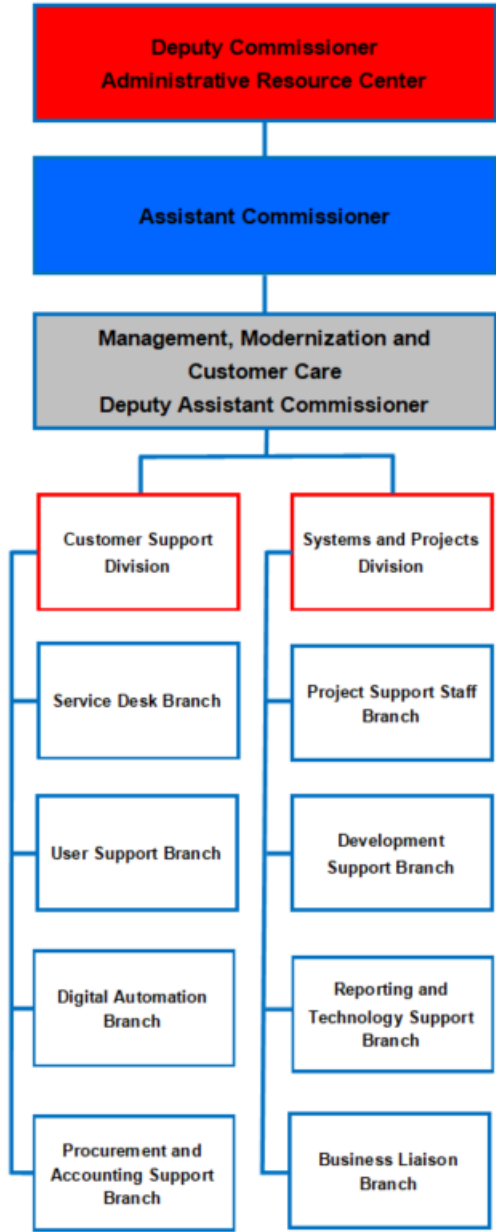
Operate and Maintain Financial Management  
Systems

Internal Project Support

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







## Accounting Services

Accounting Services consists of the following:

- Recording financial transactions in Oracle Federal Financials (Oracle), including appropriation, apportionment, allocations, revenue agreements, accounts receivable, collections, commitments, obligations, accruals, accounts payable, disbursements, and journal entries.
- Examining and processing vendor and other employee payments.
- Examining and processing revenue and other collections.
- Managing and verifying general ledger transactions in Oracle.

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 Oracle system 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. If the invoice amount is greater than the obligated amount, a modification is required unless overage tolerances have been pre-approved by the customer agency.

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.

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. If ARC is waiting for customer approval, IPAC payments will be posted in suspense prior to posting the obligation.

Third-party payroll services provide ARC with 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, Oracle 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:

- Acquisition.
- 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 are 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.

Personnel actions submitted by a manager 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.

Personnel actions submitted by an employee (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 USA Staffing Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the USA Staffing 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). An EBB HR Assistant verifies eligibility, sets the effective date, and obtains certification by an EBB Specialist, except for annual open enrollment season, or non QLE, self only elections made in EPP. 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 USA Staffing Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the USA Staffing 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.

HRSD serves as HR Systems support and is responsible for user access controls for HRConnect, webTA, GovTA, and 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 Hosting Service (MHS), 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, as needed, 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 ARC and customer agency travelers into ConcurGov, which 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, provided 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 operations are led by the Executive Director of ARC, whose mission is to deliver responsive, customer focused, cost effective administrative support to customer agencies. ARC's governance structure and leadership establish the tone at the top, emphasizing operational excellence, transparency, and accountability.

Management meetings are held regularly to review special processing requests, monitor operational performance, and discuss the development and progress of ongoing projects. These meetings ensure effective oversight and alignment with organizational objectives.

ARC implements robust hiring procedures, including reference checks and periodic background, credit, and security screenings every three to five years, to maintain a high standard of personnel integrity. Confidentiality of customer agency information is a cornerstone of ARC's operations, emphasized during the orientation program and reiterated in the personnel manual provided to all employees.

ARC provides employees with the essential tools and knowledge to excel in their roles through mandatory orientation for new hires and access to formal external training opportunities. The training covers key topics such as Prompt Pay and Voucher Examination, Appropriation Law, Federal Acquisition Regulations, Federal Travel Regulations, Reconciling with and Reporting to Treasury, Federal Accounting Fundamentals, USSGL Practical Applications, Budgeting and Accounting, and Computer Security Awareness. By offering comprehensive training, ARC helps employees stay informed and proficient in their respective fields.

Employees participate in annual written performance evaluations and salary reviews, guided by predefined goals and objectives developed in collaboration with their supervisors. Senior management reviews completed appraisals to maintain fairness and accountability, with records preserved as permanent components of personnel files

Documented position descriptions for employees are maintained, reviewed, and updated as necessary to promote clarity in roles and responsibilities, reinforcing ARC's strong internal control environment.

### **Risk Assessment**

ARC has placed into operation a risk assessment process to identify and address risks that may impact its ability to deliver reliable services to customer agencies. As part of this process, management is responsible for identifying significant risks within their respective areas of oversight and deploying appropriate controls and measures to effectively mitigate and manage those risks.

### **Monitoring**

ARC management consistently evaluates the quality of internal control performance as an integral part of daily operations. This includes engaging with staff and reviewing data to ensure transactions are processed within an effective internal control environment. A key example of a

monitoring control is the review conducted by management within ARC's ARAD, which reconciles Oracle subledger data to related general ledger accounts. Additionally, ARC performs monthly reconciliations to ensure the accuracy of budgetary-to-proprietary account relationships. ARC also reconciles GTAS submitted reports to the trial balance and the statement of budgetary resources to maintain accuracy and accountability. As part of the monitoring process, ARC utilizes its annual System and Organization Controls (SOC) 1 Report to identify and address opportunities to enhance controls.

ARC management further ensures oversight by obtaining and reviewing SOC 1 reports from relevant subservice organizations. For ARC systems not covered by a SOC 1 report, system verification letters are prepared to document the implemented information security controls. If exceptions are identified, ARC reaches out to the subservice organization to obtain additional information as necessary.

### **Monitoring Subservice Organizations**

ARC reviews SOC 1 reports by obtaining relevant SOC 1 reports, which are then carefully reviewed to identify any control exceptions that may impact ARC's control environment. Complementary controls within these reports are evaluated and linked to the controls outlined in ARC's SOC 1 report. Management reviews and approves the findings, and relevant documentation about subservice organizations is made accessible to customer agencies. If applicable, ARC contacts subservice organizations to gather additional information regarding exceptions.

For Fiscal Service subservice organizations that do not have a SOC 1 report, ARC obtains a system verification letter. The system verification letter undergoes a detailed review and is approved by ARC. Once approved, the document is provided to customer agencies to maintain transparency and meet their informational needs.

## **INFORMATION AND COMMUNICATION**

### **Information Systems**

ARC oversees and performs application administration for a range of systems: Oracle, PRISM, OBI, ConcurGov, moveLINQ, oneARC, OneStream XF, webTA, GovTA, and IPP. Several of these applications - PRISM, ConcurGov, moveLINQ, oneARC, OneStream XF, webTA/GovTA, and IPP serve as feeder systems into Oracle, which is hosted by Oracle Customer Success Services (OCSS). Additionally, OBI and PRISM are hosted by OCSS.

ConcurGov is hosted by SAP Concur, while the Federal Reserve Bank of St. Louis manages IPP hosting. MHS hosts moveLINQ on its contracted Microsoft Azure Government Cloud platform. Similarly, Microsoft Azure Government also hosts OneStream XF. Salesforce hosts the oneARC system via its contracted Amazon Web Services (AWS) GovCloud+ platform. ARC is the designated system owner of webTA/GovTA; however, hosting and management responsibilities for these systems are handled by the Information and Security Services (ISS) office within Fiscal Service.

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

In relation to Oracle OBI, the Oracle R12 and Oracle databases are operated by Oracle Customer Success Services (OCSS) within an Oracle Cloud Infrastructure system environment. The system employs a two-tier web-based architecture comprising a front-end Internet user interface and a database housed within a secure network. Access to the front-end interface is safeguarded by a secure Lan2Lan (L2L) tunnel administered by the Bureau of Fiscal Service. Tunnel connectivity is tightly controlled and restricted to approved customer-assigned network ranges by the Bureau of Fiscal Service administrators.

Oracle serves multiple critical functions, including budget execution, federal report generation, general ledger management, purchasing, accounts payable and receivable, project accounting, fixed assets, and manufacturing. ARC utilizes Oracle Business Intelligence (OBI) as a reporting tool, offering users the ability to create customized ad-hoc reports for data query purposes. This intuitive tool enables reporting, analysis, and web publishing, empowering business users across all organizational levels to access operational data directly from Oracle tables in real time.

### **PRISM**

OCSS operates PRISM using an Oracle 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 OCSS 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. 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.

IPP data is stored and backed-up on the storage area network (SAN) and replicates every minute between the Federal Reserve System's East Rutherford Operational Center (EROC) and Dallas, TX-based replication site.

### **webTA/GovTA**

Ultimate Kronos Group's (UKG) webTA and GovTA serve as the primary time and attendance systems for most customer agencies whose payroll is processed by the National Finance Center (NFC). During FY2025, the webTA system will transition to GovTA. ARC is implementing this change through a three-phase approach, beginning with 2025 Pay Period 9 and concluding with 2025 Pay Period 15. This phased rollout ensures a smooth and efficient conversion process. Transactions that are entered in webTA/GovTA interface with NFC, and NFC ultimately sends payroll data back to ARC in order to be interfaced with Oracle. webTA/GovTA 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/GovTA database administrator and provides primary support for tape backup and recovery. webTA/GovTA 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 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 Software as a Service (SaaS)-based E-Gov Travel solution. ConcurGov is a cloud-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.

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

### **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 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 is responsible for the system backups of moveLINQ and data is maintained for six years.

### **Robotic Process Automation**

The Tungsten Automation<sup>1</sup> software is a tool used to create robotic process automations (RPA) to automate repetitive tasks and manual processes. ARC's RPAs are developed and managed by the Digital Automation Branch (DAB). Access to the Tungsten Automation 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 the Management Console, where RPA runs are scheduled and monitored. The 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 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. 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, and messaging channels. Questions and comments from these channels can become part of a case queue, and customers can easily collaborate using Salesforce Chatter. Salesforce applications can be fully integrated with back-office applications.

ARC has configured a Salesforce GovCloud+ instance to handle Budgetary, Purchasing, Payroll, Accounting, Accounts Receivable and Accounts Payable Financial Management requests from customer agency contacts. The request values and approvals stored in the Salesforce instance for

---

<sup>1</sup> Tungsten Automation (formerly Kofax) is software used by ARC that allows it control access to RPAs that are created to automate business processes. Tungsten Automation allows ARC to develop, test, and deploy the RPA.

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.

Procurement, Finance and Travel lines of business also have service desk ticket management inside Salesforce. Service desk ticket management is a streamlined process that handles customer issues or requests. Tickets are created, assigned, routed, resolved and closed within the oneARC application.

## **Communication**

ARC employs a structured approach to communication to ensure that all employees fully understand their roles and responsibilities within the organization. Methods include orientation and training programs for newly hired personnel, which provide foundational knowledge of their duties. Time-sensitive messages and critical information are disseminated efficiently via email. Additionally, managers conduct periodic staff meetings to foster collaboration and alignment on organizational goals and priorities.

Each employee is provided with a written position description, which includes a clear responsibility to escalate significant issues and exceptions to higher levels of management promptly. Managers proactively address employees' ongoing development needs by identifying relevant training opportunities. These opportunities are offered through ARC's employee training and career development programs, internal training sessions, and professional conferences.

## CONTROL OBJECTIVES AND RELATED CONTROLS

ARC's control objectives and related controls are included below.

### 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.

#### **Description of Controls**

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

#### **PRISM System Interface**

An obligation is created when a customer agency enters into a legally-binding contract with a vendor for goods or services. The obligation is entered into 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 helps to 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.

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 provide ARC a signed copy of the agreement or Miscellaneous Obligation Form to obligate 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 verify that submissions align with authorization authority and contain sufficient accounting details. The obligation is then manually entered into Oracle. If information provided by customer agency is insufficient, then the ARC technician will inquire with the customer agency. Some obligations are submitted through the oneARC portal and the technicians input them into Oracle. Once posted, obligations in Oracle are accessible to both ARC and customer agencies through ad hoc OBI reports.

## Temporary Duty Travel System Interface

ARC and customer agency travelers create travel authorizations using ConcurGov, which routes them to Approving Officials for review and approval. Approving Officials review and electronically approve authorizations. ConcurGov prevents self-approval without proper access.

Approved data is sent to Oracle via SAP Concur integration, where obligations are recorded if funds are available, and accounting strings are valid. Daily, ARC reviews OBI Status Report to identify and correct interface errors, with manual entry for transactions requiring correction. ARC Travel Services performs daily reconciliation of approved authorizations to verify accurate processing in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

## Relocation Travel System Interface

RSB personnel enter PCS travel authorizations into moveLINQ which routes them to Approving Officials for review and approval. Once signed, relocation coordinators designate the document as "approved" in moveLINQ.

For non-payment agencies, daily reconciliation reports with approved documents are sent to customer agency officials. For payment agencies, approved documents are interfaced into Oracle via batch integration, where obligations are recorded. An accounting technician performs a daily reconciliation between moveLINQ and Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

## 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 established by the customer agency and configured in Oracle by USB ARC staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent supervisory review to ensure completeness and accuracy in Oracle.

### Document Numbering

All accounting entries recorded into Oracle require a transaction or document identification number. Oracle is configured to prevent the use of duplicate document numbers on processing of obligation 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.

### Complementary Customer Agency Controls

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.

### **Control Objective 2 – Disbursements**

Controls provide reasonable assurance that non-payroll disbursements are authorized, 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. When a customer 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. A customer 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 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 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### Non-IPP Customer Agency Invoice Approvals

Non-IPP invoices are either sent to ARC or directly to the customer agency. When received by ARC, the customer agency provides approval via the oneARC application, or ARC forwards the invoice to an authorized agency contact for approval before ARC manually processes the obligation in Oracle.

If invoices are sent to the customer agency, the customer agency reviews and approves the invoice through the oneARC application.

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

A GLB accountant performs a review of all foreign payments prior to disbursement. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

#### 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 monthly 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 submit travel vouchers using ConcurGov, which routes them to Approving Officials for review and approval. ConcurGov ensures compliance with regulations and prevents self-approval. Once approved, SAP Concur's integration sends voucher data to Oracle, where disbursements are recorded if the accounting string is valid, and funds are available.

Daily, ARC reviews OBI Status Reports to identify and correct interface errors, with manual entry for transactions requiring correction. ARC Travel Services reconciles approved vouchers daily to ensure all ConcurGov vouchers are properly interfaced and processed in Oracle.

#### Relocation Services Travel Vouchers Approvals

RSB personnel enter and audit each PCS travel voucher in moveLINQ which electronically routes to an Employee/Approving Official 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 via batch processing to Oracle which records a disbursement in the general ledger. Approved vouchers in moveLINQ are reconciled by an Accounting Technician with an Oracle generated report to help ensure that all moveLINQ vouchers have been processed in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

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

Invoices processed by IPP undergo random sampling as part of a 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 on 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 for 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 of an accountant and help to ensure that 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.

#### Random Sampling of Temporary Duty Travel Vouchers Review

TSB staff complete post-payment audits of TDY travel vouchers to verify the accuracy of the interfaced data and compliance with FTR. Agencies falling into FTR or the FTR/ARC category type are subject to a 41-point audit worksheet comprised of 36 critical error checks and 5-noncritical informational checks. The ARC Travel Sampling Plan is broken down into two separate components: the Quality Sample and Statistical Sample. The Quality Sample is a weekly sample and includes two parts: 1) A 100% audit of vouchers equal to or greater than the sampling threshold (\$2,500 or \$1,000), 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 communicated via e-mail to the traveler, document preparer, and/or Approving Official for review and necessary action.

#### 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 backdating 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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. If interest is determined to be due on a foreign invoice, a manual interest invoice is entered into Oracle and paid to the vendor.

#### 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 customer agencies of their FBWT activity and balances and to assist customer agencies in reconciling their FBWT general ledger balances to Treasury's balances:

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

As month-end approaches ARC accountants reduce the probability of month-end differences relating to 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 create 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 established by the customer agency and configured in Oracle by USB ARC staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent supervisory review to ensure completeness and accuracy in Oracle.

### Intragovernmental Transactions

ARC adheres to applicable intragovernmental elimination guidance in the Treasury Financial Manual (TFM). This involves recording transactions at a level that allows for identification of ARC's governmental trading partners and for reconciling the transactions/balances with trading partners on a quarterly basis in GTAS. For the non-fiduciary transactions of ARC's Treasury customer agencies, ARC accountants prepare and submit confirmations to the appropriate trading partners in accordance with the elimination reconciliation guidance. Upon submitting the confirmations to the trading partners, ARC works with the trading partners to reconcile transactions/balances and identify and record any necessary adjustments. For non-Treasury customers, if there are any elimination differences that require an explanation, an accountant will enter the explanation in the GTAS module and an ARC supervisor or an Agency designee will certify the explanation in GTAS. For Treasury customers, the eliminations reporting is handled through the TIER reporting process.

### Document Numbering

All accounting entries recorded into Oracle require a transaction or document identification number. Oracle is configured to prevent 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 receipt 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.

### **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 report. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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 customer agencies 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. Oracle is configured to prevent processing of documents containing duplicate identification numbers, 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 certifies that the TROR and Debt Collection Activities report submitted to the Treasury is accurate and consistent with agency accounting systems.
- Review and approve the annual submission of the TROR and Debt Collection Activities report.

## **Control Objective 4 – Deposits**

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

## **Description of Controls**

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

## **Safeguarding Checks**

Checks received by the mailroom are scanned individually with the supporting documentation that came with each check. Each check with the documentation is saved as a separate file in a central location. The checks, along with the original documentation, are sent to the A3F mail drop by the mail deliverer and signed for 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 to provide a formal record. 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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 manually enters deposit information into the OTCnet system. A deposit ticket and the accompanying check(s) are secured in a locked money bag, which a mail clerk collects and delivers to the local federal depository. The ARC accounting technician retains a copy of the deposit ticket for comparison against the bank teller's deposit receipt and the confirmed deposit ticket from OTCnet. Upon verification of the bank teller receipt and OTCnet confirmed deposit ticket against the retained copy, an ARC accounting technician records the cash receipt in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### 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.

### **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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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 (monthly, or 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, 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.

### **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 detailed 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 through the oneARC application 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 resolves any differences identified. All those that require corrections are posted in either the current accounting period or in a subsequent accounting period.

### Complementary Customer Agency Controls

Customer 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.

### **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.

### Description of Controls

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

#### Transaction Set-up Controls

ARC records proprietary and budgetary accounting entries using the USSGL at the transaction level. This is accomplished using a combination of selecting a relevant transaction code, leveraging system setup configurations, Sub-Ledger Accounting (SLA) rules 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.

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.

### General Ledger Account Reconciliations

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. If invalid relationships are identified an accounting technician or an accountant corrects the transaction or prepares an entry to resolve the invalid relationships. 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.

### GTAS Edit Checks

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. ARC investigates and resolves any Treasury Appropriation Fund Symbol (TAFS) failed by the GTAS system.

### 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 accountants investigate 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### Financial Statement Variance Analysis

For Treasury and DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant and approved by the bureau CFO or designee prior to submission to Treasury. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.

For non-Treasury and non-DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant prior to submission to OMB. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.

### 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 CFOs or designee in support of financial reports' completeness, accuracy and timely submission for external use.
- Review and provide approval of TIER submission.

### **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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### Document Numbering

All accounting entries recorded into Oracle require a transaction or document identification number. Oracle is configured to prevent 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.

### **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 enable 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

### 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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. 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 Treasury and DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant and approved

by the bureau CFO or designee prior to submission to Treasury. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.

For non-Treasury and non-DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant prior to submission to OMB. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.

### 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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 ("attestation statement"). Upon receipt of the customer agency monthly attestation statement, 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.

### Complementary Customer Agency Controls

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

- Review and timely approve the annual submission of the TROR and Debt Collection Activities report.
- Provide timely certification of GTAS to ARC prior to system certification.
- Review and provide timely approval of TIER submissions.

- Ensure that the CFO timely certifies 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 timely approved by Treasury and DHS's CFO's or designee in support of financial reports' completeness, accuracy and timely submission for external use.
- Review and provide timely authorization of DATA Act files prior to submission.

### **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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

#### Reconciliation – Budgetary and Proprietary Account Relationships

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.

#### 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 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.

#### Document Numbering

All accounting entries recorded into Oracle require a transaction or document identification number. Oracle is configured to prevent 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.

### **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 the user can prepare and/or approve a manual JE. Oracle system controls require that all manual JEs be routed to an approver. Once a user has entered a JE, Oracle automatically routes it to an authorized approver's queue. Documentation supporting the JE accompanies each request for approval. The approver compares the documentation to Oracle and approves the JE or returns it to the preparer for revisions, if necessary.

Once a user submits a JE in OneStream XF, it becomes accessible for review and approval by any supervisor. Each approval request is accompanied by supporting documentation. The approver compares the documentation to OneStream XF and approves the JE or returns it to the preparer for revisions, if necessary.

#### **Document Numbering**

All accounting entries recorded into Oracle require a transaction or document identification number. Oracle is configured to assign all manual JEs a specific journal category and journal source. ARC has developed and implemented a standard document-numbering scheme.

#### **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 JEs 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 JEs that are initiated by the customer agency.

## **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.

#### **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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.

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.

### **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.

### **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).
- 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 submit requests to remove suppliers no longer needed in a timely manner.

## 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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.

### **Control Objective 15 – Sufficiently Funded Requisitions**

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

#### **Description of Controls**

ARC management has configured the automated contract writing system (PRISM) to enforce award approval limits for each Contracting Officer based on their assigned dollar thresholds, thereby preventing approvals that exceed their authorized levels. ARC management has configured PRISM 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.

## 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 an internal 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).

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:

- 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, resolves 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. 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, and 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.
- 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, resolves 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 USA Staffing Onboarding system, the EBB HR Assistant manually inputs the form into HRConnect. If the form is received within the USA Staffing 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.

### **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 EPP, an appropriate form, or USA Staffing Onboarding system.

Employees are encouraged, whenever possible, to initiate FEHB and TSP elections using EPP's self-service option so they are processed automatically and bypass ARC HR. When elections are received via the appropriate 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. If the form is received within the USA Staffing 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.

### 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 Fair Labor Standards Act (FLSA) status and the agency's policy for paying FLSA Exempt employees.
- Employee converted to a senior level position, depending on the employee's FLSA status and the agency's policy for paying FLSA-exempt employees.

A 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 via USA Staffing Onboarding as part of the onboarding process. The information electronically transmits to HRConnect, where a PAPB or EBB HR Assistant inputs and releases the payroll documents to NFC. The HR Assistant verifies the payroll documents applied in NFC and a different HR Assistant verifies the information in NFC is correct. If the payroll documents do not apply or apply incorrectly in NFC, the HR Assistant, along with assistance from an HR Specialist, resolve any issues. After PAYE runs, the PAPB HR Assistant 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 assistant inputs and releases the request in HRConnect. The assistant verifies the action applied in NFC and a different assistant verifies the information in NFC is correct. After PAYE runs, the assistant confirms that the employee was paid correctly by verifying the information in PINQ.

## 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/GovTA, ConcurGov, moveLINQ, IPP, OneStream XF, and HRConnect 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 using multifactor authentication (MFA). MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me. 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. Customer agencies are required to submit a formal request for account termination to revoke a user's access. At that time, the Oracle user access is end-dated in the system to remove their access within two business days. Oracle end users' access is monitored, and end dated after 90 days of inactivity by an external automated tool. ARC Oracle system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool. Annually, ARC generates a report listing Oracle system users to validate system users across ARC and each customer agency. The Service Desk Branch updates the permissions for users based on the responses received.

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 for the end user by Roles that determine the type of data (Financial, PRISM, Payroll) and Virtual Private Database to limit the data to specific orgs, sites and accounting values.

The Customer Support Division (CSD), Operation Support 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 occasionally require temporary access privileges as functional users to address user inquiries. An edit check prevents an ARC Oracle application administrator from adding or removing any responsibilities from their own user ID.

Administrative access to the underlying Oracle servers and databases is limited to OCSS 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 using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, or ID.me. 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. Customer agencies are required to submit a formal request for account termination in order to revoke a user's access. At that time, the PRISM user access is end-dated in the system to remove their access within two business days. Oracle end users' access is monitored, and end dated after 90 days of inactivity by an external automation tool. ARC PRISM system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool.

Annually, ARC generates an OBI report listing users for ARC and 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.

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 Responsibility Overview matrix to determine whether 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 CSD/OSD/SPSD employees requiring the access for the performance of job duties. 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/GovTA<sup>2</sup>

Access to webTA/GovTA was restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, ID.me or Login.gov. All personnel require access to webTA/GovTA 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/GovTA. 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/GovTA 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/GovTA access.

Annually, an HR administrator from the HR Systems Help Desk distributes a list of webTA timekeepers and supervisors to every customer agency, including ARC, to support their annual access review process. 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 also verifies agency users master timekeeper, master supervisor, and telework coordinator. 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. Updates are made to the users permissions based on the responses received. The HR Systems Help Desk also conducts a semi-annual review of users with Administrator and HR Administrator access. This review is to ensure that only authorized users in RTSB, LAB and HRSD have these roles.

User access within webTA/GovTA 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/GovTA 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

---

<sup>2</sup> The scope of the description of webTA/GovTA controls applies only to full service webTA/GovTA customer agencies.

granted HR specific roles with supervisor approval. Administrative access to the underlying webTA/GovTA servers and databases is limited to server and database administrators within the ISS.

### ConcurGov

Access to ConcurGov restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me. 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. A confirmation e-mail is sent to the user and agency travel contact(s) by the TSD helpdesk after the registration information is verified and the profile is created. The email instructs the traveler how to access ConcurGov.

Changes to a user's identification (i.e., name change) or to the user's role in ConcurGov requires an ARC System Access Form to be resubmitted, an e-mail from the user copying his/her Approving Official or agency travel contact, or an email directly from the user's 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 (including ARC) for review and verification of the accounts. Updates are made to user permissions based on the responses received.

### 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 using MFA that includes PIV credential or ID.me.
    - Once authentication is complete, the user is forwarded to the moveLINQ system if they have been configured for system access.
    - Users will be able to see their own records ONLY as configured in their access account, once the documents have had workflow started.
    - 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 whitelisted 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 must be signed by the customer agency approving official, the moveLINQ administrator that added the user and the reviewing moveLINQ administrator.
  - Access is granted using MFA.
    - 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.
    - 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 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 must 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 using MFA.
    - 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.
    - 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 using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, Login.gov or ID.me. 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. 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 by ARC.

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. Updates are made by ARC to user permissions based on the responses received. 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.

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

#### OneStream XF

Access to OneStream XF is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms 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. Customer agencies are required to submit a formal request for account termination to revoke a user's access. At that time, the OneStream XF user access is end-dated in the system to remove their access within two business days. OneStream XF end users' access is monitored, and end dated after 60 days of inactivity by an external automation tool. ARC OneStream XF system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool. 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.

## HRConnect

Users access HRConnect via MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, Login.gov or ID.me. 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 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.

User 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 HR Specialist 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 using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or Login.gov. 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 require a new access form to be submitted by the customer agency.

Semi-annually, an HR Specialist 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. 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.

## oneARC

Access to oneARC is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, Login.gov or ID.me. 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 can 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) every quarter. 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, provisioned with the identified permission sets, and provided access to one of three roles as determined by the customer agency authorizing official. Permission sets for external users are linked to each separate module. The three customer roles are User, Executive, or Manager. As part of agency setup, agencies must identify their authorization officers to receive the necessary permissions.

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 employee roles can be one of ARC User, ARC Supervisor, ARC Executive, or ARC Manager. Internal employees' access is also tied to a permission set that allows them to work their identified customer cases. To modify an internal user's access, 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/GovTA, 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, webTA/GovTA or USA Staffing 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.

### **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. OCSS provides notification to ARC of standard software releases, along with associated Release Notes outlining changes. Additionally, ARC processes customized application extension changes to Oracle. 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, OCSS 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/GovTA

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

When a new webTA/GovTA release is received from UKG, ARC RTSB, HRSD, 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/GovTA releases is restricted to the database and webTA/GovTA application administrators under the authority of ISS. The new webTA/GovTA release is not applied to production until it has been successfully tested and then approved by the HRSD Director.

## 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. 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 RTSB, PSS and ARAD staff test the new release in a separate test environment by running test scripts and analyzing the results. 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.

After the RPA developer completes the initial development of the change, testing is conducted in the Acceptance region of the RPA Management Console, a dedicated non-production environment. The developer then provides RPA output materials for Process Owner review. If satisfactory, the code then proceeds to a final peer code review. Once the code is 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.

### oneARC

Requests for changes to oneARC workflows are submitted by the business area responsible for the process. The oneARC Product Owner reviews and approves the change request and, if the request 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 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.

## **Control Objective 20 – Data Center Physical Access and Environmental Controls**

Controls provide reasonable assurance that the data center hosting webTA/GovTA servers has implemented appropriate safeguards to protect systems and data from unauthorized access and physical damage, or operational disruption resulting from environmental hazards

### Description of Controls

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.

### Fiscal Service Physical Controls

Fiscal Service has documented policies and procedures for controlling physical access to Fiscal Service buildings and to the data center used to host webTA/GovTA servers. These include:

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

The 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/GovTA 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.

Duly authorized vendors and employees 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, decide 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 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.

### **Control Objective 21 – Computer Operations**

Controls provide reasonable assurance that system problems and errors are recorded, analyzed, and resolved.

## Description of Controls

### 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/GovTA

webTA/GovTA support personnel have access to online documentation produced by UKG. 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.

### 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 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 CSD 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.

### **Control Objective 22 – 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**

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.

Differential backups of Network File Shares are created daily and retained for a period of 1 Year. Daily differential backups are written directly to the IBM Cloud Object Storage (ICOS). It will remain on the ICOS for the 1 Year retention period. The ICOS is distributed across three Fiscal Service physical locations.

### **webTA/GovTA**

Differential backups of WebTA/GovTA servers are created nightly and retained for a period of 90 days. Daily differential backups are replicated to Kansas City where they are kept for an additional 90 days.

## 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 receipt 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 provide approval of TIER submission.
- Review and provide authorization of 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 JEs that are initiated by the customer agency.
- Send valid and approved requests to record manual JEs 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, webTA/GovTA or USA Staffing authorized approvers.
- Review and approve listings of users with current Oracle, OBI, PRISM, webTA/GovTA, 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.

The CCACs listed above are also provided in Control Objectives 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16, and 18 in the “Management of Administrative Resource Center’s Control Objectives and Related Controls, and KPMG LLP’s Test of Operating Effectiveness and Results of Tests” 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 ARC's Oracle 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.

***Common Approach to Identity Assurance (CAIA)*** – Provides authentication and identification services to Fiscal Service applications.

## **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 a cloud-based 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 Customer Success Services (OCSS)*** – OCSS provides the computer processing, infrastructure and support for Oracle, OBI, and PRISM. OCSS 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 is a cloud based solution for financial consolidation and reporting, enabling the preparation/performance of financial statements, notes, and reconciliations. OneStream XF provides customers the ability to see draft statements, review reports and drill down on transactions to lower levels.

## **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.

## **MHS**

*moveLINQ* – moveLINQ is a 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 Financial Management 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 CAIA, CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA/GovTA.
- Responsible for granting, reviewing, and removing user access to CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, webTA/GovTA.
- 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/GovTA.
- Responsible for maintaining physical access and environment controls for CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA/GovTA.
- Responsible for performing data back-ups for CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and webTA/GovTA.
- 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/GovTA.

### **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, Control Objective 17 – Payroll Documents, and Control Objective 18 – System Access

- 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 and Control Objective 18 – System Access

- 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.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
1.01	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.	For a selection of days, inspected the corresponding reports used to identify Oracle obligation transactions to determine whether the obligation mismatches were reviewed and that actions were taken for documents identified on the reports.	No exceptions noted.
1.02	Upon receipt of a signed agreement or Misc Obligation Form from the customer agency and/or Procurement, the ARC technician responsible for processing the customer agency’s accounting transactions reviews the documentation to assess whether 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. If information provided by customer agency is insufficient, then the ARC technician will inquire with the customer agency.	For a selection of customer agencies, for a selection of manually-entered obligations, inspected the corresponding customer agency approvals to determine whether manually-entered obligations were approved prior to being entered into Oracle by ARC Staff.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
1.03	Daily, ARC reviews the OBI Status Report to identify and correct interface errors, with manual entry for transactions requiring correction. ARC Travel Services reconciles approved authorizations daily to assess whether the obligation was accurately processed into Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of days, inspected the corresponding ConcurGov to Oracle interface reconciliations to determine whether 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.	No exceptions noted.
1.04	RSB personnel enter PCS travel authorizations into moveLINQ which routes them to Approving Officials for review and approval. Once signed, relocation coordinators designate the document as “approved” in moveLINQ.	For a selection of days where travel authorizations could be entered, inspected the corresponding interface reconciliations to determine whether they were approved by an Approving Official.	No exceptions noted.
1.05	To assess accuracy of interfaced obligations, an accounting technician reconciles reports from moveLINQ and Oracle daily. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of days, inspected the corresponding reconciliations of travel authorizations from moveLINQ to Oracle to determine whether the interface activity was reconciled daily by an accounting technician, all approved travel authorizations in moveLINQ completely and accurately interfaced with Oracle, and any discrepancies identified were corrected.	No exceptions noted.
1.06	Budget execution settings are established by the customer agency and configured in Oracle by USB ARC staff. These system settings undergo an	For a selection of customer agencies, inspected the corresponding budget execution set-up configurations in Oracle to determine whether the	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent supervisory review to assess completeness and accuracy in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	settings were set-up in Oracle by ARC and ARC reviewed them with customer agencies within the past year, they were approved by a supervisor, and any discrepancies identified were corrected.	

**Control Objective 2 – Disbursements**

Controls provide reasonable assurance that non-payroll disbursements are authorized, complete, accurate, timely processed, and documented in accordance with ARC policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
2.01	A daily reconciliation is performed 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of days, inspected the corresponding reconciliation packages to determine whether daily reconciliations were performed, the approved IPP invoices successfully interfaced with Oracle, new awards or modifications for IPP vendors were successfully interfaced with IPP, and any discrepancies identified were corrected.	No exceptions noted.
2.02	Non-IPP invoices are either sent to ARC or directly to the customer agency. If invoices are sent to ARC, ARC reviews the invoice to confirm the customer agency provided approval via the oneARC application, or ARC forwards the invoice to an authorized agency contact for approval before ARC manually processes the obligation in Oracle.  If invoices are sent to the customer agency, the customer agency reviews and approves the invoice through the oneARC application.	For a selection of non-IPP transactions, inspected the corresponding invoices with customer agency authorization and related general ledger entries to determine whether invoices were authorized before processing.	No exceptions noted.
2.03	Oracle controls set at the user identification and/or vendor level help ensure that payment of	Observed an accountant process an invoice over \$2,500 to note whether the system automatically	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	non-IPP and RSB transactions 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.	placed the invoice on hold and routed it to a secondary lead accounting technician or an accountant for review and approval.	
2.04	A GLB accountant performs a review of all foreign payments prior to disbursement. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of foreign payments, inspected the corresponding invoices to determine whether a GLB accountant performed a review of the payment of the invoice and authorization before the disbursement was made and any discrepancies identified were corrected.	No exceptions noted.
2.05	ARC obtains customer agency approvals for IPACs that decrease an ARC customer agency's Fund Balance with Treasury (FBWT) in advance of the disbursement, 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 obtains customer agency approval after the IPAC has been recorded.	For a selection of IPAC disbursements, inspected the corresponding customer approvals to determine whether ARC obtained customer agency approvals prior to the disbursements made and said disbursements were posted in the proper accounting period, unless delaying posting would prevent posting in the proper accounting period, in which case approval was obtained after processing.	No exceptions noted.
2.06	Daily, ARC reviews OBI Status Reports to identify and correct interface errors, with manual entry for transactions requiring correction. ARC Travel Services reconciles approved vouchers daily to assess whether all ConcurGov vouchers	For a selection of customer agencies, for a selection of days, inspected the corresponding ConcurGov voucher reconciliations to determine whether approved vouchers in ConcurGov were reconciled to Oracle daily by an accounting	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	are properly interfaced and processed in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	technician, and any discrepancies identified were corrected.	
2.07	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.	For a selection of days, inspected the corresponding interface reconciliations to determine whether Relocation Technicians stamped the documents as approved.	No exceptions noted.
2.08	Approved vouchers in moveLINQ are reconciled by an Accounting Technician with an Oracle generated report to help ensure that all moveLINQ vouchers have been processed in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of days, inspected the corresponding reconciliations of travel authorizations from moveLINQ to Oracle to determine whether the reconciliations were performed, all moveLINQ vouchers were processed into Oracle, and any discrepancies identified were corrected.	No exceptions noted.
2.09	ARC reviews 10% of all invoices processed by IPP for each customer agency on a monthly basis.  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	For a selection of customer agencies, for a selection of months, inspected corresponding reviews of 10% of all processed invoices by IPP to determine whether the reviews were performed and discrepancies were resolved.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	services provided were within the period of performance authorized by the contract.		
2.10	Non-IPP invoices less than \$2,500 are subject to a monthly random sample post payment audit which is performed by accountant and approved by Lead Accountant.	For a selection of months, inspected the corresponding reviews of invoices of non-IPP invoices less than \$2,500, to determine whether the reviews were performed, reviews were subject to random sampling by a lead accounting technician or an accountant for post payment review, and discrepancies, if any, were addressed.	No exceptions noted.
2.11	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.	For a selection of months, inspected the corresponding 100% post audit management monthly reviews of invoices greater than \$2,500 that were processed and approved by the same individual to determine whether all such invoices were reviewed by a supervisor and discrepancies, if any, were addressed.	No exceptions noted.
2.12	<p>TSB staff completes post-payment audit reviews of TDY travel vouchers.</p> <p>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 equal to or greater than the sampling threshold (\$2,500 or \$1,000), trips with advances, trips showing duplicate M&amp;IE, and</p>	For a selection of customer agencies, for a selection of weeks, inspected the corresponding audit worksheets to determine whether the quality sampling was performed, that audit worksheets were completed for selected vouchers and reviewed, and that any errors were emailed to the traveler, document preparer, and/or Approving Official for review and necessary action.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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. All audit results are sent via e-mail to the primary agency travel point of contact(s) to review and/or take action. Errors are communicated via e-mail to the traveler, document preparer, and/or Approving Official for review and necessary action.	For a selection of customer agencies, for a selection of months, inspected the corresponding audit worksheets to determine whether the statistical sampling was performed, that audit worksheets were completed for selected vouchers and reviewed, and that any errors were emailed to the traveler, document preparer, and/or Approving Official for review and necessary action.	
2.13	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of days, inspected the corresponding reconciliations performed by the ARC SPS certifying officer to determine whether 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, the interfaces uploaded completely, and any discrepancies noted were resolved.	No exceptions noted.
2.14	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	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliations of SmartPay activity to determine whether the reconciliations were performed, reviewed, and that any differences were resolved.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	and the action, if any, that is needed to resolve the discrepancy.		
2.15	<p>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.</p> <p>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.</p> <p>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.</p>	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliations to determine whether accountants performed reconciliations of the CARS Account Statements and Undisbursed Appropriation Account Ledger Reconciliations, supervisory reviews were completed, and any discrepancies noted were resolved.	No exceptions noted.
2.16	Budget execution settings are established by the customer agency and configured in Oracle by USB ARC staff. These system settings undergo an annual review with the customer agency, followed	For a selection of customer agencies, inspected the corresponding budget execution set up configurations in Oracle to determine whether the settings were set-up in Oracle by USB staff, and	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	by input into Oracle by USB staff and a subsequent supervisory review to assess completeness and accuracy in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	ARC reviewed them with customer agencies within the past year.	
2.17	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 a selection of Treasury customer agencies, for a selection of quarters, inspected the corresponding non-fiduciary transaction confirmations completed by ARC accountants to determine whether reconciliations of transactions and balances with trading partners were completed, and that any necessary adjustments were identified and recorded.	No exceptions noted.
2.18	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 a selection non-Treasury customer agencies, for a selection of quarters, inspected the corresponding Intra-governmental Certified Explanation of Balances completed by ARC accountants to determine whether 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.	No exceptions noted.

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

Controls provide reasonable assurance that unfilled customer orders, receivables, and cash receipts are complete, accurate, timely processed, and documented in accordance with ARC policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
3.01	<p>ARC only processes unfilled customer orders, receivables, and cash receipts with customer agency approval.</p> <p>To help ensure that cash receipts are posted in the proper accounting period, ARC obtains customer agency approval after the cash receipt has been recorded.</p>	<p>For a selection of unfilled customer orders, inspected the corresponding customer agency approvals to determine whether ARC obtained customer agency approvals prior to processing the unfilled customer orders and said orders were posted in the proper accounting period, unless delaying posting would prevent posting in the proper accounting period, in which case approval was obtained after posting.</p> <p>For a selection of receivables, inspected the corresponding customer agency approvals to determine whether ARC obtained customer agency approvals prior to processing the receivables and said receivables were posted in the proper accounting period, unless delaying posting would prevent posting in the correct period, in which case approval was obtained after posting.</p> <p>For a selection of cash receipts, inspected customer agency approvals to determine whether ARC obtained customer agency approvals prior to processing the cash receipts and said receipts were</p>	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		only posted in the proper accounting period, unless delaying posting would prevent the cash receipt from posting in the correct period, in which case approval was obtained after posting.	
3.02	<p>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.</p> <p>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.</p>	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliations to determine whether accountants performed reconciliations of the CARS Account Statements and general ledger FBWT balances, reviews were completed, and any discrepancies noted were resolved.	No exceptions noted.
3.03	Accountants that are responsible for preparing the TROR and Debt Collection Activities report review and reconcile all activity (i.e., new receivables, revenue accruals, collections, adjustments and write-offs) with receivables due from the public on a quarterly basis. An ARC supervisory accountant reviews the report. If	For a selection of customer agencies, for a selection of quarters, inspected the corresponding TROR reports completed by ARC accountants to determine whether: they were completed, all activities were reconciled with receivables due from the public, the reports were reviewed by an ARC supervisory accountant, and any discrepancies noted were resolved.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	discrepancies arise, they are investigated, and corrective actions are taken as needed.		
3.04	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 a selection of Treasury customer agencies, for a selection of quarters, inspected the corresponding non-fiduciary transaction confirmations completed by ARC accountants to determine whether reconciliation of transactions and balances with trading partners was completed, and that any necessary adjustments were identified and recorded.	No exceptions noted.
3.05	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 a selection of non-Treasury customer agencies, for a selection of quarters, inspected the corresponding Intra-governmental Certified Explanation of Balances completed by ARC accountants to determine whether 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.	No exceptions noted.

**Control Objective 4 – Deposits**

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
4.01	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 to provide a formal record. 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of check deposit logs, inspected the corresponding checks received by the mailroom and the associated deposit check log to determine whether the deposit check log agreed to the original checks, an ARC administrative staff member, who did not have Oracle access to post account receivable transactions, logged all checks received in the branch’s check deposit log, and any discrepancies noted were resolved.	No exceptions noted.
4.02	The checks are locked in a secure location (safe) until they are ready to be deposited.	Observed the placement of badge readers and observed an individual attempt to access the Fiscal Services Building to note whether such access controls help prevent unauthorized persons from obtaining physical access to the building where the safe is located.	No exceptions noted.
4.03	Upon settlement with the FRB, the ARC accounting technician reconciles the batch list	For a selection of check deposit records, inspected the corresponding check attributes to determine	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	with the paper checks. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	whether the ARC accounting technician performed the reconciliation and discrepancies identified were addressed.	
4.04	<p>On the “deposit reporting and processing” side of OTCnet, an ARC accounting technician manually enters deposit information into the OTCnet system.</p> <p>Upon verification of the bank teller receipt and OTCnet confirmed deposit ticket against the retained copy, an ARC accounting technician records the cash receipt in Oracle. If discrepancies arise, they are investigated, and corrective actions are taken as needed.</p>	<p>For a selection of check deposits, inspected the corresponding posting to Oracle by ARC staff to OTCnet to determine whether the total checks were posted completely and accurately to Oracle.</p> <p>For a selection of check deposits, inspected the corresponding records to determine whether they were deposited and recorded in Oracle by an ARC staff member other than the individual who processed the deposit.</p>	No exceptions noted.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
5.01	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of months, inspected the corresponding monthly payroll accruals to determine whether the customer agencies' monthly payroll accruals were documented, entered timely and accurately, reversed, and reviewed monthly by an ARC accountant and supervisor and that any discrepancies identified were corrected.	No exceptions noted.
5.02	Leave accruals are recorded and reviewed based on an agreed upon schedule with the customer agency (monthly or quarterly) and reversed prior to recording the next scheduled leave accrual. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of months, inspected the corresponding leave accruals to determine whether the leave accruals were documented, entered timely and accurately, reversed, and reviewed monthly by an ARC accountant and supervisor and that any discrepancies identified were corrected.	No exceptions noted.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
6.01	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.	<p>For a selection of customer agencies, for a selection of pay periods, inspected the corresponding interface status reports to determine whether:</p> <ul style="list-style-type: none"> <li>• The payroll accountant reviewed said reports and corrected all of the transactions that did not properly interface with the system and contacted the customer agency for resolution of erroneous accounting codes, funding issues, or other circumstances that would prevent the payroll from being recorded.</li> <li>• Until the errors were cleared, the data was viewed as invalid and could not be posted to the general ledger.</li> </ul>	No exceptions noted.
6.02	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 resolves any differences identified. All those that	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliation of the payroll disbursements recorded in Oracle to the payroll disbursements as reflected in Treasury's cash systems to determine whether: the reconciliations were completed by an	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	require corrections are posted in either the current accounting period or in a subsequent accounting period.	ARC accountant, any differences identified were investigated and resolved, reconciliations were reviewed by a supervisory accountant, and differences requiring corrections were posted in the current or subsequent accounting periods.	

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
7.01	System administrators require authorization from a supervisor or manager to establish new posting models for transaction processing.	For a selection of models posted for transaction processing, inspected the corresponding approvals to determine whether system administrators obtained authorization from supervisors or managers prior to posting the models for transaction processing.	No exceptions noted.
7.02	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.	For a selection of newly established posting models, inspected the corresponding supervisory approvals of the new posting models and TFM/USSGL guidance to determine whether the new posting models were authorized and were in agreement with TFM/USSGL guidance.	No exceptions noted.
7.03	Accountants perform general ledger account reconciliations (utilizing Oracle, Excel, or other source files as subledgers) on balance sheet accounts to help ensure related accounting	For a selection of customer agencies, for a selection of months, inspected the corresponding general ledger account reconciliations completed by ARC accountants to determine whether: the	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	transactions were posted to the appropriate general ledger accounts. Upon completion, the subledger reconciliations are reviewed by a supervisor. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	general ledger accounts postings were completed for all recorded transactions, discrepancies identified were corrected by an accounting technician or accountant, and reconciliations were reviewed by an ARC supervisor.	
7.04	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.	For a selection of customer agencies, for a selection of months, inspected the corresponding budgetary-to- proprietary account relationship reconciliations completed by ARC accountants to determine whether the reconciliations were performed and reviewed by an ARC supervisor, general ledger accounts postings were completed for all recorded transactions, and invalid relationships identified were corrected by an accounting technician or accountant.	No exceptions noted.
7.05	ARC manually uploads the GTAS files created from Oracle for its non-Treasury customers into the GTAS system. ARC investigates and resolves any Treasury Appropriation Fund Symbol (TAFS) failed by the GTAS system.	Observed ARC staff manually load the GTAS files created from Oracle into the GTAS system to note whether Oracle and GTAS performed USSGL validations and no failures were identified.	No exceptions noted.
7.06	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	For a selection of customer agencies, for a selection of months, inspected the corresponding TIER Submission Checklists to determine whether ARC accountants reviewed GTAS edit reports and resolved any invalid attributes or out-	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	Checklist, which is further reviewed by a supervisor.	of-balance attributes included in corresponding TIER submissions.	
7.07	ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream XF tables on a quarterly basis to determine compliance with the TFM reporting requirements. ARC accountants investigate and resolve any differences between TFM crosswalks and ARC's internally prepared financial statements.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding TIER Submission Checklists to determine whether ARC accountants compared TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream XF tables to assess compliance with the TFM reporting requirements and investigated and resolved any differences identified during the comparison.	No exceptions noted.
7.08	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.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements to determine whether ARC accountants compared Treasury and DHS customer agencies' quarterly financial statements to ARC's internally prepared financial statements and resolved any differences, and comparisons were reviewed by a supervisor.	No exceptions noted.
7.09	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.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding results of ARC's comparison of the TFM financial statement crosswalk and internally prepared	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	financial statements to determine whether ARC accountants prepared the BS, SNC, and SCNP during the third and fourth quarters, and in the fourth quarter, the SBR and SCA are included, ARC accountants compared the OneStream XF Trail Balance to the Oracle trial balance and GTAS balance, comparisons were reviewed by a supervisor, and ARC investigated and resolved any differences.	
7.10	For Treasury and DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant and approved by the bureau CFO or designee prior to submission to Treasury. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.	For a selection of customer agencies, for Q4 FY24, inspected the corresponding financial statement variance analysis to determine whether ARC accountants prepared fourth quarter financial statement variance analyzes, such analyses were performed and reviewed by an ARC supervisor accountant and approved by the bureau CFO prior to submission to Treasury.	The following exception was noted:  For 1 of 5 FY24 Q4 financial statement reviews selected for testing, the ARC supervisor did not perform a financial statement variance review.
<p><u>Management's Response</u></p> <p>Management concurs with the exception and will initiate appropriate corrective actions.</p>			
7.11	For non-Treasury and non-DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement	For a selection of customer agencies, for Q4 FY24, inspected the corresponding financial statement variance analysis to determine whether	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant prior to submission to OMB. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.	ARC accountants prepared third and fourth quarter financial statement variance analyzes, and such analyses were performed and reviewed by an ARC supervisor accountant prior to submission to OMB.	

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
8.01	In the automated JE process method, accruals are recorded by using the automated JE 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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, inspected the corresponding manual JE templates of the period-end payroll accrual data loaded into Oracle to determine whether the entries were imported successfully, reviewed, posted to the general ledger, and any discrepancies noted were resolved.	No exceptions noted.
8.02	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. For the manual year-end accruals, a supervisor reviews and posts the accrual.	For a selection of manual JEs, inspected the corresponding manual JE templates of the non-invoice related expense accruals loaded into Oracle to determine whether the entries were reviewed and approved by a supervisory accountant.	No exceptions noted.
8.03	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	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliation of revenue and expense accrual balances in the general ledger to the subledger	The following exception was noted:  For 1 of 10 monthly reconciliations

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.	detail to determine whether ARC accountants prepared the reconciliation, a supervisor reviewed the reconciliation, and any differences noted were corrected by an accounting technician or accountant in a subsequent accounting period.	selected for testing, the ARC supervisor did not perform a review of the October 2024 reconciliation until June 2025, more than seven months after the month-end close.
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			
8.04	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, inspected the corresponding budget execution set-up configurations in Oracle to determine whether the settings were input in Oracle by ARC, ARC reviewed them with customer agencies within the past year, they were approved by a supervisor, and any discrepancies identified were corrected..	No exceptions noted.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
9.01	All fourth quarter GTAS submissions require certification by an ARC supervisor or manager, or other designated customer agency representative. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, inspected the corresponding fourth quarter GTAS submissions to determine whether selected submissions were reviewed and certified by an ARC supervisor/manager or customer agency representative, and any discrepancies identified were corrected.	No exceptions noted.
9.02	Supervisory accountants validate the TIER data to help ensure reporting deadlines are met by reviewing an accountant-prepared TIER Submission Checklist. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of months, inspected the corresponding TIER Submission Checklists to determine whether TIER submissions were reviewed by an ARC supervisor before being processed by TIER, and any discrepancies identified were corrected.	No exceptions noted.
9.03	ARC prepares monthly Prompt Payment reports for its customer agencies following Treasury guidelines. Independent accountants or analysts review all reports. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of months, inspected the corresponding review of the Prompt Payment reports to determine whether they were reviewed by an independent accountant or analyst before submission, and any discrepancies identified were corrected.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
9.04	ARC accountants compare TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream XF table on a quarterly basis to help assess compliance with the reporting requirements. ARC investigates and resolves any differences between TFM crosswalks and ARC's internally prepared financial statements.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding reconciliation of customer agencies' TFM financial statement crosswalks to ARC's internally prepared financial statements or OneStream XF table to determine whether the reconciliations were performed and any differences noted were resolved.	No exceptions noted.
9.05	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.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements to determine whether ARC performed the reconciliations, the reconciliation was reviewed by a supervisor, and any differences noted were investigated and resolved.	No exceptions noted.
9.06	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. If	For a selection of customer agencies, for a selection of quarters, inspected the corresponding results of ARC's comparison of the TFM financial statement crosswalk and internally prepared financial statements to determine whether ARC accountants prepared the BS, SNC, and SCNP during the third and fourth quarters, and in the fourth quarter, the SBR and SCA are included, ARC accountants compared the OneStream XF Trail Balance to the Oracle trial balance and	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	discrepancies arise, they are investigated, and corrective actions are taken as needed.	GTAS balance, comparisons were reviewed by a supervisor, and ARC investigated and resolved any differences.	
9.07	For Treasury and DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant and approved by the bureau CFO or designee prior to submission to Treasury. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.	For a selection of customer agencies, for Q4 FY24, inspected the corresponding financial statement variance analysis to determine whether ARC accountants prepared fourth quarter financial statement variance analyzes, such analyses were performed and reviewed by an ARC supervisor accountant and approved by the bureau CFO prior to submission to Treasury.	The following exception was noted:  For 1 of 5 FY24 Q4 financial statement reviews selected for testing, the ARC supervisor did not perform a financial statement variance review.
<p><u>Management's Response</u></p> <p>Management concurs with the exception and will initiate appropriate corrective actions.</p>			
9.08	For non-Treasury and non-DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2024, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by an ARC supervisory accountant prior to submission to OMB. However, the updated Circular A-136 issued in July 2025 removed this requirement for FY 2025, and the analyses are no longer necessary.	For a selection of customer agencies, for Q4 FY24, inspected the corresponding financial statement variance analysis to determine whether ARC accountants prepared fourth quarter financial statement variance analyzes, and such analyses were reviewed by an ARC supervisor accountant prior to submission to OMB.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
9.09	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, for a selection of quarters, inspected the corresponding TROR and Debt Collection Activities Reports to determine whether the reports were prepared by an ARC accountant, reviewed by an ARC supervisory accountant and any discrepancies identified were corrected.	No exceptions noted.
9.10	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 ("attestation statement"). Upon receipt of the customer agency monthly attestation statement, 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.	<p>For a selection of non-Treasury and non-Homeland Security customer agencies, for a selection of months, inspected the corresponding DATA act files to determine whether the customer agencies' monthly DATA Act submissions were completed, reviewed, and authorized by the customer agency prior to being timely submitted in the DATA Act Broker.</p> <p>For a selection of non-Treasury and non-Homeland Security customer agencies, for a selection of quarters, inspected the corresponding DATA act submissions to determine whether the customer agencies certified the three monthly DATA Act submissions for the selected quarter.</p>	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	ARC updates the status of the three monthly DATA Act File submissions to “Certified” on behalf of the customer agency.		

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
10.01	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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.	For a selection of customer agencies, inspected the corresponding budget execution set-up configurations in Oracle to determine whether the settings were set-up in Oracle by ARC and ARC reviewed them with customer agencies within the past year, they were approved by a supervisor, and any discrepancies identified were corrected.	No exceptions noted.
10.02	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.	For a selection of customer agencies, for a selection of months, inspected the corresponding budgetary-to-proprietary account relationship reconciliations completed by ARC accountants to determine whether: 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.	No exceptions noted.
10.03	ARC accountants perform monthly reconciliations of CARS Account Statement balances to general ledger FBWT balances which are reviewed by	For a selection of customer agencies, for a selection of months, inspected the corresponding reconciliations to determine whether accountants performed reconciliations of the CARS Account	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>ARC staff other than the individual performing the reconciliation.</p> <p>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.</p>	<p>Statements and general ledger FBWT balances, reviews were completed, and any discrepancies noted were resolved.</p>	

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
11.01	Documentation supporting the JE accompanies each request for approval. The approver compares the documentation to Oracle and approves the JE or returns it to the preparer for revisions, if necessary.	For a selection of customer agencies, for a selection of manual JEs, inspected the corresponding support for JEs to determine whether each manual JE had supporting documentation that was compared to Oracle and was approved by a supervisor.	No exceptions noted.
11.02	Once a user submits a JE in OneStream XF, it becomes accessible for review and approval by any supervisor. Each approval request is accompanied by supporting documentation. The approver compares the documentation to OneStream XF and approves the JE or returns it to the preparer for revisions, if necessary.	For a selection of customer agencies, for a selection of manual JEs, inspected the corresponding support for JEs to determine whether each manual JE had supporting documentation that was compared to OneStream XF and was 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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
12.01	<p>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.</p> <p>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.</p> <p>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).</p>	<p>For a selection of customer agencies, inspected the corresponding investment instructions to determine whether they were documented, provided to ARC, and defined the investment objectives for the agencies.</p> <p>For a selection of investment purchases, inspected the corresponding investment purchase review documentation to determine whether the investment purchases were reviewed by ARC staff other than the individual who processed the investment purchase, and any discrepancies identified were followed up on.</p>	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
12.02	<p>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. If discrepancies arise, they are investigated, and corrective actions are taken as needed.</p>	<p>For a selection of days, inspected the corresponding daily reconciliation of investment account transactions within FedInvest to the dollar amounts recorded in Oracle to determine whether reconciliations were performed, and any discrepancies noted during the reconciliation were addressed.</p>	<p>No exceptions noted.</p>
12.03	<p>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.</p> <p>Once the reconciliation is complete, it is reviewed by a supervisory ARC accountant.</p> <p>If discrepancies exist with either reconciliation, research is conducted to determine the cause, adjust investments if necessary, and document corrective actions.</p>	<p>For a selection of customer agencies, for a selection of months, inspected the corresponding investment reconciliations to determine whether investment activity was reconciled, reviewed by a supervisory ARC accountant, and any discrepancies noted during the reconciliation were addressed.</p>	<p>No exceptions noted.</p>

### 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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
13.01	<p>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.</p> <p>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.</p>	<p>Inspected a list of Oracle users with access to make changes to Supplier and Bank records and their corresponding job titles, to determine whether users had the appropriate privileges as they were commensurate with their roles and responsibilities.</p> <p>Inspected a list of Oracle users with access to process vendor payments to determine if users have access to both process vendor payments and make changes to Supplier and Bank records.</p>	No exceptions noted.
13.02	<p>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.</p>	<p>For a selection of days, inspected the corresponding audit reports signed by the reviewing ARC staff to determine whether the Supplier and Bank record changes were reviewed and approved, and any discrepancies identified were corrected.</p>	<p>The following exception was noted:</p> <p>Management was unable to provide evidence of the secondary review of changes to Supplier and Bank records for 5 of 15 days selected for testing.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
<u>Management's Response</u> Management concurs with the exception and will initiate appropriate corrective actions.			

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
14.01	The acquisition file documentation is reviewed by a warranted Contracting Officer. If discrepancies arise, they are investigated, and corrective actions are taken as needed. 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.	For a selection of acquisitions awarded, inspected the corresponding award document, and award recommendation, award summary, vendor matrix, or procurement checklist to determine whether the award was signed by a warranted Contracting Officer acting within their approval threshold to certify that the documents were complete and accurate, met procurement and regulatory requirements, and any discrepancies identified were resolved.	No exceptions noted.

**Control Objective 15 – Sufficiently Funded Requisitions**

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
15.01	ARC management has configured the automated contract writing system (PRISM) to enforce award approval limits for each Contracting Officer based on their assigned dollar thresholds, thereby preventing approvals that exceed their authorized levels.	Inquired of management and inspected award authorizations in PRISM and the list of warranted Contracting Officers to determine whether warranted Contracting Officers were only able to approve awards within their assigned dollar thresholds.	The following exception was noted:  Management was unable to provide evidence of a valid warrant for 1 of 30 individuals assigned the Contracting Officer role in PRISM. As a result, the individual was assigned the role without proper authority.
<p><u>Management’s Response</u></p> <p>Management concurs with the exception and will initiate appropriate corrective actions.</p>			
15.02	ARC management has configured PRISM controls to prevent procurement awards from being made without sufficient funding.	Observed an ARC staff member attempt to process a procurement award in PRISM for amount greater than the funding provided to note whether the system prevented the procurement award from being made.	No exceptions noted.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
16.01	<p>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.</p> <p>An EBB Specialist reviews the hire to determine eligibility for Retirement, Federal Employees Health Benefits (FEHB) and Federal Employees’ Group Life Insurance (FGLI), and provides the information via an internal database or the USA Staffing Onboarding. A PAPB HR Assistant then utilizes the New Hire Checklist, and other supporting documentation, to code and release the personnel action in HRConnect.</p> <p>The PAPB HR Assistant verifies the action</p>	<p>For a selection of new employee personnel actions in HRConnect, inspected the corresponding new hire checklists to determine whether new employee personnel actions were documented, reviewed, authorized, and correctly applied.</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p> <p>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.</p> <p>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.</p>		
16.02	<p>Depending on the category, the personnel action is authorized by EBB, WRB, or PAPB:</p> <p>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</p>	<p>Inspected the corresponding Fiscal Service HR separation listing and the ARC HRConnect active employee listing to determine whether there were no separated employees who retained access to HRConnect.</p> <p>For a selection of separating employee personnel actions in HRConnect, inspected the corresponding separation request documentation</p>	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p> <p>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.)</p> <p>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.</p> <p>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</p>	<p>to determine whether the requested actions were reviewed, approved and carried out by the appropriate personnel.</p>	

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	PAPB HR Assistant verifies the information in NFC is correct.		
16.03	<p>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.</p> <p>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.)</p> <p>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.)</p> <p>All personnel actions related to Pathways employees are reviewed and coded by a PAPB</p>	For a selection of customer agencies, for a selection of maintenance employee personnel action requests, inspected the corresponding personnel action forms to determine whether the requests were reviewed, approved, and correctly applied by the appropriate personnel.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>HR Assistant. The PAPB HR Assistant forwards the personnel action to an ESD Specialist for final review and approval.</p> <p>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.</p> <p>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.</p> <p>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.</p>		
16.04	<p>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</p>	<p>For a selection of FEGLI elections, inspected the corresponding related Life Insurance Election forms to determine whether eligibility was verified and certified by an EBB Specialist, and the action was correctly applied.</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	requests documentation to verify the employee's eligibility.		

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
17.01	When elections are received via the appropriate 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. 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.	For a selection of customer agencies, for a selection of FEHB and TSP elections, inspected the corresponding FEHB and TSP election forms and NFC screenshots to determine whether the forms were verified by an EBB Specialist and that the election was correctly applied.	No exceptions noted.
17.02	Employees receive payment for unused annual leave and compensatory time when they meet any of the following criteria:	For a selection of customer agencies, for a selection of employees who received payment for unused annual leave or compensatory time, inspected the corresponding approval forms,	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p> <p>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.</p>	<p>payment reports, timecards, verification payments, and NFC screenshots to determine whether approvals were obtained, criteria were met, and the employee was appropriately paid.</p>	
17.03	<p>The information electronically transmits to HRConnect, where a PAPB or EBB HR Assistant inputs and releases the payroll documents to NFC. The HR Assistant verifies the payroll documents applied in NFC and a different HR Assistant verifies the information in NFC is correct. If the</p>	<p>For a selection of customer agencies, for a selection of written employee requests for payroll changes and/or deductions submitted to PAPB, inspected the corresponding approval forms, HRC screenshots and NFC screenshots to determine</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>payroll documents do not apply or apply incorrectly in NFC, the HR Assistant, along with assistance from a HR Specialist, resolve any issues. After PAYE runs, the PAPB HR Assistant confirms that the employee was paid correctly by verifying the information in PINQ.</p> <p>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 assistant inputs and releases the request in HRConnect. The assistant verifies the action applied in NFC and a different assistant verifies the information in NFC is correct.</p>	<p>whether the request was submitted, approved (if needed) and correctly applied.</p>	

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
<b>Oracle and OBI</b>			
18.01	Access to Oracle and OBI are restricted to users using multifactor authentication (MFA). MFA is accomplished utilizing Common Approach to Identity Assurance (CAIA) mechanisms PIV credentials or ID.me.	Observed an Oracle logon session to note whether the user was required to use CAIA in order to authenticate.	No exceptions noted.
18.02	Prospective Oracle users must complete, sign, and submit an approved Administrative Resource Center System Access Form for End User Applications to request access to Oracle. The end user’s signature indicates that they are familiar with the Privacy Act information and security requirements and will comply with the 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.	For a selection of new Oracle users, inspected the corresponding user access request forms to determine whether the forms were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as authorized.	No exceptions noted.
18.03	Changes to existing Oracle user profiles require an e-mail to be sent to the Oracle Support Team mailbox by an authorized individual requesting	For a selection of changes to Oracle user profiles, inspected the corresponding authorizing documentation to determine whether updates to	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	the change and defining what access should be added/deleted/changed.	access rights were authorized and access was granted as authorized.	
18.04	Customer agencies are required to submit a formal request for Oracle account termination in order to revoke a user's access. At that time, the Oracle's user access is end-dated in the system to remove their access within 2 business days.	For a selection of requests for the termination of Customer Agency employees' Oracle access, inspected the corresponding Oracle Terminations listing and access removal requests to determine whether the requests for the termination of access were completed and removal of access was performed in a timely manner.	No exceptions noted.
18.05	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. On a daily basis, Oracle inactivity reports are reviewed.	For a selection of days, inspected the corresponding daily Oracle inactivity reports to determine whether the reports were reviewed.	No exceptions noted.
18.06	Annually, ARC generates a report listing Oracle system users to validate system users across ARC and each customer agency. The Service Desk Branch updates the permissions for users based on the responses received.	For a selection of customer agencies, inspected the corresponding annual Oracle user access review to determine whether the annual reviews were performed changes provided by the customer agencies were applied.	No exceptions noted.
18.07	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	Inspected a listing of user accounts and user access in Oracle to determine whether each user's access is restricted to distinct operating units or customer agency.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	(ledger) or multiple ones. For OBI, data access is restricted for the end user by Roles that determine the type of data (Financial, PRISM, Payroll) and Virtual Private Database (VPD) to limit the data to specific orgs, sites and accounting values.		
18.08	The Customer Support Division (CSD), Operation Support 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.	Inspected the corresponding user roles assigned to Oracle application administrators and compared them to the BTD Allowable Responsibilities Table to determine whether the functional user permissions were restricted and commensurate with job responsibilities.	No exceptions noted.
18.09	Individuals with ARC Oracle application administrator privileges perform multiple functions, including that of the Oracle Support Team members. As a result, these individuals occasionally require temporary access privileges as functional users to address user inquiries.	Inspected the corresponding configuration settings in Oracle to determine whether the rule was set to prevent the ARC Oracle application administrator from adding or removing responsibilities from their own user ID.  Observed an ARC Oracle application administrator attempt to add responsibilities to his/her user ID to note whether the application	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		automatically blocked the attempt to add responsibilities to the user's ID.	
<b>PRISM</b>			
18.10	Access to PRISM is restricted to users using multifactor MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, Login.gov, or ID.me.	Observed a PRISM logon session to note whether the user was required to use CAIA in order to authenticate.	No exceptions noted.
18.11	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 the 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.	For a selection of new PRISM users, inspected the corresponding user access request forms to determine whether the forms were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as authorized.	The following exception was noted:  Management was unable to provide evidence that 1 of 30 contracting officers held a valid warrant. As a result, a contracting officer was granted the contracting officer role in PRISM without a valid warrant.
<p><u>Management's Response</u></p> <p>Management concurs with the exception and will initiate appropriate corrective actions.</p>			

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.12	Changes to existing PRISM 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.	For a selection of changes to PRISM user accounts, inspected the corresponding authorizing documentation to determine whether updates to the accounts were authorized and access was granted as authorized.	No exceptions noted.
18.13	Customer agencies are required to submit a formal request for PRISM account termination to revoke a user's access. At that time, the PRISM user's access is end-dated in the system to remove their access within 2 business days.	For a selection of requests for the termination of customer agency employees' inspected the corresponding internal PRISM access to determine whether the requests for the termination of access were completed and removal of access was performed in a timely manner.	No exceptions noted.
18.14	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. On a daily basis, Oracle inactivity reports are reviewed.	For a selection of days, inspected the corresponding daily PRISM inactivity reports to determine whether the reports were reviewed.	No exceptions noted.
18.15	Annually, ARC generates an OBI report listing users for ARC and 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.	For a selection of customer agencies, for a selection of user account reviews, inspected the corresponding customer agencies' annual PRISM user access review and the system-generated user access list to determine whether the user access lists were provided to customer agencies for	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		review and changes provided by the customer agencies were applied.	
18.16	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 set up 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.	Inspected the corresponding PRISM user listing to determine whether the roles/responsibility of users to make changes was limited to the appropriate group.	No exceptions noted.
18.17	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 Responsibility Overview 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.	For a selection of changes to PRISM functional access privileges, inspected the corresponding access requests to determine whether SDB reviewed the changes and deemed the changes were appropriate.	No exceptions noted.
18.18	The system administrator responsibility in PRISM is limited to certain employees requiring the access for the performance of their job duties.	Inspected the corresponding PRISM user listing to determine whether individuals with the system	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		administrator responsibility were appropriate and from the group that were allowed to have this role.	
<b>WebTA</b>			
18.19	Access to webTA is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, Login.gov, or ID.me.	Observed a webTA logon session to note whether the user was required to use CAIA.	No exceptions noted.
18.20	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.	For a selection of new webTA users with elevated privileges, inspected the corresponding user access request forms to determine whether the forms were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as authorized.	No exceptions noted.
18.21	Changes to existing webTA elevated access require a new access form to be submitted by the customer agency.	For a selection of changes to existing webTA users with elevated privileges, inspected the corresponding user access request forms to determine whether forms were completed, access was authorized, and access was granted as authorized.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.22	<p>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.</p>	<p>For a selection of access removal requests for webTA and webTA Fiscal Service elevated users, inspected the corresponding access removal requests to determine whether a HR administrator from the HR Systems Help Desk removed any access.</p>	<p>No exceptions noted.</p>
18.23	<p>Annually, an HR administrator from the HR Systems Help Desk distributes a list of webTA timekeepers and supervisors to every customer agency, including ARC, to support their annual access review process. The review also verifies agency users master timekeeper, master supervisor, and telework coordinator. 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. Updates are</p>	<p>For a selection of customer agencies, inspected the corresponding evidence of the annual distribution of the list of timekeepers and supervisors sent out to each customer agency, and evidence of the customer agency's response to determine whether annual access reviews were completed and access changes identified by customer agencies were applied.</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	made to user permissions based on the responses received.		
18.24	The HR Systems Help Desk also conducts a semi-annual review of users with Administrator and HR Administrator access. This review is to ensure that only authorized users in RTSB, LAB and HRSD have these roles.	For a selection of semi-annual reviews of privileged users, inspect the corresponding evidence of the review to determine whether semi-annual access reviews were completed and that only authorized users in RTSB, LAB and HRSD have privileged access.	No exceptions noted.
18.25	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.	Inspected the corresponding webTA user listing to determine whether users are not assigned to both the HR administrator and system administrator roles.	No exceptions noted.
18.26	Periodically, there is a need for the webTA 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.	Inspected the listing of WebTA modified users to determine whether system administrators were granted an HR Role in production.	No system administrators were provisioned temporary access during the reporting period. As a result, we were unable to conclude on the operating effectiveness of this control.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.27	Administrative access to the underlying webTA servers and databases is limited to server and database administrators within the ISS.	<p>Inspected the corresponding webTA user listing to determine whether users are not assigned both the HR administrator and system administrator roles.</p> <p>Inspected a listing of webTA user accounts with administrative access to the underlying webTA databases and organizational chart to determine whether administrative access was limited to database administrators within ISS.</p>	No exceptions noted.
<b>GovTA</b>			
18.28	Access to GovTA was restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, Login.gov, or ID.me.	Observed a GovTA logon session to note whether the user was required to use CAIA.	No exceptions noted.
18.29	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	For a selection of new GovTA users with elevated privileges, inspected the corresponding user access request forms to determine whether the forms were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as authorized.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	specifications, which will allow the user to perform his/her duties in GovTA.		
18.30	Changes to existing GovTA elevated access require a new access form to be submitted by the customer agency.	For a selection of changes to existing GovTA users with elevated privileges, inspected the corresponding user access request forms to determine whether forms were completed, access was authorized, and access was granted as authorized.	No exceptions noted.
18.31	Upon receipt of an Administrative Resource Center System Access Form for End User Applications requesting the deletion of a GovTA 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 GovTA access.	Inspected the GovTA modifications listing to determine whether users were removed during the reporting period,	No GovTA users were terminated during the reporting period. As a result, we were unable to conclude on the operating effectiveness of this control.
18.32	Annually, an HR administrator from the HR Systems Help Desk distributes a list of GovTA timekeepers and supervisors to every customer agency, including ARC, to support their annual access review process. The list is limited to those	Inquired of management to determine whether the GovTA annual review was performed during the reporting period.	The GovTA annual recertification was not performed during the reporting period. As a result, we were

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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. Updates are made to user permissions based on the responses received.		unable to conclude on the operating effectiveness of this control.
18.33	The HR Systems Help Desk also conducts a semi-annual review of users with Administrator and HR Administrator access. This review is to ensure that only authorized users in RTSB, LAB and HRSD have these roles.	Inquired of management to determine whether the GovTA semi-annual review was performed during the reporting period.	The GovTA privileged user semi-annual recertification was not performed during the reporting period. As a result, we were unable to conclude on the operating effectiveness of this control
18.34	User access within GovTA 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 GovTA are limited to certain employees, ensuring no one serves in both administrator roles.	Inspected the corresponding GovTA user listing to determine whether users are not assigned to both the HR administrator and system administrator roles.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.35	Periodically, there is a need for the GovTA 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.	Inspected the listing of GovTA modified users to determine whether system administrators were granted an HR Role in production during the reporting period.	No system administrators were provisioned temporary access during the reporting period. As a result, we were unable to conclude on the operating effectiveness of this control.
18.36	Administrative access to the underlying GovTA servers and databases is limited to server and database administrators within the ISS.	Inspected a listing of GovTA user accounts with administrative access to the underlying GovTA servers and organizational chart to determine whether administrative access was limited to server administrators within ISS.	No exceptions noted.
<b>ConcurGov</b>			
18.37	Access to ConcurGov is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me.	Observed a user access the ConcurGov system to note whether the user was required to use CAIA in order to authenticate.	No exceptions noted.
18.38	All ConcurGov 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	For a selection of new ConcurGov users, inspected the corresponding user access request forms and e-mails to determine whether the forms	As it relates to the first procedure, no exceptions were noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p>	<p>or e-mails were completed, and access was granted as requested.</p> <p>For the new ConcurGov users referenced in the test above, inspected corresponding user access forms and emails to determine whether any users were Budget Reviewers or Approving Officials.</p>	<p>As it relates to the second procedure, no Budget Reviewers or Approving Officials were included among the new ConcurGov users selected for testing. As a result, we were unable to conclude on the operating effectiveness of this aspect of the control.</p>
18.39	<p>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, an e-mail from the user copying his/her Approving Official or agency travel contact, or an email directly from the user's Approving Official or agency travel contact.</p>	<p>For a selection of changes to ConcurGov users, inspected the corresponding authorizing documentation to determine whether access changes were documented, access was authorized, and authorized access matched that which was configured in ConcurGov.</p>	<p>No exceptions noted.</p>
18.40	<p>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.</p>	<p>For a selection of employee terminations requests made for Fiscal Service employees and termination requests made from customer agencies, inspected the corresponding ConcurGov access removal requests and the ConcurGov</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		access list to determine whether ConcurGov access was removed.	
18.41	On an annual basis, TSD staff create and distribute reports of ConcurGov users and distributes to customer agency (including ARC) Travel contacts for review and verification of the accounts. Updates are made to user permissions based on the responses received.	For a selection of customer agencies, inspected the corresponding evidence of the ConcurGov user reports distributed to customer agency Travel contracts to determine whether each customer agency completed an annual user access review/verification and changes provided by the customer agencies were applied.	No exceptions noted.
<b>moveLINQ – Employee Portal</b>			
18.42	Access to moveLINQ Employee Portal is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me.	Observed a user login to moveLINQ’s web-based Employee Portal to note if they were required to authenticate via MFA.	No exceptions noted.
18.43	New/modified user moveLINQ Employee Portal accounts are created with the receipt of a Request for Relocation provided by the customer agency Contact.	For a selection of new/modified moveLINQ users, inspected the corresponding access forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted
18.44	moveLINQ Employee Portal access is removed once all relocation records have been deleted from the system.	For a selection of Fiscal Service users’ and customer users’ termination requests for moveLINQ, inspected the corresponding moveLINQ System User Audit Report to	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		determine whether the removal of access was documented and performed.	
18.45	Users will be able to see their own records only as configured in their access account, once the documents have had workflow started.	Inspected the corresponding moveLINQ user list to determine whether users do not have conflicting roles that create a separation of duties issue.	No exceptions noted.
<b>moveLINQ – Agency Contract/Approval Portal</b>			
18.46	Access to moveLINQ Approval Portal is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanism PIV credentials.	Observed a user login to moveLINQ’s web-based Approval Portal to note if they were required to authenticate via MFA.	No exceptions noted.
18.47	New/modified moveLINQ Approval Portal 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 must be signed by the customer agency approving official, the moveLINQ administrator that added the user and the reviewing moveLINQ administrator.	For a selection of new/modified moveLINQ users, inspected the corresponding access forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.
18.48	To remove a user’s moveLINQ Approval Portal account, customer agencies submit a request for account termination. At that time, the moveLINQ	For a selection of Fiscal Service users’ and customer agency users’ termination requests for moveLINQ, inspected the corresponding moveLINQ System User Audit Reports to	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	Approval Portal user account is disabled in the system.	determine whether the removal of access was documented and performed.	
18.49	moveLINQ Approval Portal 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.	Inspected the corresponding moveLINQ user list to determine whether users do not have conflicting roles that create a separation of duties issue.	No exceptions noted.
<b>moveLINQ – Expense Management Portal</b>			
18.50	Access to moveLINQ Expense Management Portal is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanism PIV credentials.	Observed a user login to moveLINQ’s web-based Expense Management Portal to note if they were required to authenticate via MFA.	No exceptions noted.
18.51	New/modified moveLINQ Expense Management Portal 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 must be signed by a supervisor, the moveLINQ administrator that added the user, and the reviewing moveLINQ Branch Manager or System Owner (SO).	For a selection of new/modified moveLINQ users, inspected the corresponding access forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.52	To remove a user's moveLINQ Expense Management Portal account customer agencies submit a request for account termination. At that time, the moveLINQ Expense Management Portal user account is disabled in the system.	For a selection of Fiscal Service users' and customer users' termination requests for moveLINQ, inspected the corresponding moveLINQ System User Audit Reports, to determine whether the removal of access was documented and performed.	No exceptions noted.
18.53	moveLINQ Expense Management Portal 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.	Inspected the corresponding moveLINQ user list to determine whether users do not have conflicting roles that create a separation of duties issue.	No exceptions noted.
<b>IPP</b>			
18.54	Access to IPP is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me.	Observed an IPP user login to the web-based system to note whether the user was required to use CAIA.	No exceptions noted.
18.55	Internal and external IPP 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,	For a selection of new IPP accounts, inspected the corresponding access forms to determine whether access requests were documented, employees acknowledged that they understood the Privacy Act requirements, access was approved, and access was configured as authorized.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p> <p>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.</p>		
18.56	<p>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 by ARC.</p>	<p>For a selection of employee termination requests made from customer agencies and for Fiscal Service users, inspected the corresponding user access termination requests to determine whether employees did not retain access to IPP after their termination date.</p>	<p>No exceptions noted.</p>
18.57	<p>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. Updates are made by ARC to user</p>	<p>For a selection of customer agencies, inspected the corresponding annual account recertification for IPP supporting documentation to determine whether ARC contacted customer agencies to initiate the recertifications, and results were</p>	<p>No exceptions noted.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	permissions based on the responses received. 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.	returned to FRB St. Louis so that access changes could be applied as necessary.  Inspected the corresponding ARC/Fiscal Service IPP user recertification to determine whether it was completed and sent to FRB St. Louis.	
18.58	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	Inspected the corresponding IPP user listing to determine whether users are not assigned conflicting roles.	No exceptions noted.
<b>OneStream XF</b>			
18.59	Access to OneStream XF is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me.	Observed a OneStream XF user log in to note whether the user was required to use CAIA.	No exceptions noted.
18.60	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	For a selection of new OneStream XF users, inspected the corresponding user access request forms to determine whether the requests were documented, employees acknowledged that they understood the Privacy Act requirements, access	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.	was approved, and access was configured as authorized.	
18.61	Changes to existing OneStream XF 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.	For a selection of employee changes to OneStream XF users, inspected the corresponding user access request forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.
18.62	Customer agencies are required to submit a formal request for account termination in order to revoke a user's access. At that time, the OneStream XF user access is end-dated in the system to remove their access within 2 business days.	For a selection of employee termination requests made from customer agencies and Fiscal Service, inspected the corresponding email requests and inactivity reports to determine whether the termination of access was completed and removal of access was performed in a timely manner.	No exceptions noted.
18.63	OneStream XF end users' access is monitored, and end dated after 60 days of inactivity by an external automation tool. ARC OneStream XF system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool. On a daily basis, OneStream XF inactivity reports are reviewed.	For a selection of days, inspected the corresponding OneStream XF inactivity reports to determine whether the reports were reviewed.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.64	Annually, ARC generates a report listing OneStream XF 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.	<p>Inspected the corresponding HUD annual account recertification and the system-generated user access list to determine whether 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.</p> <p>Inspected the corresponding ARC/Fiscal Service OneStream XF IPP user recertification to determine whether ARC Service Branch Desk completed OneStream XF IPP user recertification and modifications were made as needed.</p>	No exceptions noted.
18.65	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.	Inspected access levels within OneStream XF to determine whether access levels were restricted by cubes.	No exceptions noted.
18.66	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.	Inspected the corresponding listing of OneStream XF administrators and the Fiscal Service personnel listing to determine whether all administrators were OSD/SPSD employees.	No exceptions noted.
<b>HRCconnect</b>			

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.67	Users' access HRConnect via MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, Login.gov or ID.me.	Observed a HRConnect user log in to note whether the user was required to use CAIA.	No exceptions noted.
18.68	HRConnect users that require elevated access (e.g., admin, HR and PDS roles) are given that level of access following receipt of an Administrative Resource Center System Access Form for End User Application signed by the agency's authorized approver. The end user's signature indicates they are familiar with the Privacy Act information and security requirements and will comply with computer security rules. The form defines the user's access specifications, which will allow the user to perform his/her duties in HRConnect.	For a selection of new or modified access changes to HRConnect users with elevated privileges, inspected the corresponding user access request forms to determine whether the requests were documented, employees acknowledged that they understood the Privacy Act requirements, access was approved, and access was configured as authorized.	No exceptions noted.
18.69	Changes to existing HRConnect elevated access requires a new access form to be submitted by the customer agency.	For a selection of new or modified access changes to HRConnect users with elevated privileges, inspected the corresponding user access request forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.
18.70	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	For a selection of employee terminations, inspected the corresponding requests and HRConnect access list to determine whether the	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	agency, the HR Systems Help Desk removes any elevated access from existing users.	removal of access was documented and performed.	
18.71	Semi-annually, an HR Specialist on the HR Systems Help Desk sends out a list of HRConnect 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.	For a selection of customer agencies, inspected the corresponding customer agencies annual HR Connect user access review and associated system-generated access lists to determine whether the lists were provided to customer agencies for review and changes provided by the customer agencies were applied.	No exceptions noted.
<b>USA Staffing</b>			
18.72	Access to USA Staffing Onboarding is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or Login.gov.	Observed a user access USA Staffing to note whether the user was required to use CAIA.	No exceptions noted.
18.73	Users that require USA Staffing 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	For a selection of new or modified access changes to USA Staffing Onboarding users with elevated privileges, inspected the corresponding user access request forms, to determine whether access was documented, employees acknowledged that they understood the Privacy Act requirements,	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.	access was approved, and access was configured as authorized.	
18.74	Changes to existing USA Staffing elevated access requires a new access form to be submitted by the customer agency.	For a selection of new or modified access changes to USA Staffing Onboarding users with elevated privileges, inspected the corresponding user access request forms, to determine whether access was documented, approved, and access was configured as authorized.	No exceptions noted.
18.75	Semi-annually, an HR Specialist on the HR Systems Help Desk sends out a list of USA Staffing 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.	<p>For a selection of customer agencies, inspected the corresponding semi-annual account recertification and user access list to determine whether 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.</p> <p>Inspected the corresponding ARC/Fiscal Service USA Staffing Onboarding user recertification to determine whether HR Systems Help Desk completed the user recertification and modifications were made as needed.</p>	<p>The following exception was noted:</p> <p>For 1 of 5 USA Staffing semi-annual reviews selected for testing, users who could not be verified by the HR Systems Help Desk were not removed as required by policy.</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			
18.76	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.	For a selection of employee termination requests made from customer agencies and from Fiscal Service, inspected the corresponding USA Staffing Onboarding Account records to determine whether the removal of access was documented and performed.	No exceptions noted.
<b>oneARC</b>			
18.77	Access to oneARC is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, Login.gov or ID.me.	Observed a user access oneARC to note whether the user was required to use CAIA.	No exceptions noted.
18.78	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.	For a selection of new oneARC users, inspected the corresponding user access request forms to determine whether access was documented, employees acknowledged that they understood the Privacy Act requirements, access was approved, and access was configured as authorized.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
18.79	Changes to existing oneARC 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.	For a selection of changes to oneARC users, inspected the corresponding authorizing documentation to determine whether updates to access rights were authorized and access was configured as authorized.	No exceptions noted.
18.80	To remove a oneARC user's access there are 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.	For a selection of oneARC access removals, inspected the corresponding oneARC Terminations listing, access request forms and email requests, to determine whether termination of oneARC access was completed and access was removed.	No exceptions noted.
18.81	oneARC load sheets are prepared from provided lists from the accounting area. Customer agencies/Internal Management complete a review of all users (previously loaded ones, and new ones) every	For a selection of recertified users, inspected the corresponding oneARC user access reviews to determine if review of user access was performed and any users not on the list completed a System Access Form.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	quarter. If a user is not on this list, they must complete the System Access Form.		
18.82	oneARC authorization officials are not able to approve their own access (so each agency has a minimum of two authorization officials).	For a selection of new oneARC users, inspected the corresponding user access request forms to determine whether access was documented, approved, and access was configured as authorized.	No exceptions noted.
18.83	oneARC internal employees' access is tied to a permission set that allows them to work customer cases. To modify an internal user's access, 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.	For a selection of changes to oneARC users, inspected the corresponding authorizing documentation to determine whether updates to access rights were authorized and configured as authorized.	No exceptions noted.

**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.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
<b>Oracle, OBI and PRSIM</b>			
19.01	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, OCSS database administrators. After the approved request has been completed (i.e., the associated change is implemented in the production environment), the performer updates the request in My Oracle Support accordingly, and the request is then closed.	For a selection of changes processed in ESM/ServiceNow and My Oracle Support, inspected the corresponding ESM/ServiceNow tickets to determine whether the changes were tested and approved prior to being implemented in the production environment.	No exceptions noted.
19.02	For emergency changes to a production instance of Oracle, OBI, or PRISM, ARC requires verbal	For a selection of emergency changes processed in My Oracle Support for Oracle and PRISM,	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.	inspected the corresponding ESM/ServiceNow tickets to determine whether the emergency changes were approved by an ARC Oracle or PRISM application administrator in My Oracle Support the next business day.	
<b>webTA</b>			
19.03	When a new webTA release is received from UKG, ARC RTSB, HRSD, 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 then. approved. by the HRSD Director.	Inspected the latest version associated with webTA to determine whether any releases were implemented during the reporting period.	No WebTA releases were implemented during the reporting period. As a result, we were unable to conclude on the operating effectiveness of this control.
<b>GovTA</b>			
19.04	When a new GovTA release is received from UKG, ARC RTSB, HRSD, and HROD staff test the new release in a separate test instance by running test scripts and analyzing the results. The ability to apply GovTA releases is restricted to the database and GovTA application administrators under the authority of ISS. The new GovTA release is not applied to production until it has	Inspected the latest version associated with GovTA to determine whether any releases were implemented during the reporting period.	No GovTA releases were implemented during the reporting period. As a result, we were unable to conclude on the operating

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	been successfully tested and then approved by the HRSD Director.		effectiveness of this control.
<b>OneStream XF</b>			
19.05	When a new OneStream XF release is received, OneStream Support provides notification to ARC along with associated Release Notes outlining changes. 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.	For a selection of OneStream XF releases, inspected the corresponding change management records to determine whether releases were only released to production by application administrators after successful testing and appropriate approvals were obtained.	No exceptions noted.
19.06	ARC RTSB, PSS and ARAD staff test the new release in a separate test environment by running test scripts and analyzing the results. 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. Upon successful completion of testing, ARC RTSB perform a backup of Production prior to moving the approved migration file to Production. After the	For a selection of OneStream XF releases, inspected the corresponding change management records to determine whether releases were tested in a separate non-production environment using testing scripts and were only released to production by authorized application administrators after successful testing and appropriate approvals were obtained.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	approved request has been completed, all parties are notified and associated service ticket is closed.		
<b>RPA</b>			
19.07	<p>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.</p> <p>After the RPA developer completes the initial development of the change, testing is conducted in the Acceptance region of the RPA Management Console, a dedicated non-production environment. The developer then provides the RPA output materials for Process Owner review. If satisfactory, the code then proceeds to a final peer code review. Once the code reviewed, the Process Owner's test plan and go live approval is obtained.</p>	For a selection of new RPAs or changes to RPAs implemented into production, inspected the corresponding change documentation to determine whether the RPAs were tested in the Acceptance region and approved prior to production implementation.	No exceptions noted.
19.08	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	For a selection of new RPAs or changes to RPAs implemented into production that could have a security impact or create a new business process, inspected the corresponding change management	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	<p>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.</p> <p>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.</p>	<p>records to determine whether the RPAs were approved prior to production implementation.</p>	
<b>oneARC</b>			
19.09	<p>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.</p>	<p>For a selection of oneARC workflow changes, inspected the corresponding change documentation to determine whether the changes were tested in a non-production environment.</p>	<p>No exceptions noted.</p>
19.10	<p>A resource within the oneARC administration team uploads the packaged change to the</p>	<p>For a selection of oneARC workflow changes, inspected the corresponding change documentation to determine whether the changes</p>	<p>The following exception was noted:</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	production region. The Product Owner then approves the closure of the JIRA ticket.	were approved prior to being implemented to production.	Management was unable to provide evidence demonstrating that all 15 tickets selected for testing were approved prior to being implemented into production. Although approval records exist, they lacked timestamps or sequencing details necessary to confirm the approval dates.
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			

**Control Objective 20 – Data Center Physical Access and Environmental Controls**

Controls provide reasonable assurance that the data center hosting webTA/GovTA servers has implemented appropriate safeguards to protect systems and data from unauthorized access and physical damage, or operational disruption resulting from environmental hazards.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
20.01	The Fiscal Service Asset Protection Division (APD) issues employee badges, after performing security background checks and fingerprinting.	For a selection of new employees issued identification badges, inspected the corresponding investigation summaries to determine whether a background check was completed for each individual and each employee had their fingerprints on file.	No exceptions noted.
20.02	Terminated employees are required to surrender identification badges and are removed from the Physical Access Control System (PACS) immediately.	Inquired of management to determine whether PACS retained the date of removal to identify when users’ physical access privileges were removed from the system.	The following exception was noted:  The PACS access report only included individuals with current access and excluded disablement data for disabled/removed users. As a result, we were unable to conclude on the operating effectiveness of this control.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			
20.03	Physical access to the ISS data center is restricted to authorized users only.	Observed an individual attempt to access the Fiscal Services Building to note whether he/she displayed his/her identification badges while inside the facility.	No exceptions noted.
20.04	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.	<p>For a selection of employees granted one-day badges to the ISS data center, inspected the corresponding access request approvals from the individual's branch manager to determine whether the request was tracked in ESM/ServiceNow and approved.</p> <p>Inquired of management to determine whether PACS retained the date of provisioning to identify when users' physical access privileges were added to the system.</p>	<p>As it relates to the first procedure, no exceptions were noted.</p> <p>As it relates to the second procedure, the following exception was noted:</p> <p>The PACS access report only included individuals with current access and excluded disablement data for disabled/removed users. As a result, we were unable to conclude on the operating</p>

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
			effectiveness of this aspect of the control.
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			
20.05	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.	For a selection of months, inspected the corresponding access violation logs to determine whether the logs were reviewed by ISS, access violation logs were reviewed timely, and unauthorized access attempts made during the selected months were followed-up on, if necessary.	The following exception was noted: Management did not complete the October review of access violation logs until December 5, 2024, exceeding the one-month review window required by policy.
<p><u>Management's Response</u>  Management concurs with the exception and will initiate appropriate corrective actions.</p>			
20.06	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.	For a selection of days, inspected the corresponding ISS visitor log to determine whether 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.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
20.07	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.	For a selection of days, inspected the corresponding logs of issued one-day badges to determine whether one day badges were issued and returned following the completion of the work, and the logs annotating the badges were maintained and reviewed upon check out and check in.	No exceptions noted.
20.08	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.	Inspected the most recently completed annual review and recertification of individuals with access to the data center and access requests from ISS to determine whether the review/recertification was performed.  Inspected the listing of users with access to the data center to determine whether the identified users with unauthorized access identified during the review described in the test above were removed or authorization was granted.	No exceptions noted.
20.09	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	Observed the ThousandEyes tool to note whether the tool was implemented for use by ISS staff to monitor websites, FTP servers, and intrusion detection software every ten minutes, it automatically generated alerts, alerts were reviewed by ISS, and actions were taken as necessary.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	monitored by environmental monitoring software that provides continuous checking and alarming capabilities for temperature changes, water, and humidity threats.	Observed the Andover monitoring application to note whether the application was installed and used to monitor ISS data center environmental conditions and alert ARC staff in time for them to minimize resulting service interruptions.	
20.10	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.	<p>Observed the ISS data center to note whether sprinklers, hand-held fire extinguishers, and raised floors were present.</p> <p>Inspected completed maintenance work orders and inspection reports for the uninterruptible power supply (UPS) and the emergency power generator to determine whether the generator and UPS were maintained.</p> <p>Observed the Andover monitoring application to note whether redundant air conditioning (AC) units were available and in operation in the event of a main AC equipment failure.</p>	No exceptions noted.

**Control Objective 21 – Computer Operations**

Controls provide reasonable assurance that system problems and errors are recorded, analyzed, and resolved.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
21.01	When possible, TSD staff resolve ConcurGov issues. If TSD staff cannot resolve an issue, the issue is escalated to SAP Concur.	For a selection of issues escalated to Concur, inspected the corresponding escalated issue tickets to determine whether the issues were documented and resolved.	No exceptions noted.
21.02	If the administrator cannot resolve an issue, the issue is escalated to mLINQS, the vendor.	For a selection of moveLINQ incidents that the moveLINQ Administrator was unable to resolve, inspected the corresponding records requesting support to determine whether the issues were escalated to the mLINQ help desk for resolution.	No exceptions noted.
21.03	System owners will contact the appropriate technical or functional area to address the OneStream 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.	Observed the ThousandEyes tool to determine whether it was used to monitor OneStream and alerts were set-up to notify personnel of system issues.	No exceptions noted.
21.04	If the HR Systems Help Desk cannot resolve an HRConnect issue, the issue is escalated to the Treasury Tier 2 help desk. The HR Systems Help Desk notifies users of the outage or malfunction	Inspected the internal application setup and security documentation and any various manuals and documentation produced by HR to determine if HR support personnel have adequate access to materials.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	and notifies them again when the issue is resolved.	Inspected the HRConnect operations manuals to determine if the manuals are supplied to each employee assigned system maintenance responsibilities.	

**Control Objective 22 – Backups**

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
22.01	Differential backups of WebTA servers are created nightly and retained for a period of 90 days. Daily differential backups are replicated to Kansas City where they are kept for an additional 90 days.	Inspected the backup configuration for webTA to determine if it is configured to complete a nightly differential backup, retain the backup for 90 days, and send backups to an alternate processing site for an additional 90 days.	No exceptions noted.
22.02	Differential backups of GovTA servers are created nightly and retained for a period of 90 days. Daily differential backups are replicated to Kansas City where they are kept for an additional 90 days.	Inspected the backup configuration for GovTA to determine if it is configured to complete a nightly differential backup, retain the backup for 90 days, and send backups to an alternate processing site for an additional 90 days.	The following exception was noted: Management did not include 1 of 7 GovTA production servers in the nightly differential backup, contrary to backup policy.
<p><u>Management’s Response</u> Management concurs with the exception and will initiate appropriate corrective actions.</p>			

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

## Continuity of Operations

If the main building becomes inoperable, network operations will be transferred to the KROC facility in alignment with the ISS data center's Disaster Recovery Plan (DRP). This facility utilizes a "warm site" strategy to ensure operational recovery. Meanwhile, Fiscal Service workloads, including applications and services currently hosted in the data centers, will be migrated to cloud-based solutions with disaster recovery architectures tailored to each application's business continuity needs. Development and operations will be conducted remotely by ISS personnel, Fiscal Agents, Financial Agents, and contractor support teams.

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

FRB St. Louis conducts an annual disaster recovery exercise as part of its contingency planning. The test evaluates the failover of the IPP system from its hosting facility in EROC to Dallas, ensuring a successful transition. However, agencies are not required to redirect to a new IP address in Dallas for file submissions, as the process is manually intensive.

The Oracle system has a robust contingency plan overseen by ARC, ensuring that all essential functions continue smoothly with ARC employees' support. Disaster recovery testing is conducted annually in coordination with Fiscal Service's ISS and the Data Center's Disaster Recovery Plan (DRP). The primary Oracle database servers, housed at OCSS's main site on the east coast, are replicated in near real-time to a backup location in the western United States using Oracle Active Data Guard.

The moveLINQ system undergoes annual testing as part of the BCP. Microsoft conducts yearly contingency testing to ensure the platform's reliability. This annual BCP testing includes verifying Fiscal Service's access to the moveLINQ system within the MHS environment, as well as the availability of support tools hosted at Fiscal Service.

**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/>