Audit Report



OIG-27-015

FINANCIAL MANAGEMENT

Report on the Description of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Shared Services System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2025 to June 30, 2026

October 19, 2026

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

October 19, 2026

MEMORANDUM FOR ANNA M. MOURAD, ASSISTANT COMMISSIONER
CENTER FOR FINANCIAL MANAGEMENT
BUREAU OF THE FISCAL SERVICE

DAVID ATEN, INTERIM ADMINISTRATOR
TREASURY COMMON SERVICES CENTER
DEPARTMENT OF THE TREASURY

FROM: Shiela Michel /s/
Acting Director, Financial Statement Audits

SUBJECT: Report on the Description of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Shared Services System and the Suitability of the Design and Operating Effectiveness of its Controls for the Period July 1, 2025 to June 30, 2026

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 Center for Financial Management and Treasury Common Services Center's description of its shared services system (the "system") titled "Management of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Description of its Shared Services System" throughout the period July 1, 2025 to June 30, 2026, 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 Bureau of Fiscal Service Center for Financial Management (CFM) and Treasury Common Services Center's (TCSC) descriptions of its shared services system, management's written assertions, 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, 2025 to June 30, 2026;
- 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, 2025 to June 30, 2026, and subservice organizations and customer agencies applied the complementary controls assumed in the design of CFM and TCSC's controls throughout the period July 1, 2025 to June 30, 2026; and
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period July 1, 2025 to June 30, 2026 if complementary subservice organization controls and complementary customer agency controls, assumed in the design of CFM and TCSC's controls, operated effectively throughout the period July 1, 2025 to June 30, 2026.

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 CFM and TCSC's description of its 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 October 16, 2026, 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) 486-1415.

Attachment

Department of the Treasury

Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center Shared Services Financial Management, Procurement, and Human Resources Transactions and General Computer and Monitoring Controls

Report on the Description of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services 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, 2025 to June 30, 2026

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER SHARED SERVICES

REPORT ON THE DESCRIPTION OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER SHARED SERVICES SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS

FOR THE PERIOD JULY 1, 2025 TO JUNE 30, 2026

Table of Contents

Section	Description	Page
I.	**INDEPENDENT SERVICE AUDITORS' REPORT PROVIDED BY KPMG LLP**	**1**
II.	**MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER ASSERTION**	**5**
III.	**MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER DESCRIPTION OF ITS SHARED SERVICES SYSTEM**	**8**
	OVERVIEW OF OPERATIONS	9
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, AND MONITORING	26
	Control Environment	26
	Risk Assessment	26
	Monitoring	26
	Monitoring Subservice Organizations	27
	INFORMATION AND COMMUNICATION	28
	Information Systems	28
	Communication	31
	COMPLEMENTARY CUSTOMER AGENCY CONTROLS	32
	SUBSERVICE ORGANIZATIONS	35
	COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS	38
	CONTROL OBJECTIVES AND RELATED CONTROLS	43
IV.	**MANAGEMENT OF BUREAU OF FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT'S AND TREASURY COMMON SERVICES CENTER'S CONTROL OBJECTIVES AND RELATED CONTROLS, AND KPMG LLP's TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS**	**84**
	FINANCIAL MANAGEMENT PROCESSING CONTROLS	86
	Control Objective 1 – Obligations	86
	Control Objective 2 – Disbursements	89
	Control Objective 3 – Unfilled Customer Orders, Receivables, and Cash Receipts	96
	Control Objective 4 – Deposits	99
	Control Objective 5 – Payroll and Leave Accruals	101
	Control Objective 6 – Payroll Disbursements	102
	Control Objective 7 – USSGL	103

Control Objective 8 – Period-End Accruals 106
Control Objective 9 – Governmentwide Reporting 108
Control Objective 10 – Budget 112
Control Objective 11 – Manual Journal Entries 115
Control Objective 12 – Federal Investments 116
Control Objective 13 – Supplier and Bank Records Changes 118
PROCUREMENT PROCESSING CONTROLS 119
Control Objective 14 – Acquisitions and Contracts 119
Control Objective 15 – Sufficiently Funded Requisitions 120
HUMAN RESOURCES PROCESSING CONTROLS 121
Control Objective 16 – Personnel Actions 121
Control Objective 17 – Payroll Documents 124
GENERAL COMPUTER CONTROLS 127
Control Objective 18 – System Access 127
Control Objective 19 – Application Changes 146
V. OTHER INFORMATION PROVIDED BY THE MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER 150
Continuity of Operations 151

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

Assistant Commissioner, Center for Financial Management
Bureau of the Fiscal Service

Interim Administrator, Treasury Common Services Center
Department of the Treasury

Scope

We have examined management of Bureau of the Fiscal Service Center for Financial Management (CFM) and Treasury Common Services Center (TCSC)'s accompanying description of its Shared Service system (the System) for processing customer agencies' transactions throughout the period July 1, 2025 to June 30, 2026 titled "Management of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Description of its Shared Service 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 Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Assertion" (the Assertion). The controls and control objectives included in the Description are those that management of CFM and TCSC 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 Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center", is presented by management of CFM and TCSC to provide additional information and is not a part of the Description. Information about CFM and TCSC's continuity of operations 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.

CFM and TCSC use 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 CFM and TCSC and excludes the control objectives and related controls of the subservice organizations. The Description also indicates that certain control objectives specified by CFM and TCSC can be achieved only if complementary subservice organization controls assumed in the design of CFM and TCSC's controls are suitably designed and operating effectively, along with the related controls at CFM and TCSC. 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 CFM and TCSC's controls are suitably designed and operating effectively, along with related controls at CFM and TCSC. Our examination did not

KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

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 CFM and TCSC 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. CFM and TCSC are 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, 2025 to June 30, 2026. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

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

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

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of customer agencies and their auditors who audit and report on customer agencies' financial statements and may not, therefore, include every aspect of the System that each individual customer agency may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating

effectiveness of the controls to achieve the related control objectives stated in the Description, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

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

Opinion

In our opinion, in all material respects, based on the criteria described in the Assertion:

- the Description fairly presents the System that was designed and implemented throughout the period July 1, 2025 to June 30, 2026;
- 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, 2025 to June 30, 2026, and subservice organizations and customer agencies applied the complementary controls assumed in the design of CFM and TCSC's controls throughout the period July 1, 2025 to June 30, 2026; and
- the controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved throughout the period July 1, 2025 to June 30, 2026 if complementary subservice organization controls and complementary customer agency controls, assumed in the design of CFM and TCSC's controls, operated effectively throughout the period July 1, 2025 to June 30, 2026.

Restricted Use

The purpose of this report, including the description of tests of controls and results thereof in the description of tests of controls, is solely to provide information for management of CFM and TCSC, customer agencies of CFM and TCSC's System during some or all of the period July 1, 2025 to June 30, 2026, 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, to support evaluations of the effect of CFM and TCSC's controls on customer agencies' financial statements. Accordingly, this report is not suitable for any other purpose.

KPMG LLP

Washington, DC
October 16, 2026

II. MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER ASSERTION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

October 16, 2026

Management of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Assertion

We have prepared the accompanying description of Bureau of the Fiscal Service Center for Financial Management (CFM) and the Treasury Common Services Center (TCSC)'s Shared Service system (the System) for processing customer agencies' transactions throughout the period July 1, 2025 to June 30, 2026 titled "Management of Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center's Description of Its Shared Service System" (the Description) for customer agencies of the System during some or all of the period July 1, 2025 to June 30, 2026, 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.

CFM and TCSC use 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 CFM and TCSC 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 CFM and TCSC. The Description does not extend to controls of the subservice organizations.

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, 2025 to June 30, 2026 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 CFM and TCSC's System during the period covered by the Description.

iii. does not omit or distort information relevant to CFM and TCSC'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, 2025 to June 30, 2026 to achieve those control objectives if subservice organizations and customer agencies applied the complementary controls assumed in the design of CFM and TCSC's controls throughout the period July 1, 2025 to June 30, 2026. 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 CFM and TCSC;

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,

Anna M. Mourad

Anna Mourad
Assistant Commissioner, Center for Financial Management
Bureau of the Fiscal Service

David Aten
Interim Administrator, Treasury Common Services Center
Department of the Treasury

III. MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER DESCRIPTION OF ITS SHARED SERVICES SYSTEM

OVERVIEW OF OPERATIONS

The Center for Financial Management (CFM) (previously Administrative Resources Center) is a unit within the Bureau of the Fiscal Service (Fiscal Service). CFM offers financial management services to federal customers on a fully cost recoverable, fee-for-service basis.

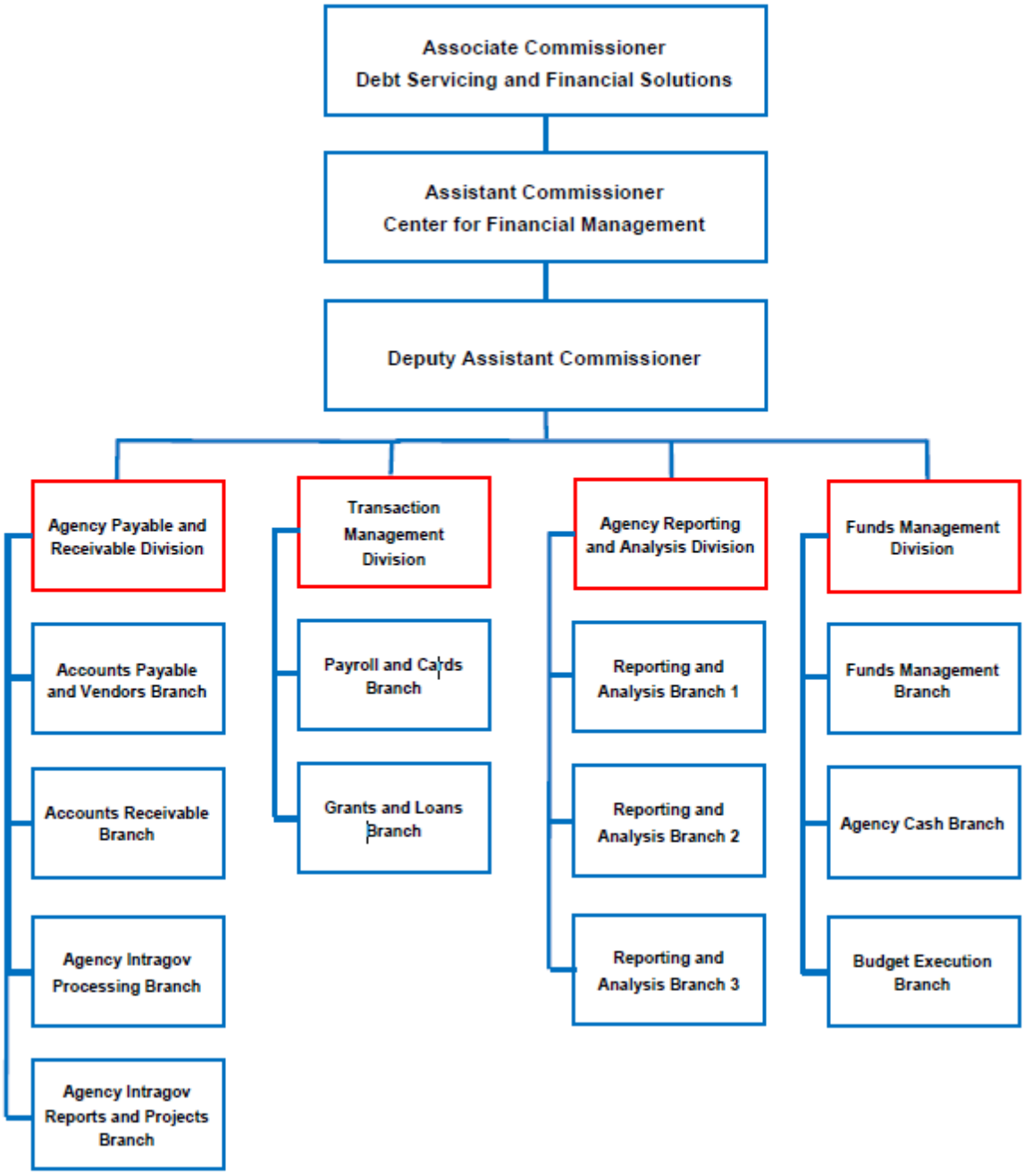
The Treasury Common Services Center (TCSC) is a shared service provider established in 2025 under the Assistant Secretary for Management (ASM) to deliver high-quality, cost-effective, and reliable common administrative services across the Treasury Department. These services include Human Resources, Technology, Acquisition, and Travel and are offered on a competitive, full-cost, fee-for-service basis.

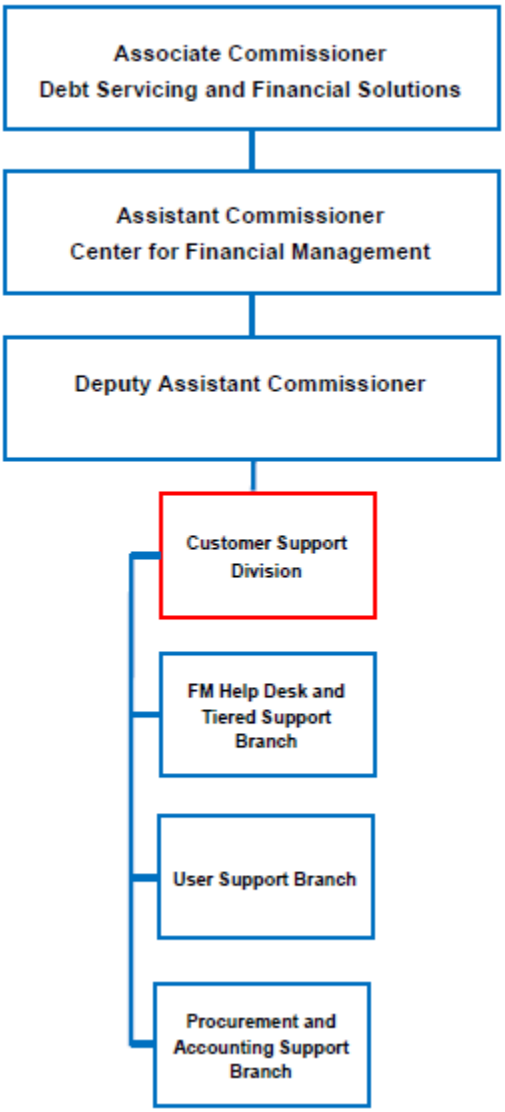
CFM and TCSC divisions and branches provide the following services for customer agencies:

Agency Payable and Receivable Division (APRD)	**Services Provided**
Accounts Payable and Vendors Branch (APVB)	Accounting Document Processing Reporting 1099 Reporting Supplier Table Update and Maintenance
Accounts Receivable Branch (ARB)	Accounting Document Processing Reporting Debt Collection Treasury Report on Receivables Reporting
Agency Intragov Processing Branch (AIPB)	Intragovernmental Business Document Processing
Agency Intragov Reports and Projects Branch (AIRPB)	Intragovernmental Business Reporting
Transaction Management Division (TMD)	**Services Provided**
Payroll and Cards Branch (PCB)	Accounting Record and Reconcile Payroll Purchase Card Processing
Grants and Loans Branch (GLB)	Accounting Document Processing Reporting Grant, Foreign Transaction, and Loan Activity
Agency Reporting and Analysis Division (ARAD)	**Services Provided**
Reporting and Analysis Branch 1 (RAB1)	Accounting Reporting, Analysis, and Audit Support
Reporting and Analysis Branch 2 (RAB2)	Accounting Reporting, Analysis, and Audit Support
Reporting and Analysis Branch 3 (RAB3)	Accounting Reporting, Analysis, and Audit Support

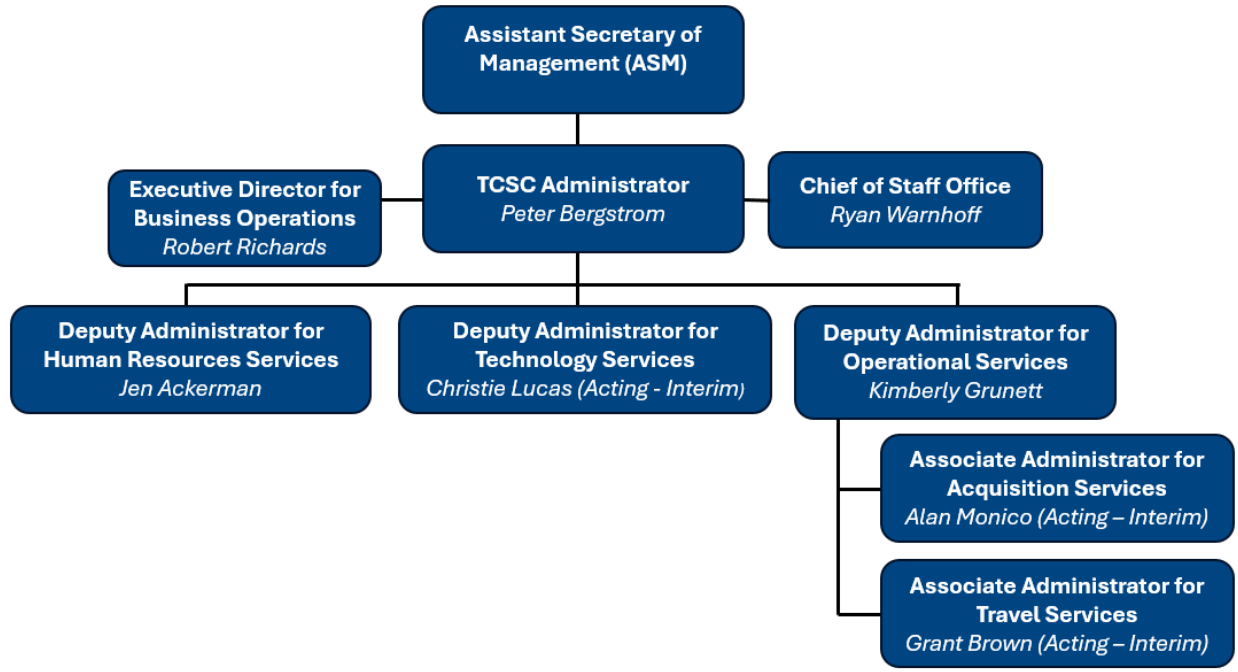
Funds Management Division	**Services Provided**
Funds Management Branch (FMB)	Document Processing Reporting Investment Activities
Agency Cash Branch (ACB)	Provides Cash Related Services Disbursements to Non-federal Entities Check Scanning Fund Balance with Treasury Reconciliation
Budget Execution Branch (BEB)	Accounting Reporting Budget
Customer Support Division (CSD)	**Services Provided**
FM Help Desk and Tiered Support Branch	Financial Management System Support
User Support Branch (USB)	Financial Management System Support and Training
Procurement and Accounting Support Branch (PASB)	Operate and Maintain Financial Management Systems
Division of Procurement Services (DPS)	**Services Provided**
Treasury Acquisitions Branch (TAB)	Procurement
Fiscal Service Acquisitions Branch (FSAB)	Procurement
Non-Treasury Acquisitions Branch (NTAB)	Procurement
Human Resources Operations Services Provided Division (HROD)	**Services Provided**
Employee Benefits Branch (EBB)	Processes and Monitor 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
Employment Services Division (ESD)	**Services Provided**
Classification and Support Branch (CSB)	Position Classification
Staff Acquisition Branch 1 (SAB1)	Staff Acquisition
Staff Acquisition Branch 2 (SAB2)	Staff Acquisition
Human Resources Systems Division	**Services Provided**
Help Desk and Reports Branch (HDRB)	HR Systems Support and HR Reports
Systems Support Branch (SSB)	HR Systems Support and Training
Travel Services Division (TSD)	**Services Provided**
Relocation Services Branch (RSB)	Relocation
Temporary Services Branch (TSB)	Temporary Duty
Systems and Projects Division (SPSD)	**Services Provided**
Project Support Staff Branch (PSSB)	Application Development, Analysis, and Project Management
Development Support Branch (DSB)	Application Development, Analysis, and Project Management
Reporting and Technology Support Branch (RTSB)	Operate and Maintain Financial Management Systems
Business Liaison Branch (BLB)	Internal Project Support

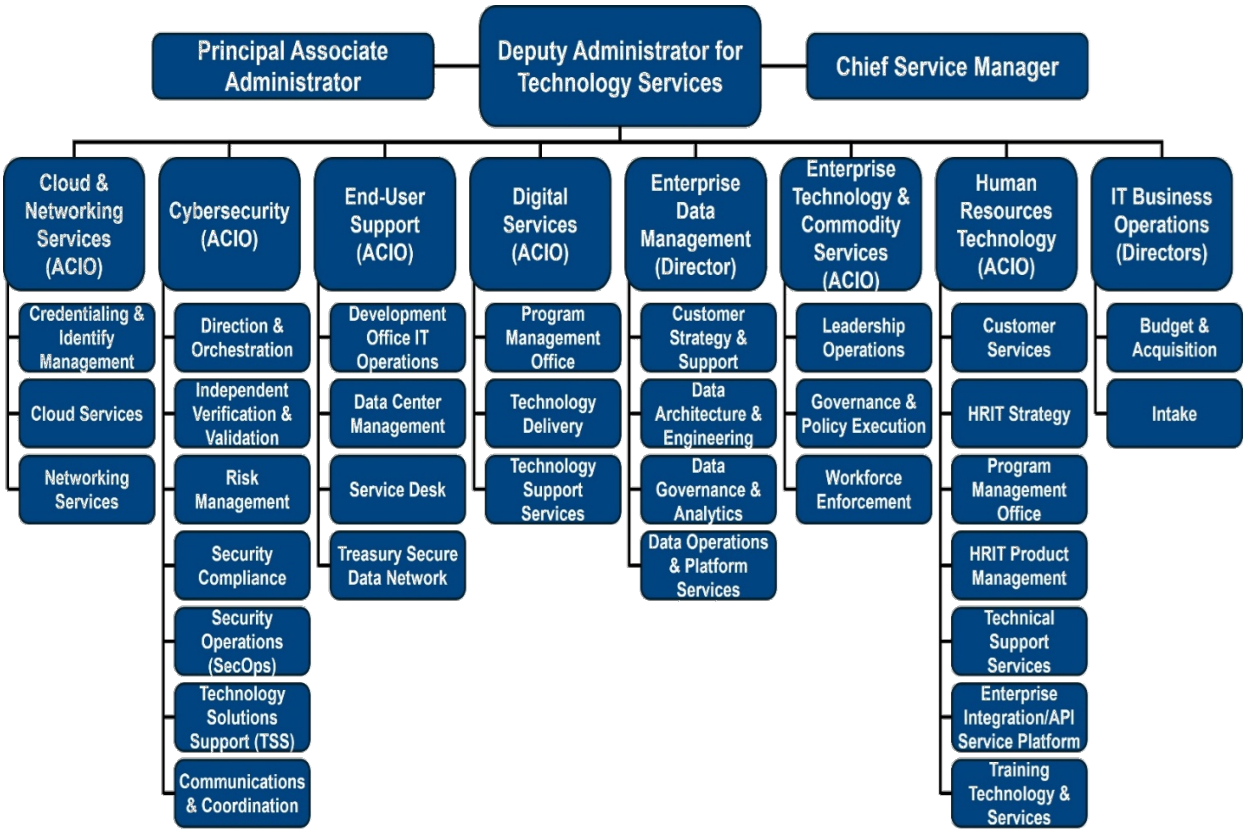
These CFM services are provided by the divisions as shown in the following organizational charts below:

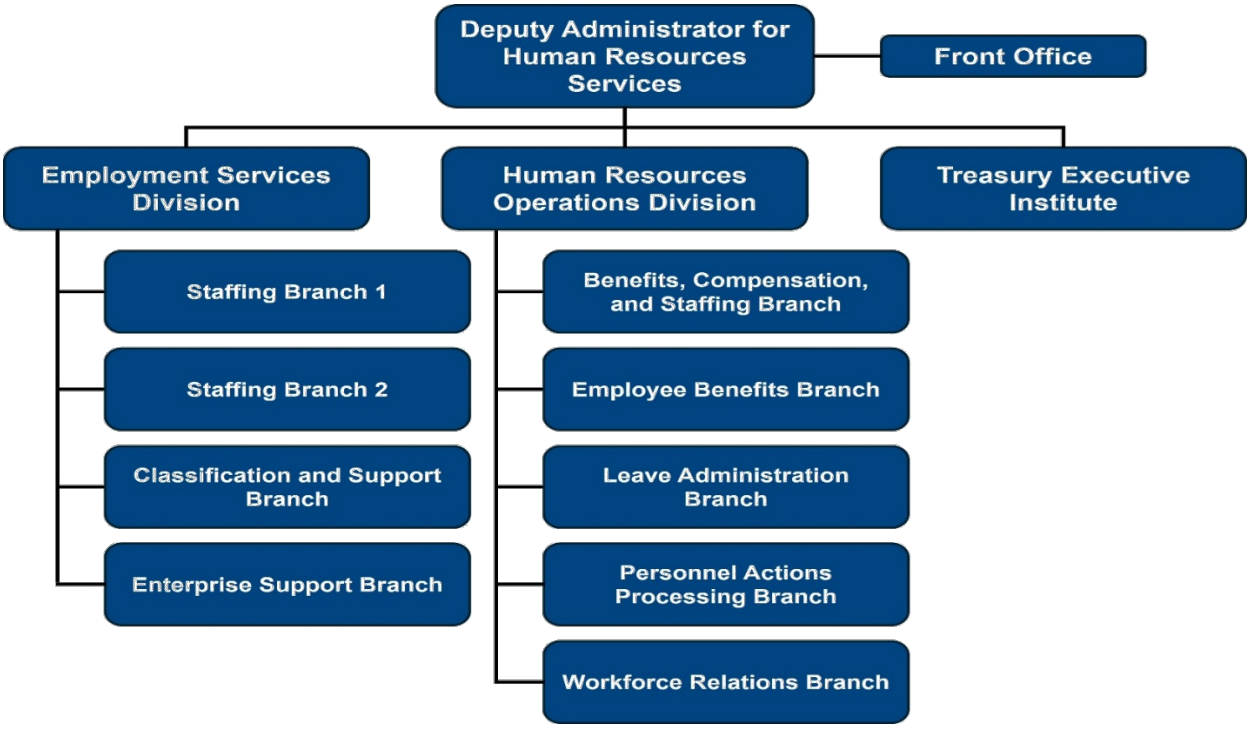


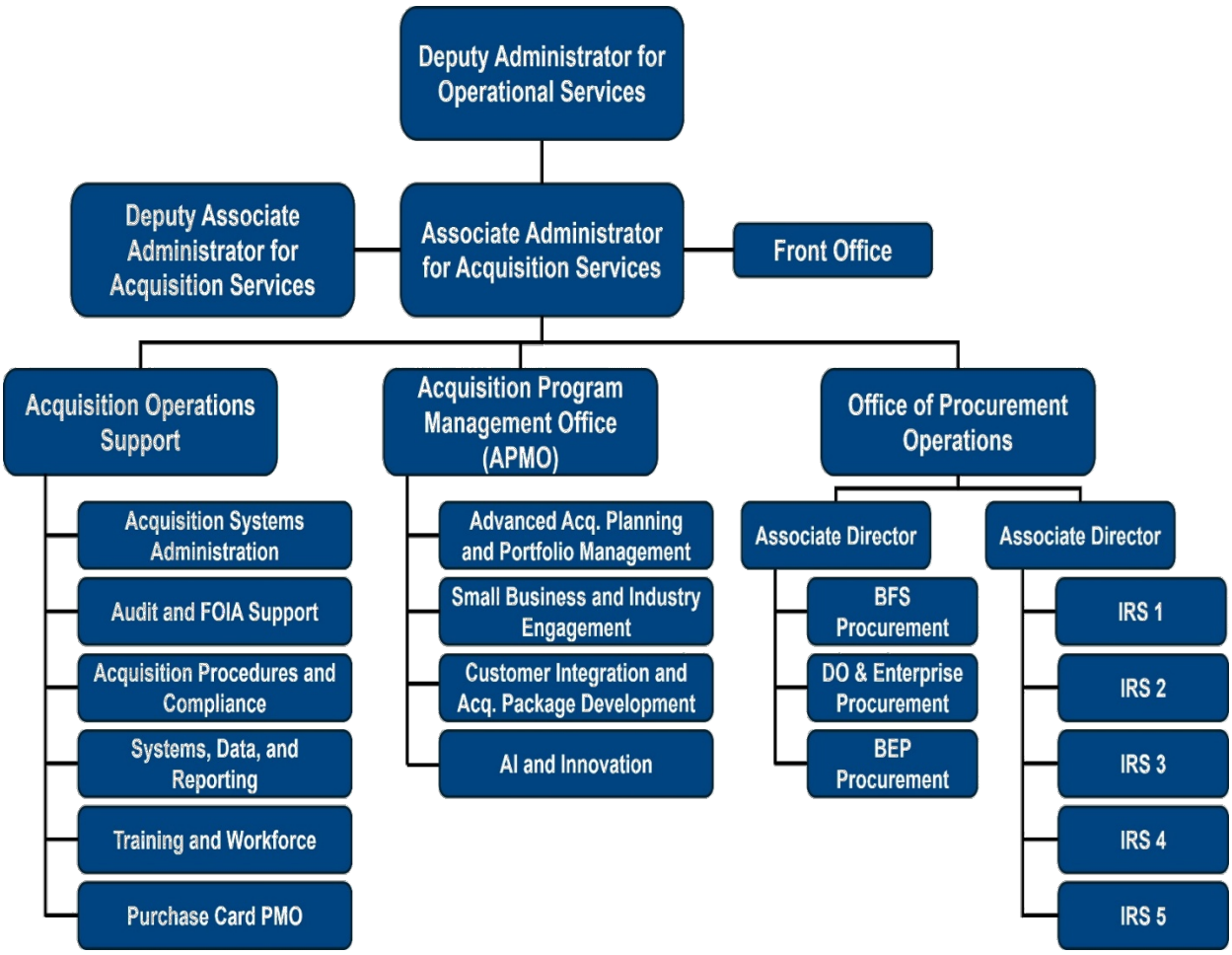

Associate Commissioner
Debt Servicing and Financial Solutions
Assistant Commissioner
Center for Financial Management
Deputy Assistant Commissioner
Customer Support Division
FM Help Desk and Tiered Support Branch
User Support Branch
Procurement and Accounting Support Branch

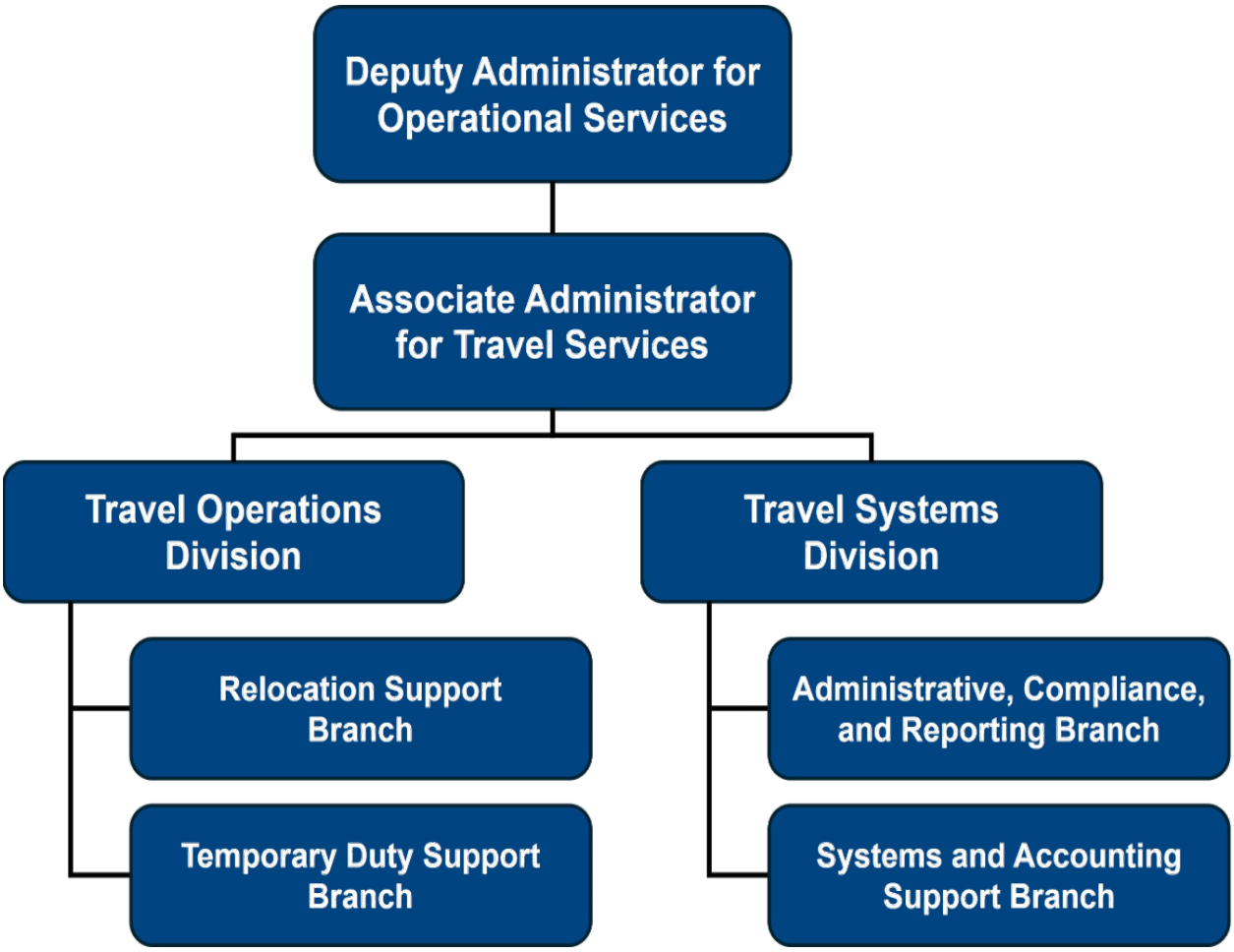
These TCSC services are provided by the divisions as shown in the following organizational charts below:






Deputy Administrator for Human Resources Services
Front Office
Employment Services Division
Human Resources Operations Division
Treasury Executive Institute
Staffing Branch 1
Staffing Branch 2
Classification and Support Branch
Enterprise Support Branch
Benefits, Compensation, and Staffing Branch
Employee Benefits Branch
Leave Administration Branch
Personnel Actions Processing Branch
Workforce Relations Branch


Deputy Administrator for Operational Services
Deputy Associate Administrator for Acquisition Services
Associate Administrator for Acquisition Services
Front Office
Acquisition Operations Support
Acquisition Program Management Office (APMO)
Office of Procurement Operations
Acquisition Systems Administration
Audit and FOIA Support
Acquisition Procedures and Compliance
Systems, Data, and Reporting
Training and Workforce
Purchase Card PMO
Advanced Acq. Planning and Portfolio Management
Small Business and Industry Engagement
Customer Integration and Acq. Package Development
AI and Innovation
Associate Director
Associate Director
BFS Procurement
DO & Enterprise Procurement
BEP Procurement
IRS 1
IRS 2
IRS 3
IRS 4
IRS 5


Deputy Administrator for Operational Services
Associate Administrator for Travel Services
Travel Operations Division
Travel Systems Division
Relocation Support Branch
Temporary Duty Support Branch
Administrative, Compliance, and Reporting Branch
Systems and Accounting Support Branch


Executive Director for Business Operations
Financial Management Division
Workforce Operations & Experience Division
Partner Management Division
Governance, Accountability & Operational Excellence Division
Communications Division

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, CFM has developed financial management service guidelines for customer agencies. The guidelines are available to customers via CFM'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 CFM processes.

Prior to providing accounting services, CFM meets with customer agencies to learn and understand the authorizing legislation and mission. This enables CFM 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.

CFM's Oracle system provides 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.

CFM offers commitment accounting to customer agencies to better enable them to monitor and control their funds availability. When applicable, CFM 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.

CFM 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.

CFM 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, CFM 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 CFM to be manually processed (non-IPP). CFM 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 CFM 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 CFM for processing in accordance with the Prompt Payment Act.

All invoices are examined by CFM 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 CFM 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, CFM 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.

CFM transmits EFT and check payment files to the Department of the Treasury (Treasury) for payment using Treasury's Secure Payment System (SPS). In addition, CFM processes most intragovernmental payments using Fiscal Services IPAC system. CFM obtains customer agency approval prior to initiating an IPAC payment to another federal agency. CFM 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. CFM records most IPAC payments in the accounting period the IPAC payment was made. If CFM is waiting for customer approval, IPAC payments will be posted in suspense prior to posting the obligation.

Third-party payroll services provide CFM with a file of payroll data at least bi-weekly (weekly if payroll adjustment files are applicable) to interface with Oracle. CFM reconciles all payroll transactions recorded to disbursements reported by the third-party processor. CFM 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.

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

CFM 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, CFM reconciles general ledger accounts to help ensure transactions are posted to the appropriate accounts.

CFM 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 CFM's accounting records.

Budget Services

CFM 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

CFM 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, CFM has created a standard suite of management and external reports that are available to all customer agencies. CFM 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

CFM and TCSC perform 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.

CFM and TCSC perform all system change activities in accordance with established procedures for evaluating, authorizing, and implementing system changes. To this end, CFM and TCSC maintain responsibility for System Integration Testing (SIT), providing customers an opportunity to perform User Acceptance Testing (UAT), and approving production changes.

Acquisition Services

TCSC provides acquisition and procurement support services, including acquisition planning, contract award, contract administration, and purchase card administration.

TCSC Acquisition Lifecycle

- **Identify the Requirement & Requisition Submission**
    - A customer agency defines the need, develops initial requirements, and submits a procurement request through Procurement Request Information System Management (PRISM).
    - The request includes required acquisition documents, such as Performance Work Statement (PWS), Statement of Work (SOW), Statement of Objective (SOO), Independent Government Cost Estimate (IGCE), verification of fundings, and applicable approvals.
- **Market Research**
    - TCSC acquisition professionals, Contract Specialist (CS)/and Contracting Officers (CO), perform market research to identify available commercial products or services, potential

sources, commercial practices, and industry capabilities.
    - Used to inform the acquisition strategy, acquisition plan, requirements document, and solicitation approach.
- **Acquisition Planning and Strategy**
    - The CS/CO review the requirement and develop an acquisition strategy.
    - The strategy determines the appropriate procurement method based on factors such requirement type, estimated value, complexity, and market conditions.
- **Solicitation and Evaluation**
    - The CS/CO prepares and posts the solicitation to the Governmentwide Point of Entry (GPE) via SAM.gov, as required by RFO Part 5.
    - Prospective contractors submit Quotations (RFO Part 13), Bids (RFO Part 14), or Proposals (RFO Part 15) in response to the solicitation.
    - The CO, with support from Technical Subject Matter Experts, evaluates Quotations, Bids, or Proposals solely on the factors, subfactors, and criteria specified in the solicitation.
- **Contract Award**
    - The CO awards the contract resulting from the solicitation to the responsible successful offeror whose Quotation, Bid, or Proposal represents the best value to the Government and satisfies the customer agency's requirements, in accordance with the RFO regulations and TCSC procedures.
- **Contract Administration**
    - Following contract award, the CS/CO performs contract administration activities throughout the contractual period of performance to ensure that the contractor's performance is in accordance with the terms and conditions of the contract.
    - Contract administration activities include executing authorized contract modifications, monitoring contract performance, resolving contractual issues, ensuring compliance, managing deliverables, and completing contract closeout.

Human Resources Services

The TCSC 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.

TCSC-HRIT serves as HR Systems support and is responsible for user access controls for HRConnect, GovTA, and NFC.

Travel Services

The TCSC Travel Services Division (TSD) provides relocation services and temporary duty services.

Relocation Services consist of the following:

- Operating and maintaining moveLINQ, a government relocation expense management system in compliance with the Federal Travel Regulations (FTR), 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 TCSC into moveLINQ. Prior to being submitted in moveLINQ, the vouchers are reviewed for accuracy by a second TCSC employee. Completed documents are submitted to the traveler and/or Approving Official for review and approval via the Portal, as appropriate. TCSC processes payments and the approved documents are interfaced and reconciled to Oracle, as needed, for customer agencies.

Authorizations, Amendments, and Advances:

- Relocation authorizations, amendments, and advances are entered by the TCSC Travel Relocation Coordinator into moveLINQ. Once the applicable document is stamped Sent to AO status, it is routed for signature to the employee/approving official via the Employee and Approval Portals. Once the employee (if required by the Agency) and approving official sign the document using a stamp, the Relocation Coordinator stamps the document approved. The document interfaces to the financial system the following business day.

Vouchers:

- Employees enter regular vouchers requests into the moveLINQ Employee Portal. TCSC Travel processes the voucher upon receipt and routes it for secondary review. The secondary reviewer verifies the voucher for accuracy before submitting it for employee and approving official signatures using the stamps in the Employee and Approval Portals. Once the voucher is stamped for signature by the employee and approving official, the voucher group stamps the voucher Approved. The following business day, the voucher interfaces to the financial system.
- Third-party vouchers are entered into moveLINQ and stamped Approved by TCSC Travel as the Transportation Officer. No signatures required. The following business day, the voucher interfaces to the financial system.
- RITA vouchers are entered into moveLINQ by TCSC Travel upon receiving the signed RITA Certification and supporting documentation. Once the voucher has been reviewed for accuracy and successfully processed, it is routed for secondary review. The secondary reviewer verifies the voucher for accuracy before submitting it for employee and approving official signatures using the stamps in the Employee and Approval Portals. Once the voucher is stamped for signature by the employee and approving official, the voucher group stamps the voucher Approved. The following business day, the voucher interfaces to the financial system.
- Invoice corrections are entered into moveLINQ by TCSC Travel upon receiving a request for reclass by form or by email. Once the document is entered, it is stamped approved by the voucher group. No signatures required on $0 voucher reclasses.

Financial System Interface & Payment Process:

- Upon interface to the financial system, the moveLINQ to Oracle Daily Comparison process is completed by the person processing the interface. This process confirms moveLINQ and Oracle match on all document types ensuring valid error-handling occurred and verifying the two systems remain in sync. Authorization and amendments that pass moveLINQ and Oracle validations are imported as approved/reserved and funds are encumbered. Advances and Vouchers that pass moveLINQ and Oracle validations import and are matched to the applicable authorization (purchase order). Once the voucher passes pre-payment validation, it is validated. Invoices over $2,500 are placed on hold by the system and require secondary review. Once the voucher is validated and secondary reviewed, if applicable, the validated invoice is processed into a payment batch by CFM the following business day and goes to Treasury. The document leaves Treasury the following day and is paid and Treasury confirms under the financial system.

Temporary Duty services consist of the following:

- Operating and maintaining the ETS systems (ConcurGov and GO.gov) 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/requests and vouchers/expense reports) and miscellaneous employee reimbursements are entered by TCSC and customer agency travelers into ConcurGov/GO.gov, 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/request and voucher/expense report is reconciled to Oracle daily. ConcurGov/GO.gov 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

CFM operations are led by the Assistant Commissioner of CFM, and TCSC operations are led by the Executive Director of TCSC. Both's mission is to deliver responsive, customer focused, cost-effective administrative support to customer agencies. CFM's and TCSC'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.

CFM and TCSC implement 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 CFM's and TCSC's operations, emphasized during the orientation program and reiterated in the personnel manual provided to all employees.

CFM and TCSC provide 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, CFM and TCSC help 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 CFM's and TCSC's strong internal control environment.

Risk Assessment

CFM and TCSC have each 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, CFM and TCSC management are 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

CFM and TCSC management consistently evaluate 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 CFM's ARAD, which reconciles Oracle subledger data to related general ledger accounts. Additionally, CFM performs monthly

reconciliations to ensure the accuracy of budgetary-to-proprietary account relationships. CFM 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, CFM and TCSC utilizes it's annual System and Organization Controls (SOC) 1 Report to identify and address opportunities to enhance controls.

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

Monitoring Subservice Organizations

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

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

INFORMATION AND COMMUNICATION

Information Systems

CFM oversees and performs application administration for a range of systems: Oracle, PRISM, OBI, oneARC, OneStream XF, and IPP. Several of these applications - PRISM, oneARC, OneStream XF, 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.

The Federal Reserve Bank of St. Louis manages IPP hosting. Microsoft Azure Government hosts OneStream XF. Salesforce hosts the oneARC system via its contracted Amazon Web Services (AWS) GovCloud+ platform.

TCSC oversees and performs application administration for: ConcurGov, GO.gov, moveLINQ, and GovTA, all of which serve as feeder systems into Oracle, which is hosted by OCSS.

ConcurGov is hosted by SAP Concur and IBM hosts GO.gov. MHS hosts moveLINQ on its contracted Microsoft Azure Government Cloud platform. TCSC is the designated system owner of 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 Fiscal Service. Tunnel connectivity is tightly controlled and restricted to approved customer-assigned network ranges by 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. CFM 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 Services 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 CFM 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. 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 host system a backup contingency site in the southwestern United States.

GovTA

Ultimate Kronos Group's (UKG) GovTA serves as the primary time and attendance systems for most customer agencies whose payroll is processed by the National Finance Center (NFC). Transactions that are entered in GovTA interface with NFC, and NFC ultimately sends payroll data back to CFM in order to be interfaced with Oracle. Prior to June 2026, GovTA used an Oracle database, which ran on the TCSC subnet and accessed data in the TCSC demilitarized zone (DMZ) using Red Hat Linux, an Apache web server, and a Tomcat application server. ISS served as the GovTA database administrator and provided primary support for tape backup and recovery. GovTA used 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) accessed the database on a specified port that was defined in the Access Control List. Only select IP addresses that were defined in the Access Control List were permitted to connect to the database IP. External security was provided by ISS through firewall rules and router access control lists. In June 2026, migrated to the Treasury CAELUM cloud platform in Amazon Web Services. The application and its PostgreSQL database operate within secure, private network environments and are not directly accessible from the public internet. Authorized users access GovTA through Treasury-approved security and network controls. Access between the web application and database is limited to approved application components and designated network ports. CAELUM provides centralized network protections, access controls, encryption, logging, monitoring, and other security safeguards, while automated database backups and recovery capabilities protect GovTA data.

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 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.

GO.gov

IBM's travel system GO.gov is the system selected by General Services Administration as the government's Software as a Service (SaaS)-based E-Gov Travel solution. GO.gov is a self-service travel system that incorporates traditional reservation and fulfillment support and a fully-automated booking process. GO.gov uses system processes and audits to help ensure compliance to the FTR and/or Agency policy. GO.gov is used to prepare, examine, route, approve, and record travel requests and expense reports. It is used to process all temporary duty travel (TDY) requests, expense reports, local expense reports, and miscellaneous employee reimbursements. Approved documents interface with Oracle for obligation or payment during a

real time interface process. GO.gov users consist of travelers, document preparers, budget reviewers, Approving Officials, Verifiers, and administrators.

IBM is responsible for system backup of GO.gov 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[1] software is a tool used to create robotic process automations (RPA) to automate repetitive tasks and manual processes. RPAs are developed and managed by Office of the CIO's Automation Platform Configuration & Management Branch (APCMB). 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. SailPoint is used to request and track access authorizations 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 APCMB 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

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

The Salesforce enterprise system is a Customer Relationship Management system that allows users to provide customized support to their customers and manage customer accounts, cases, and communications via phone, email, and messaging channels. Utilizing Salesforce's built-in communication tool, Chatter, communications become a permanent part of each case. Salesforce can also fully integrate with other back-office applications.

CFM has configured oneARC, a centralized customer-facing portal used by agency contacts to submit and manage Financial Management requests across Budget, Purchasing, Accounts Payable, Accounts Receivable, and Payroll Accounting, inside a Salesforce GovCloud+ instance. Instead of relying on group email inboxes, oneARC provides a controlled, workflow-driven mechanism which captures required request details, supporting documentation, communication, and approvals, all within the environment.

oneARC routes requests through predefined workflows to the appropriate CFM assignment group, ensuring a standardized process is followed and providing record reporting for audit tracking. This allows the full lifecycle of each request to be in one centralized location.

In addition to Financial Management requests, oneARC also offers a Service Desk application which allows for CFM lines of business to use oneARC Service Desk to log, route, resolve, and close customer tickets within the oneARC application.

Communication

CFM 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 CFM's employee training and career development programs, internal training sessions, and professional conferences.

TCSC uses a structured communication approach to ensure employees understand their roles, responsibilities, priorities, and internal control expectations. Communication is delivered through onboarding, role-specific training, staff meetings, leadership updates, and email updates on operational guidance and policy changes. Standards promote clear, consistent messaging through branding, tone, and plain language requirements, supported by clearance and approval processes to ensure accuracy.

Each employee receives a position description outlining responsibilities and the expectation to promptly elevate significant issues and risks. Managers reinforce communication through regular engagement and support professional development via TCSC training, Treasury resources, internal training, and conferences. TCSC also manages internal and external communication channels to support executive messaging and ensure information is consistent across the organization.

COMPLEMENTARY CUSTOMER AGENCY CONTROLS

CFM's and TCSC's controls related to its system supporting the delivery of CFM's and TCSC's system cover only a portion of the overall internal control for each CFM and/or TCSC customer agency. It is not feasible for the control objectives related to CFM's and TCSC's services to be achieved solely by CFM and/or TCSC. Therefore, each customer agency's internal control over financial reporting should be evaluated in conjunction with CFM's and TCSC'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:

- Properly approve and accurately enter obligations into the procurement and travel systems in the proper period.
- Send approved requests to record manual obligations to CFM in a timely manner.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to CFM.
- Compare actual expenditure results to budgeted amounts.
- Maintain and communicate to CFM a list of individuals authorized to request obligations when it is not communicated in the authorizing agreement.
- Approve and return relocation travel documents to RSB for processing in moveLINQ in a timely manner.
- Review the financial reports provided by CFM to help ensure that disbursement transactions are complete and accurate.
- Approve invoices for payment and send approved invoices to CFM 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.
- Maintain and communicate to CFM a list of individuals authorized to approve invoices.
- 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 CFM 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.
- Approve travel vouchers and accurately enter the vouchers/expense reports into ConcurGov or GO.gov in the proper period.
- Ensure relocation documents are authorized and completely and accurately processed in their agency financial system in a timely manner.
- Maintain and communicate to TCSC a list of individuals authorized to approve invoices and travel vouchers when it is not communicated in the authorizing agreement.
- Send approved and accurate documentation of unfilled customer orders, receivables, and cash receipts transactions to CFM in the proper period.
- Review unfilled customer orders, receivable and advance reports for completeness, accuracy, and validity.

- 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.
- Provide assistance, when requested, to determine a check's purpose and validity prior to deposit.
- Review the financial reports provided by CFM to help ensure that monthly payroll and leave accruals are complete and accurate.
- Review and confirm the leave accrual schedule annually.
- Verify that payroll processed by third-party providers is complete and accurate.
- Review the financial reports provided by CFM to help ensure that payroll disbursements are complete and accurate.
- Review and confirm CFM customer agency specific payroll disbursement procedures on an annual basis.
- Review and approve, prior to submission, the financial reports prepared by CFM 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.
- Review open accrual reports for completeness, accuracy, and validity.
- Approve and send revenue and expense accruals to CFM in a timely manner.
- Review the financial reports provided by CFM to help ensure that accruals are complete and accurate.
- Review and timely approve the annual submission of the TROR and Debt Collection Activities report.
- Provide timely certification of GTAS to CFM 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.
- Review the financial reports provided by CFM to help ensure that budget entries are complete and accurate.
- Submit approved budget plans to CFM in a timely manner.
- Communicate OMB apportionment status to CFM.
- 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.
- Send valid and approved requests to record manual JEs to CFM in a timely manner if they are initiated by the customer agency.
- Maintain and communicate to CFM a list of individuals authorized to submit manual JEs that are initiated by the customer agency.
- Provide CFM with 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 legislative revisions, that authorize the customer agency to invest with the investment account set-up.

- Work with CFM 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 CFM any known delays to receipt or disbursement activity that may impact investments.
- Communicate to CFM any larger than normal receipt or disbursement activity that may impact investments.
- Review active supplier reports provided by CFM and submit requests to remove suppliers no longer needed in a timely manner.
- Help ensure all personnel actions are submitted in HRConnect timely.
- Notify TCSC timely regarding separating employees.
- Review and approve listings of users with current Oracle, OBI, PRISM, IPP, OneStream and XF access to help ensure appropriateness and provide changes to CFM in a timely manner.
- Notify CFM timely regarding separating employees.
- Routinely review approvers within oneARC to confirm that only authorized users and responsibilities are executing actions and approvals.
- Review and approve listings of users with current GovTA, ConcurGov and HRConnect access to help ensure appropriateness and provide changes to TCSC in a timely manner.
- Notify TCSC timely of any changes to HRConnect, GovTA or USA Staffing authorized approvers.

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 Bureau of the Fiscal Service Center for Financial Management and Treasury Common Services Center Description of Its Shared Service System" section of this report.

SUBSERVICE ORGANIZATIONS

In order to provide financial management services, CFM and TCSC relies on systems and services provided by other organizations external to CFM and TCSC (subservice organizations). The achievement of control objectives depends on whether controls at the subservice organizations anticipated in the design of CFM's and TCSC'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. CFM performs reconciliations between the account summary and transaction reports.

Secure Payment System – CFM 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 CFM'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. CFM 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, CFM 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 CFM'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. CFM 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.

IBM

GO.gov – IBM developed and hosts the GO.gov system, which is an E-Gov travel system. IBM 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. CFM 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 TCSC 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 TCSC 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 CFM 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 TCSC provides the application administration. TCSC 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 CFM 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 – TCSC 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 TCSC.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

CFM and TCSC 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 CFM and/or TCSC. It is not feasible for the control objectives related to services provided by CFM and TCSC to be achieved solely by CFM and TCSC. Therefore, each customer agency's internal control over financial reporting must be evaluated in conjunction with CFM's and TCSC'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 CFM's and TCSC's control objectives that depend upon them are described for each of CFM's and TCSC'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 GovTA.
- Responsible for granting, reviewing, and removing user access to CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, 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 GovTA.
- Responsible for maintaining physical access and environment controls for CARS, SPS, CIR, TROR, CSNG, IPP, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and GovTA.
- Responsible for performing data back-ups for CARS, SPS, CIR, TROR, CSNG, IPAC, OTCnet, GTAS, InvestOne, FedInvest, and 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 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.
- Responsible for configuring and adjusting internal audit rules, overriding specific policy blocks, handling master data sync issues, troubleshooting Single Sign-On (SSO) login failures, profile synchronization issues, integration issues, and any other issues that surface for 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.
- Responsible for configuring and adjusting internal audit rules, overriding specific policy blocks, handling master data sync issues, troubleshooting Single Sign-On (SSO) login failures, profile synchronization issues, integration issues, and any other issues that surface.

IBM

Control Objective 1 – Obligations and Control Objective 2 – Disbursements

- Responsible for providing reasonable assurance that GO.gov 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 GO.gov.
- Responsible for providing reasonable assurance that administrative access to data, programs, and application functions are restricted to authorized users in GO.gov.
- Responsible for providing reasonable assurance that deployment and enhancements of GO.gov 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 GO.gov.
- Responsible for maintaining physical access and environment controls for GO.gov.
- Responsible for performing data back-ups for GO.gov.
- Responsible for configuring and adjusting internal audit rules, overriding specific policy blocks, handling master data sync issues, troubleshooting Single Sign-On (SSO) login failures, profile synchronization issues, integration issues, and any other issues that surface.

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.
- Responsible for ensuring the system does not allow an individual to add or remove responsibilities to their own ID.
- Responsible for identifying, correcting, or escalating system errors that arise within the components they operate.

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.
- Responsible for identifying, correcting, or escalating system errors that arise within the components they operate.

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.

- Responsible for configuring and adjusting internal audit rules, overriding specific policy blocks, handling master data sync issues, troubleshooting Single Sign-On (SSO) login failures, profile synchronization issues, integration issues, and any other issues that surface for moveLINQ.

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.

CONTROL OBJECTIVES AND RELATED CONTROLS

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 policies and procedures.

CFM Description of Controls

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

PRISM System Interface

An obligation is created when a customer agency enters 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.

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 reconciled 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 CFM a signed copy of the agreement or Miscellaneous Obligation Form to obligate funds. Upon receipt from the customer agency and/or Procurement, the CFM 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 CFM 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 CFM and customer agencies through ad hoc OBI reports.

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 legal level with the set-up of the

fund in Oracle and reviewed after passage of appropriation legislation and a high-level budget is loaded into Oracle. Upon receipt and input of a detailed financial plan, additional controls, below the legal level, can be established at the allocation level when desired by the customer agency.

Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. 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 processing of obligation documents. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM user attempts to enter a transaction identification number that already exists, Oracle issues an error message that alerts the user of the duplication.

TCSC Description of Controls

Temporary Duty Travel System Interface

ConcurGov

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

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

Accepted files are loaded into Oracle as obligations in the general ledger. An OBI report is generated and reviewed to identify and correct data interface errors and exceptions between ConcurGov and Oracle. Transactions with errors are reviewed and manually entered into the financial system. Approved authorizations in ConcurGov are reconciled daily by TCSC with an OBI report to help ensure that all ConcurGov authorizations have been interfaced and processed into Oracle. If discrepancies arise, they are investigated and corrective actions are taken as needed.

GO.gov

TCSC and customer agency travelers enter travel requests into GO.gov and electronically route them to Approving Officials for review and approval. GO.gov is a cloud based infrastructure self-service travel system that utilizes a fully-automated booking process. GO.gov uses system processes and audits to help ensure compliance to the FTR. GO.gov is used to prepare, examine, route, approve and record travel

requests and expense reports. Approving Officials electronically stamp the request with a status of "approved." GO.gov prevents a user from self-approving travel requests.

IBM's Interconnection Exchange Agreement (IEA) sends approved travel request data into Oracle and Oracle records the obligation, provided the accounting string for the obligation transaction is valid and funds are available.

Accepted files are loaded into Oracle as obligations in the general ledger. An OBI report is generated and reviewed to identify and correct data interface errors and exceptions between GO.gov and Oracle. Transactions with errors are reviewed and manually entered into the financial system. Approved requests in GO.gov are reconciled daily by TCSC with an OBI report to help ensure that all GO.gov requests have been interfaced and processed into Oracle. If discrepancies arise, they are investigated and corrective actions are taken as needed.

Relocation Services Authorization Approvals

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.

Relocation Travel System Interface

The following business day, approved documents (authorizations, amendments, or vouchers) import to the financial system where a Junior Analyst performs a daily reconciliation between moveLINQ and Oracle to confirm the two systems remain in sync. If discrepancies arise, they are investigated and corrective actions are taken as needed.

Complementary Customer Agency Controls

CFM 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 CFM in a timely manner.
- Review open obligation reports for completeness, accuracy, validity, and resolve any discrepancies noted in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to CFM.
- Compare actual expenditure results to budgeted amounts.
- Maintain and communicate to CFM a list of individuals authorized to request obligations when it is not communicated in the authorizing agreement.

TCSC 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.

Control Objective 2 – Disbursements

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

CFM Description of Controls

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

IPP Customer Agency Invoice Approvals

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

To submit an invoice directly into IPP, the vendor must have an IPP collector account. CFM transmits Oracle supplier table information to the Federal Reserve Bank (FRB) of St. Louis 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. 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 CFM 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 CFM or directly to the customer agency. When received by CFM, the customer agency provides approval via the oneARC application, or CFM forwards the invoice to an authorized agency contact for approval before CFM 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 established 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 a CFM 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, CFM may obtain customer agency approval after the IPAC has been recorded.

IPP Review

Invoices processed by IPP undergo random sampling as part of a post-payment audit. CFM reviews 10% of all invoices processed by IPP for each customer agency monthly. 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 for less than $2,500 are subject to a monthly random sample post payment audit which is performed by an accountant and approved by a Lead Accountant. 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.

Payment Date Calculations

Based on the customer agency's contracts with its suppliers, CFM 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 CFM staff or interfaces from the IPP invoice. Daily, Oracle selects invoices that are due for payment and creates files for manual uploading into SPS. CFM's Data Entry Operator (DEO) submits bulk files created in Oracle via drop zones to the Bureau of the Fiscal Service's National Payment Center of Excellence. The DEO creates a summary schedule in Oracle that is imported into SPS. A CFM SPS certifying officer compares the number and dollar amount of payments certified in SPS to the payment files generated by Oracle to help ensure that 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 of 30 days after the later of the invoice receipt date and the earlier 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 that 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

CFM accountants perform reconciliations of SmartPay account statement balances to Accounts Payable transaction details in Oracle which are reviewed by CFM staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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 CFM 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.

CFM accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by CFM Staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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.

Budget Execution System Controls

Customer agencies can create and monitor both legally established and internally developed budget plans in Oracle to help ensure that 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 legal level with the set-up of the fund in Oracle and reviewed after passage of appropriation legislation and a high-level budget is loaded into Oracle. Upon receipt and input

of a detailed financial plan, additional controls, below the legal level, can be established at the allocation level when desired by the customer agency.

Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. If discrepancies arise, they are investigated and corrective actions are taken as needed.

Intragovernmental Transactions

CFM adheres to applicable intragovernmental elimination guidance in the Treasury Financial Manual (TFM). This involves recording transactions at a level that allows for identification of CFM'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 CFM's Treasury customer agencies, CFM 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, CFM 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 a CFM 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. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM user attempts to enter a transaction identification number that already exists, Oracle issues an error message that alerts the user of the duplication.

TCSC Description of Controls

Temporary Duty Travel Vouchers Approvals

ConcurGov

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

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

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

GO.gov

TCSC and customer agency travelers enter travel expense reports into GO.gov and electronically route them to Approving Officials for review and approval. GO.gov is a cloud based infrastructure self-service travel system that utilizes a fully-automated booking process. GO.gov uses system processes and audits to help ensure compliance to the FTR. GO.gov is used to prepare, examine, route, approve and record travel requests and expense reports. Approving Officials electronically stamp the expense report with a status of "approved." GO.gov prevents a user from self-approving travel expense reports.

IBM's Interconnection Exchange Agreement sends approved travel expense report data into Oracle and Oracle records the disbursement provided the accounting string for the disbursement transaction is valid and funds are available.

Accepted files are loaded into Oracle as disbursements in the general ledger. An OBI Status Report is generated and reviewed to identify and correct data interface errors and exceptions between GO.gov and Oracle. Transactions with errors are reviewed and manually entered into the financial system. Approved vouchers in GO.gov are reconciled daily by TCSC using an OBI report to help ensure that all GO.gov vouchers have been interfaced and processed into Oracle.

Relocation Services Travel Vouchers Approvals

RSB personnel enter and audit each PCS travel voucher in moveLINQ. Once the voucher is entered and audited, it is electronically routed to the Employee/Approving Official for review and approval with the exception of third-party vouchers. This includes employee advances, and employee relocation travel reimbursements. TCSC Relocation Services approves all third-party vouchers, as the Transportation Officer.

All third-party invoices are examined by TCSC 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 employee voucher with their assigned status. When the signed document is received by RSB, Relocation Junior Analysts 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.

Relocation Travel System Interface

The following business day, approved documents (authorizations, amendments, or vouchers) import to the financial system where a Junior Analyst performs a daily reconciliation between moveLINQ and Oracle to confirm the two systems remain in sync. If discrepancies arise, they are investigated and corrective actions are taken as needed.

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/TCSC category type are subject to a 41-point audit worksheet comprised of 36 critical error checks and 5-noncritical informational checks. The TCSC 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.

Complementary Customer Agency Controls

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

- Review the financial reports provided by CFM to help ensure that disbursement transactions are complete and accurate.
- Approve invoices for payment and send approved invoices to CFM 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.
- Maintain and communicate to CFM a list of individuals authorized to approve invoices.
- Review and communicate customer agency required levels of budget and expenditure controls to CFM.
- 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 CFM 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.

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

- Approve travel vouchers and accurately enter the vouchers/expense reports into ConcurGov or GO.gov 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 TCSC a list of individuals authorized to approve invoices and travel vouchers when it is not communicated in the authorizing agreement.

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 CFM policies and procedures.

CFM Description of Controls

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

Customer Agency Approval

CFM only processes unfilled customer orders, receivables, and cash receipts with customer agency approval. No approval is required for checks received for deposit directly by CFM 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. CFM 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, CFM 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, CFM 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.

CFM accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by CFM staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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

CFM 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. A CFM supervisory accountant reviews the report. If discrepancies arise, they are investigated and corrective actions are taken as needed. As applicable, CFM monitors and pursues collection of delinquent balances.

Intragovernmental Transactions

CFM 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, CFM 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, CFM 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 a CFM 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. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM 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

CFM 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 CFM 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 CFM policies and procedures.

CFM Description of Controls

CFM has documented procedures for 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 a CFM designated accounting technician if delivery confirmation was requested. The CFM designated accounting technician (who does not have Oracle access to post accounts receivable transactions) receives, opens, and logs all checks received in CFM'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.

The checks are locked in a secure location (safe) until they are ready to be deposited. 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 FRB Cleveland by the CFM accounting technician. Upon settlement with the FRB, the CFM 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 CFM accounting technician destroys the checks. The cash receipt is recorded in Oracle by a CFM staff member other than the individual processing the deposit in OTCnet.

On the "deposit reporting and processing" side of OTCnet, a CFM 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 CFM 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, a CFM 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

CFM 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 CFM policies and procedures.

CFM Description of Controls

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

System Calculation of Accruals

Monthly payroll accruals are recorded and reviewed monthly 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 calculations, 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. If discrepancies arise, they are investigated and corrective actions are taken as needed. 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

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

- Review the financial reports provided by CFM 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 CFM policies and procedures.

CFM Description of Controls

CFM 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 CFM after each pay period. Payroll files are imported into Oracle. After import, the CFM 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 CFM 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 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 CFM 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

CFM 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 CFM to help ensure that payroll disbursements are complete and accurate.
- Review and confirm CFM 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.

CFM Description of Controls

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

Transaction Set-up Controls

CFM records proprietary and budgetary accounting entries using the USSGL at the transaction level. This is accomplished using a combination of selecting 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.

CFM 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.

CFM 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 CFM customer agencies. Once the changes to the USSGL are approved by Treasury and the new TFM guidance is issued (generally mid-summer), the CFM USSGL Team will communicate the appropriate changes to CFM Oracle system administrators to 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. CFM accountants prepare budgetary to proprietary account relationship reconciliations monthly 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

The CFM team maintains the integrity and accuracy of GTAS file submissions for non-Treasury customers (excluding DHS) by implementing a series of robust controls. Accountants generate GTAS bulk files within Oracle, where automated edit checks based on USSGL attributes ensure only valid files are created—any files failing these checks are not produced, preventing erroneous data from entering the submission process. Once a file passes Oracle's edit checks, CFM manually uploads it into the GTAS system. Following the upload, a designated reviewer, such as a supervisory accountant, independently examines the GTAS submission and system feedback for any Treasury Appropriation Fund Symbol (TAFS) failures. The reviewer verifies that all failed TAFS have been thoroughly investigated and resolved, and documents evidence of both the review and the resolution, ensuring a transparent and accountable process.

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 a CFM accountant is validated based on system-defined validation checks.

CFM 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, CFM accountants review the edit reports and resolve any invalid attributes or out-of-balance conditions. CFM accountants document this review by completing the TIER Submission Checklist, which is further reviewed by a supervisor.

Financial Statement Crosswalks

CFM 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, CFM accountants prepare the *Statement of Budgetary Resources (SBR*) and *Statement of Custodial Activity (SCA)* (when applicable) for all customer agencies. CFM accountants compare TFM financial statement crosswalks to CFM's internally prepared financial statements or OneStream XF tables to determine compliance with the TFM reporting requirements. CFM accountants investigate and resolve any differences between TFM crosswalks and CFM's internally prepared financial statements.

Complementary Customer Agency Controls

CFM 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 CFM 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 CFM policies and procedures.

CFM Description of Controls

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

Revenue and Expense Accruals

CFM 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, CFM 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, a CFM 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 by the Department of Labor. Customer agencies provide data for year-end payroll accruals. For the manual year-end accruals, a supervisor reviews and posts the accrual.

General Ledger to Subledger Reconciliation

On a monthly basis, CFM 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 legal level with the set-up of the fund in Oracle and reviewed after passage of appropriation legislation and a high-level budget is loaded into Oracle. Upon receipt and input of a detailed financial plan, additional controls, below the legal level, can be established at the allocation level when desired by the customer agency.

Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. The system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. 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. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM 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

CFM 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 CFM in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to CFM.
- Review the financial reports provided by CFM 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 CFM policies and procedures.

CFM Description of Controls

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

GTAS

GTAS is a web-based system for use in 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 a CFM 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, CFM 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 internal and Treasury department-defined data quality standards.

Prompt Payment

CFM 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.

Financial Statement Crosswalks

CFM 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, CFM accountants prepare the *SBR and SCA* (when applicable) for all customer agencies. CFM accountants compare TFM financial statement crosswalks to CFM's internally prepared financial statements or OneStream XF table to help ensure compliance with the reporting requirements. CFM investigates and resolves any differences between TFM crosswalks and CFM'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 quarters consolidated financial statements are submitted to the Director of OMB and Congress by the Department. The *SBR and SCA* are only submitted to the Director of the OMB and Congress for the fourth quarter. CFM accountants compare the quarterly financial statements to CFM's internally prepared financial statements and resolve any differences. The comparison is reviewed by a supervisor.

If applicable for non-Treasury customer agencies, CFM 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. 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 2026, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by a CFM supervisory accountant and approved by the bureau CFO or designee prior to submission to Treasury.

For non-Treasury and non-DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2026, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by a CFM supervisory accountant prior to submission to OMB.

Receivables

CFM accountants prepare and submit a quarterly TROR and Debt Collection Activities report for all customer agencies. These reports are reviewed by a CFM supervisory accountant prior to submission to Treasury. If discrepancies arise, they are investigated and corrective actions are taken as needed.

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, CFM utilizes Oracle to generate an Award Financial File for Treasury and Homeland Security customer agencies. CFM submits the Award Financial File into TIER for Treasury customer agencies and requests the Treasury customer agency to validate the data. CFM sends an Award Financial File to Homeland Security customer agencies.

For non-Treasury and non-Homeland Security customer agencies, DATA Act reporting is performed monthly. For those customer agencies, three files are submitted to the governmentwide DATA Act Broker system (Broker) monthly. The Broker has validation checks with the GTAS submissions. The accountants review the reports produced by 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's monthly attestation statement, CFM 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. CFM updates the status of the three monthly DATA Act File submissions to "Certified" on behalf of the customer agency.

Complementary Customer Agency Controls

CFM 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 CFM 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 CFM policies and procedures.

CFM Description of Controls

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

Budget Documentation

CFM ensures that appropriations and apportionments for customer agencies are entered and allocated in strict accordance with established regulatory requirements and documented guidance. For appropriations subject to annual enactment, CFM verifies the approved amount against the annual appropriations process, continuing resolution calculations, enacted legislation, or Treasury documentation before entry, and carefully documents and retains evidence of this verification. Apportionments are entered in Oracle only after confirming the accuracy of the customer agency's SF 132, Apportionment and Reapportionment Schedule, with records maintained for each review and entry. Upon receiving the customer agency's budget plan or reprogramming guidance, CFM allocates funding to the agency's accounting values, ensuring that allocations are consistent with the provided details. All allocations are thoroughly documented and subject to supervisory review, supporting transparency and compliance throughout the process.

For sources of funds not subject to annual appropriations (e.g., reimbursable or revolving accounts), CFM enters appropriations and apportionments based on the customer agency's SF 132 and recorded reimbursable activity. CFM reviews and documents the supporting activity prior to allocation and retains evidence of compliance.

For funds not subject to both annual appropriations and apportionment, CFM enters appropriations and apportionments at the fund level, allocating funding based on the customer agency's budget plan, recorded reimbursable activity, or reprogramming guidance. All entries and allocations are documented and reviewed for accuracy and compliance.

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 legal level with the set-up of the fund in Oracle and reviewed after passage of appropriation legislation and a high-level budget is loaded into Oracle. Upon receipt and input of a detailed financial plan, additional controls, below the legal level, can be established at the allocation level when desired by the customer agency.

Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. If discrepancies arise, they are investigated and corrective actions are taken as needed.

Reconciliation – Budgetary and Proprietary Account Relationships

CFM accountants prepare budgetary to proprietary account relationship reconciliations monthly, 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 CFM 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.

CFM accountants perform monthly reconciliations of CARS Account Statement balances to general ledger FBWT balances which are reviewed by CFM staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM 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

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

- Review the financial reports provided by CFM to help ensure that budget entries are complete and accurate.
- Submit approved budget plans to CFM in a timely manner.
- Review and communicate customer agency required levels of budget and expenditure controls to CFM.
- Communicate OMB apportionment status to CFM.
- 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 CFM policies and procedures.

CFM Description of Controls

CFM 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. In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM. When a CFM 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

CFM 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 CFM in a timely manner if they are initiated by the customer agency.
- Maintain and communicate to CFM 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.

CFM Description of Controls

CFM accountants use FedInvest, a web-based extension of InvestOne, 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

CFM 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 CFM accountant then enters the request into FedInvest and generates a buy request confirmation report for the entered transaction. Buy requests are prepared by a CFM accountant and a daily work package is then created with all the supporting documents and then two additional CFM accountants review the entered information for accuracy. Each CFM 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.

CFM accountants perform 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.

CFM accountants perform 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 CFM 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

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

- Provide CFM with 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 legislative revisions, that authorize the customer agency to invest with the investment account set-up.
- Work with CFM 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 CFM any known delays to receipt or disbursement activity that may impact investments.
- Communicate to CFM 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 CFM policies and procedures.

CFM Description of Controls

CFM has documented procedures related to supplier and bank record changes for staff to follow.

Segregation of Duties – 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 CFM staff other than the individual performing the task.

Review – Changes to Supplier and Bank Records

Daily, 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

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

- Review active supplier reports provided by CFM 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 contract awards are executed by a warranted Contracting Officer who certifies that the award is complete, accurate, and documented in accordance with TCSC policies and procedures.

TCSC Description of Controls

The acquisition dollar threshold and procurement method determine the documentation required to be maintained in the contract file. For simplified acquisitions exceeding the micro-purchase threshold, the acquisition file shall include a Vendor Matrix and an Award Summary. Alternatively, all required information from these documents may be consolidated into a single Award Recommendation. For acquisitions exceeding the simplified acquisition threshold, the acquisition file shall also include the Procurement Checklist. The Contracting Officer reviews the contract file to ensure it is complete, accurate, and compliant with the Federal Acquisition Regulation (FAR) and applicable TCSC requirements. To ensure compliance, identified discrepancies are investigated, and appropriate corrective actions are taken. Only a warranted Contracting Officer has the authority to sign a contract award that obligates the Government. The Contracting Officer's signature certifies that the contract is complete, accurate, and supported by the required acquisition documentation and that the award complies with applicable legal and regulatory requirements.

Control Objective 15 – Sufficiently Funded Requisitions

Controls provide reasonable assurance that award requisitions are approved by a warranted Contracting Officer acting within their delegated warrant authority and supported by sufficient funding.

TCSC Description of Controls

TCSC management has configured the automated contract writing system, PRISM, to enforce a Contracting Officer warrant authority by restricting award approvals to each Contracting Officer's authorized dollar threshold, thereby preventing awards that exceed delegated warrant authority. To avoid deficiencies, PRISM also includes controls that prevent contract awards from being executed without sufficient funding. To support compliance with the Digital Accountability and Transparency Act (DATA Act), PRISM incorporates system controls that help ensure applicable contract awards are accurately reported to the Federal Procurement Data System–Next Generation (FPDS-NG) and subsequently reported in USAspending.gov.

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.

TCSC Description of Controls

TCSC 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.

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, resolves 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

TCSC 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 TCSC HR. Depending on the type of personnel action, TCSC 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, 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.

Employee-submitted personnel actions (such as name changes) bypass the customer agency review process and route directly to TCSC 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 TCSC HR. However, there are some customer agencies that provide their performance (ratings based) awards to TCSC HR on spreadsheets to be uploaded directly into HRConnect by a PAPB HR Specialist. After the spreadsheet has been 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 the information in NFC is correct.

Complementary Customer Agency Controls

TCSC 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 TCSC 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.

TCSC Description of Controls

TCSC 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.

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 TCSC 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 TCSC 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 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 on-boarding 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.

Control Objective 18– System Access

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

CFM Description of Controls

CFM follows the Bureau of the 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, IPP, OneStream XF, and oneARC have been documented. The logical access controls are based on Treasury and Bureau of the 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 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 the Bureau of the Fiscal Service and CFM. 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, 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. CFM Oracle system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool. On a daily basis, Oracle inactivity reports are reviewed by a technician. Annually, CFM generates a report listing Oracle system users to validate system users across CFM and each customer agency. User access is updated according to the responses received from the customer agencies.

The Customer Support Division (CSD) employees are assigned Oracle application administrator responsibility in the Oracle application. The employees with the 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 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.

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

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 the Bureau of the Fiscal Service and CFM. 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. Updates to a user's PRISM responsibilities are audited by independent employees. 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. Customer agencies are required to submit a formal request for account termination to revoke a user's access. At that time, PRISM user access is end-dated in the system to remove their access within two business days.

Annually, CFM generates an OBI report listing users for CFM and each customer agency for review. Included for review are requisitioner and buyer approval limits by user. User access is updated according to the responses received from the customer agencies. PRISM end users' access is monitored, and end dated after 90 days of inactivity by an external automation tool. CFM PRISM system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool. On a daily basis, PRISM inactivity reports are reviewed by a technician.

The system administrator responsibility in PRISM is limited to CSD employees requiring access for the performance of job duties.

Invoice Processing Platform

Access to IPP is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me. Internal and external users must complete, sign, and submit an approved 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 CFM 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 the Bureau of the Fiscal Service and CFM. The form defines the user's access specifications, which allows 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. 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 CFM.

Annually, FRB St. Louis sends a list of all IPP users in the Bureau of the Fiscal Service Admin Disburser Account for recertification. CFM reaches out to the customer agency IPP contact to confirm the ongoing appropriateness of the customer agency's IPP users. Updates are made by CFM to user permissions based on the responses received. Then CFM certifies the results in the Shared Document with Secured Access (SDSA) that is operated by FRB St. Louis. Lastly, CFM returns the certified results to FRB St. Louis.

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 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 the Bureau of the Fiscal Service and CFM. 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. CFM 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 by a technician. Annually, CFM generates a report listing system users for each customer agency for review. User access is updated according to the responses received from the customer agencies.

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

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 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 the Bureau of the Fiscal Service and CFM. The form defines the user's access specifications, which will allow the user to perform his/her duties in oneARC. 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 cannot approve their own access (so each agency has a minimum of two authorization officials). Internal employee roles can be one of User, Supervisor, Executive, or Manager. Internal employees' access is also tied to a permission set that allows them to work on their identified customer cases. 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. 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. 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 group mailbox responsible 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.

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.

TCSC Description of Controls

TCSC follows the Department of the Treasury, Departmental Offices 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 GovTA, ConcurGov, GO.gov, moveLINQ, USAStaffing, and HRConnect have been documented. The logical access controls are based on Treasury and TCSC 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.

GovTA[2]

Access to GovTA is 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 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 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 GovTA. Changes to existing elevated access require a new access form to be submitted by the customer agency.

Upon receipt of a 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.

Annually, an HR administrator from the HR Systems Help Desk distributes a list of GovTA timekeepers and supervisors to every customer agency, including TCSC, 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

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

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 LAB and HRSD have these roles.

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 the GovTA support team within TCSC. Administrative access to the underlying GovTA servers and databases is limited to server and database administrators within the OCIO.

ConcurGov

Access to ConcurGov is restricted to users using MFA. MFA is accomplished utilizing CAIA that includes 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, TCSC sends the 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 TCSC 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 TCSC. 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 TCSC helpdesk after the registration information is verified and the profile is created. The email instructs the traveler how to access ConcurGov. Access privileges are granted in accordance with the concept of least privilege required.

Changes to a user's identification (i.e., name change) or to the user's role in ConcurGov requires a TCSC System Access Form to be resubmitted; or 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 TCSC'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, TCSC staff create reports of ConcurGov users and distribute the reports to customer agency Travel contacts (including TCSC) for review and verification of the accounts. Updates are made to user permissions based on the responses received.

GO.gov

Access to GO.gov is restricted to users using MFA. MFA is accomplished utilizing CAIA that includes PIV credentials or ID.me. All users must complete the registration process. After verifying that the traveler is not already in GO.gov or set up in Oracle, TCSC sends the traveler a GO.gov 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 TCSC 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 Departmental Offices and TCSC. The form defines the user's access specifications, which will allow the user to perform his/her duties in GO.gov. TCSC must complete a Profile Template and submit it to IBM via SFTP to create/update user profiles. A confirmation e-mail is sent to the user and agency travel contact(s) by the TCSC helpdesk after the registration information is verified and the profile is created. The email instructs the traveler how to access GO.gov. Access privileges are granted in accordance with the concept of least privilege required.

Changes to a user's identification (i.e., name change) or to the user's role in GO.gov requires a TCSC System Access Form to be resubmitted; or 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. TCSC must complete a Profile Template and submit it to IBM via SFTP to update user profiles.

GO.gov has separate roles that are assigned to users that enforce separation of duties.

Upon TCSC's receipt of an Exit Clearance form or e-mail request, TCSC must complete a Profile Template and submit it to IBM via SFTP to disable the profile and terminate GO.gov access. On an annual basis, TCSC staff creates reports of GO.gov users and distributes the reports to customer agency travel contacts for review and verification of the accounts.

moveLINQ

Access to the moveLINQ system is granted through three portals:

- The Employee Portal can be accessed from the Internet by newly hired, currently employed and retired federal government employees of Treasury and non-Treasury customer agencies.
    - New user accounts are created with the receipt of a "Request for Relocation" provided by the customer agency contact. Access is removed once all relocation records have been deleted from the system.
    - Access is granted using CAIA/SailPoint MFA that includes PIV credential or ID.me.
        - Once CAIA/SailPoint authentication is complete, the user is forwarded to the moveLINQ system if they have been configured for system access.
            - Users can only apply in the In Box their assigned status stamp to documents that have been electronically routed to them.
            - Users can see documents in their My Documents after they have been routed.
            - Users can submit vouchers for processing in the Employee Portal, submitting the documents starts a workflow that sends them to the voucher processing group.

- The Approval Portal users can only be accessed by customer agency (including users in our area) and Third-Party Vendor users.
    - The portal uses CAIA/SailPoint to grant MFA access either using PIV or ID.me.
    - New/modified user accounts are processed with the receipt of a moveLINQ System Access Form designed for either customer agency or third-party vendors.
        - The form is signed by the employee accepting the conditions noted in the form.
        - Then it is signed by either the customer agency contact or third-party vendor contact as assigned by the agency or vendor.
        - After adding or modifying the users account the form is signed by the moveLINQ administrator that added or modified the user's account.
        - Then the form is submitted to either a moveLINQ Administrator, or the RSB Manager for reviewing and signing.
        - Then a moveLINQ Administrator notifies the user and the agency or third-party contact that access has been granted, they also provide guidance documents and the URL for the portal.
            - Once authentication is complete the user is forwarded to the moveLINQ system if they have been configured for system access.
                - Users will only be able to view documents routed to them in their Inbox:
                - Their assigned customer agency/vendor 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.
- Users can only apply their assigned status stamp to documents that have been electronically routed to them.
- The Open Documents option allows users to view the assigned documents after routing.

- Disabling a user's account can be performed with the receipt of the form or an email, that is made into a PDF and signature fields are added for the preparer/first reviewer and by the second reviewer. At that time, the moveLINQ Approval Portal user account is disabled in the system.

- The Expense Management Portal is accessed by Assigned Treasury employees using their PIV card.
  - The portal uses CAIA to grant MFA access using 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.
  - New/modified/disabled Expense Management user accounts are processed with the receipt of a moveLINQ System Access Form.
    - New/modified users sign the document acknowledging acceptance of the requirements to use the system.
    - Disabled users do not sign the document.
    - The moveLINQ System Access Form document for new/modified/disabled users must be signed by a supervisor/manager. Then it is signed by the moveLINQ administrator that added/modified/disabled the user and by the reviewing moveLINQ Branch Manager, System Owner (SO), or appointed backup. At that time, the moveLINQ Expense Management Portal user account is disabled in the system.

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 a System Access Form for End User Application signed by the agency's authorized approver. The end user's signature indicates they are familiar with the Privacy Act information and security requirements and will comply with computer security rules. The form defines the user's access specifications, which will allow the user to perform his/her duties in HRConnect. Changes to existing elevated access require a new access form to be submitted by the customer agency.

User roles are automatically removed from HRConnect when he/she separates from the agency. Upon receipt of a 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 privileged roles to each customer agency for the agency to use in performing a review of access. The HR Systems Help Desk updates the permissions for users based on the responses received from the customer agencies. The Specialist on the HR Systems Help Desk also performs a similar semi-annual review for users with administrative roles to ensure that only authorized users in TCSC have those 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 a 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 a 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.

Complementary Customer Agency Controls

CFM 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, IPP, OneStream and XF access to help ensure appropriateness and provide changes to CFM in a timely manner.
- Notify CFM timely regarding separating employees.
- Routinely review approvers within oneARC to confirm that only authorized users and responsibilities are executing actions and approvals.

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

- Review and approve listings of users with current GovTA, ConcurGov and HRConnect access to help ensure appropriateness and provide changes to TCSC in a timely manner.
- Notify TCSC timely regarding separating employees.
- Notify TCSC timely of any changes to HRConnect, GovTA or USA Staffing authorized approvers.
- Help ensure all personnel actions are submitted in HRConnect timely.

Control Objective 19 – Application Changes

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

CFM Description of Controls

CFM 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 Salesforce, JIRA, and My Oracle Support for Oracle, OBI, and PRISM.

CFM processes standard software releases (i.e., patches) for Oracle, OBI, and PRISM. OCSS provides notification to CFM of standard software releases, along with associated Release Notes outlining changes. Additionally, CFM processes customized application extension changes to Oracle. Access to My Oracle support is monitored and reviewed biannually.

CFM 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. FSID staff develop customizations in a separate development instance. CSD staff test changes by running test scripts and analyzing the results in a separate test environment. Upon successful completion of testing, CSD 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 emergency changes to a production instance of Oracle, OBI, or PRISM, CFM requires verbal approval from a designated on-call manager (for all production instances). CFM application administrators document the emergency change in My Oracle Support on the next business day.

OneStream XF

CFM 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.

CFM 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, CFM 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 CFM 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.

CFM and FSID test the new release in a separate test environment by running test scripts and analyzing the results. CFM 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 CFM, FSID and ARAD running test scripts and analyzing the results. Upon successful completion of testing, CFM 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). Automation Platform Configuration & Management Branch (APCMB) 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.

Changes requiring a Security Impact Analysis (to include those that leverage existing Enterprise SIA's) are submitted to the security program and Policy and Risk Management Branch (PRMB) within the OCIO for analysis. SIA's must be submitted by the ISSO or are routed to the ISSO for approval prior to being submitted for analysis by PRMB. Upon completion (implementation) of the SIA, the security posture must be evaluated in accordance with the SIA, which is either a self or 3rd party assessment. The results are then recorded in the Bureau's Governance, Risk and Compliance platform (ServiceNow GRC).

Once the IV form is signed by both the ISSO and System Owner, a non-developer resource within the APCMB 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 DevForce 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. 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 DevForce ticket is then closed.

TCSC Description of Controls

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

GovTA

For GovTA, TCSC applies standard software releases (i.e., patches) only.

When a new GovTA release is received from UKG, TCSC 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 OCIO. The new GovTA release is not applied to production until it has been successfully tested and then approved by the HRSD Director.

IV. MANAGEMENT OF BUREAU OF FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT'S AND TREASURY COMMON SERVICES 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 CFM and TCDC.

Our examination was limited to the control objectives and related controls specified by CFM and TCSC 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, CFM's and TCSC's controls may not compensate for such weaknesses.

CFM's and TCSC's internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by CFM and TCSC. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by CFM and TCSC, we considered aspects of CFM's and TCSC's control environments, risk assessment processes, 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 policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
1.01	A report identifies all Oracle obligations modified in the previous five days and verifies those amounts reconciled 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.	For a selection of days, inspected the corresponding reports used to identify PRISM to Oracle obligation transactions to determine whether any obligation mismatches identified were reviewed and that actions were taken for documents identified on the reports.	No exceptions noted.
1.02	Upon receipt from the customer agency and/or Procurement, the CFM 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 CFM technician will inquire with the customer agency.	For a selection of customer agencies and manually entered obligations, inspected the corresponding customer agency approvals to determine whether manually entered obligations were approved prior to being entered into Oracle by CFM Staff.	No exceptions noted.
1.03	Approved authorizations in ConcurGov are reconciled daily by TCSC with an OBI report to help ensure that all ConcurGov authorizations have been interfaced and processed into Oracle. If	For a selection of customer agencies and days, inspected the corresponding ConcurGov to Oracle interface reconciliations to determine whether daily reconciliations were performed, any data	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.	interface errors or exceptions identified were corrected, any rejected transactions were manually entered into the ConcurGov, and all approved travel authorizations were interfaced and processed by Oracle.	
1.04	RSB personnel enter PCS Travel authorizations into moveLINQ which routes them to the 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 Approving Officials approved the authorization and Relocation Coordinators stamped the documents as approved.	No exceptions noted.
1.05	A Junior Analyst performs a daily reconciliation between moveLINQ and Oracle to confirm the two systems remain in sync. 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 a junior analyst, all approved travel authorizations in moveLINQ completely and accurately interfaced with Oracle, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
1.06	Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. If discrepancies arise, they are	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 CFM, CFM reviewed them with customer agencies within the past year, they were approved by a secondary user, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	investigated and corrective actions are taken as needed.		operating effectiveness of this aspect of the control.
1.07	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	No exceptions noted.
1.08	Approved requests in GO.gov are reconciled daily by TCSC with an OBI report to help ensure that all GO.gov requests have been interfaced and processed into Oracle. If discrepancies arise, they are investigated and corrective actions are taken as needed.	For a selection of customer agencies and days, inspected the corresponding GO.gov 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 GO.gov, and all approved travel authorizations were interfaced and processed by Oracle.	No exceptions noted.

Control Objective 2 – Disbursements

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
2.01	CFM only processes disbursements for invoices with customer agency approval. 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 CFM or directly to the customer agency. When received by CFM, the customer agency provides approval via the oneARC application, or CFM forwards the invoice to an authorized agency contact for approval before CFM manually processes the obligation in Oracle.	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	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.	For a selection of non-IPP invoices greater than or equal to $2,500 and processed by an accounting technician, inspected the corresponding records to determine whether a secondary accountant reviewed and approved the invoice prior to disbursement.	The following exception was noted: Due to system limitations, CFM management was unable to provide a complete and accurate population of Non-IPP invoices greater than or equal to $2,500 for the prescribed audit

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
			period July 1, 2025, to June 30, 2026; as such, we could not perform operating effectiveness testing of the control.
Management's Response Management concurs with the exception and will initiate appropriate corrective actions.			
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	IPACs that decrease a CFM 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, CFM may obtain customer agency approval after the IPAC has been recorded.	For a selection of IPAC disbursements, inspected the corresponding customer approvals to determine whether CFM obtained customer agency approval 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	TCSC and customer agency travelers enter travel vouchers into ConcurGov and electronically route them to Approving Officials for review and approval.	For a selection of travel vouchers, inspected the corresponding records to determine whether Approving Officials reviewed and approved the voucher in ConcurGov.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
2.07	All third-party invoices are examined by TCSC 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. Relocation Junior Analysts stamp the document in moveLINQ with a status of "approved".	For a selection of third-party invoices, inspected the corresponding records to determine whether TCSC reviewed and approved the voucher upon verification that the invoice was valid, and that a Junior Analyst approved the voucher in moveLINQ.	No exceptions noted.
2.08	A Junior Analyst performs a daily reconciliation between moveLINQ and Oracle to confirm the two systems remain in sync. 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. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
2.09	CFM reviews 10% of all invoices processed by IPP for each customer agency monthly. 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	For a selection of customer agencies and months, inspected the 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 for less than $2,500 are subject to a monthly random sample post payment audit which is performed by an accountant and approved by a Lead Accountant.	For a selection of months, inspected the corresponding reviews of non-IPP invoices for 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. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
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 review 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	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/TCSC category type are subject to a 41-point audit worksheet comprised of 36 critical error checks and 5-noncritical informational checks. The TCSC Travel Sampling Plan is broken down into two separate components: the Quality Sample and	For a selection of customer agencies and 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
	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.	For a selection of customer agencies and 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	A CFM SPS certifying officer compares the number and dollar amount of payments certified in SPS to the payment files generated by Oracle to help ensure that 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 reconciliation performed by the CFM 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. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
2.14	CFM accountants perform reconciliations of SmartPay account statement balances to Accounts Payable transaction details in Oracle which are reviewed by CFM staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM accountants determine the cause of the difference	For a selection of customer agencies and 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	CFM accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by CFM Staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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.	For a selection of customer agencies and 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. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
2.16	Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle.	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 CFM, CFM reviewed them with customer agencies within the past year, they were approved by a secondary user, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
2.17	CFM accountants prepare and submit confirmations to the appropriate trading partners in accordance with the elimination reconciliation guidance. Upon submitting the confirmations to	For a selection of Treasury customer agencies and quarters, inspected the corresponding non-fiduciary transaction confirmations completed by CFM accountants to determine whether	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	the trading partners, CFM works with the trading partners to reconcile transactions/balances and identify and record any necessary adjustments.	reconciliations of transactions and balances with trading partners were completed, and that any necessary adjustments were identified and recorded.	
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 a CFM supervisor or an Agency designee will certify the explanation in GTAS.	For a selection of non-Treasury customer agencies and quarters, inspected the corresponding Intra-governmental Certified Explanation of Balances completed by CFM accountants to determine whether any elimination differences that required an explanation were entered into the GTAS module and a CFM supervisor or Agency designee certified the explanation in GTAS.	No exceptions noted.
2.19	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	No exceptions noted.
2.20	TCSC and customer agency travelers enter travel expense reports into GO.gov and electronically route them to Approving Officials for review and approval.	For a selection of travel vouchers, inspected the corresponding records to determine whether Approving Officials reviewed and approved the voucher in GO.gov.	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 CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
3.01	CFM only processes unfilled customer orders, receivables, and cash receipts with customer agency approval. No approval is required for checks received for deposit directly by CFM 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. CFM 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, CFM may obtain customer agency approval after the cash receipt has been recorded.	For a selection of unfilled customer orders, receivables, and cash receipts, inspected the corresponding customer agency approvals to determine whether CFM obtained customer agency approvals prior to processing the unfilled customer order/receivable/cash receipt and said unfilled customer order/receivable/cash receipt 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.	No exceptions noted.
3.02	CFM accountants perform monthly reconciliations of CARS Account Statement balances to the Oracle general ledger FBWT balances which are reviewed by CFM staff other than the individual performing the reconciliation. If differences are identified during the reconciliations, CFM 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.	For a selection of customer agencies and 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. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
3.03	CFM accountants prepare and submit a quarterly TROR and Debt Collection Activities report for all customer agencies. 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. A CFM supervisory accountant reviews the report. If discrepancies arise, they are investigated and corrective actions are taken as needed. As applicable, CFM monitors and pursues collection of delinquent balances.	For a selection of customer agencies and quarters, inspected the corresponding TROR reports completed by CFM accountants to determine whether: they were completed, all activities were reconciled with receivables due from the public, the reports were reviewed by a CFM supervisory accountant, and any discrepancies noted were resolved.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
3.04	CFM 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, CFM works with the trading partners to reconcile transactions/balances and identify and record any necessary adjustments.	For a selection of Treasury customer agencies and quarters, inspected the corresponding non-fiduciary transaction confirmations completed by CFM 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 a CFM supervisor or a customer agency designee will certify the explanation in GTAS.	For a selection of non-Treasury customer agencies and quarters, inspected the corresponding Intra-governmental Certified Explanation of Balances completed by CFM accountants to determine whether any elimination differences that required an explanation were entered into the GTAS module and a CFM supervisor or Agency designee certified the explanation in GTAS.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
3.06	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	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 CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
4.01	The CFM designated accounting technician (who does not have Oracle access to post accounts receivable transactions) receives, opens, and logs all checks received in CFM'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.	For a selection of check deposit logs, inspected the corresponding records to determine whether a CFM administrative staff member, who did not have Oracle access to post account receivable transactions, received, opened, and logged all checks received in the branch's check deposit log 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 safe used to store checks before they are ready to be deposited to note whether such access would prevent unauthorized persons from obtaining access to the checks.	No exceptions noted.
4.03	Upon settlement with the FRB, the CFM accounting technician reconciles the batch list with the paper checks. If discrepancies arise, they are investigated and corrective actions are taken as needed.	For a selection of check deposit records, inspected the corresponding check attributes to determine whether the CFM accounting technician performed the reconciliation and discrepancies identified were addressed.	No exceptions noted.

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

Control Objective 5 – Payroll and Leave Accruals

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
5.01	Monthly payroll accruals are recorded and reviewed monthly 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 and months, inspected the corresponding monthly payroll accrual invoices to determine whether the customer agencies' monthly payroll accruals were documented, entered timely and accurately, reversed, and reviewed monthly by a CFM accountant and supervisor and that any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
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 and months, inspected the corresponding leave accruals to determine whether the leave accruals were documented, entered timely and accurately, reversed, and reviewed monthly by a CFM accountant and supervisor and that any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

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 CFM 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 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.	For a selection of customer agencies and pay periods, inspected the corresponding interface status reports to determine whether the payroll accountant reviews said report and corrects 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.	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 require corrections are posted in either the current accounting period or in a subsequent accounting period.	For a selection of customer agencies and 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 a CFM accountant, any differences identified were investigated and resolved, reconciliations were reviewed by a supervisory accountant, and any corrections made were posted in the current or subsequent accounting periods.	No exceptions noted. With respect to the difference resolution aspect of this control, no differences were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

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. CFM 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 CFM customer agencies. Once the changes to the USSGL are approved by Treasury and the new TFM guidance is issued (generally mid-summer), the CFM USSGL Team will communicate the appropriate changes to CFM Oracle system administrators to 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.
7.02	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.	For a selection of customer agencies and months, inspected the corresponding general ledger account reconciliations completed by CFM accountants to determine whether: the 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 a CFM supervisor.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
7.03	CFM accountants prepare budgetary to proprietary account relationship reconciliations monthly 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 and months, inspected the corresponding budgetary-to-proprietary account relationship reconciliations completed by CFM accountants to determine whether the reconciliations were performed and reviewed by a CFM 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.
7.04	Accountants generate GTAS bulk files within Oracle, where automated edit checks based on USSGL attributes ensure only valid files are created—any files failing these checks are not produced, preventing erroneous data from entering the submission process. Once a file passes Oracle's edit checks, CFM manually uploads it into the GTAS system. Following the upload, a designated reviewer, such as a supervisory accountant, independently examines the GTAS submission and system feedback for any Treasury Appropriation Fund Symbol (TAFS) failures. The reviewer verifies that all failed TAFS have been thoroughly investigated and resolved, and documents evidence of both the review and the resolution, ensuring a transparent and accountable process.	For a selection of customer agencies and months, inspected the corresponding review to determine whether USSGL validations were performed and any failures identified were resolved.	No exceptions noted.
7.05	After submitting the adjusted trial balances into TIER, CFM accountants review the edit reports and resolve any invalid attributes or out-of-balance conditions. CFM accountants document this review by completing the TIER Submission	For a selection of customer agencies and months, inspected the corresponding TIER Submission Checklists to determine whether CFM accountants reviewed GTAS edit reports and resolved any	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	Checklist, which is further reviewed by a supervisor.	invalid attributes or out-of-balance attributes included in corresponding TIER submissions.	
7.06	CFM accountants compare TFM financial statement crosswalks to CFM's internally prepared financial statements or OneStream XF tables to determine compliance with the TFM reporting requirements. CFM accountants investigate and resolve any differences between TFM crosswalks and CFM's internally prepared financial statements.	For a selection of customer agencies and quarters, inspected the corresponding TIER Submission Checklists to determine whether compared TFM financial statement crosswalks to CFM'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. With respect to the difference resolution aspect of this control, no differences were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

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 CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
8.01	In the automated journal entry process method, accruals are recorded by using the automated journal entry process. With this method, a CFM 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 automated journal entries, inspected the corresponding spreadsheet templates of the period-end accrual data for goods/services loaded into Oracle to determine whether the entries were imported successfully, reviewed and approved by a supervisory accountant, 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. Workers' compensation and unemployment insurance accruals are based on reports provided by the Department of Labor. Customer agencies provide data for year-end payroll accruals. For the manual year-end accruals, a supervisor reviews and posts the accrual.	For a selection of manual journal entries, inspected the corresponding 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, CFM 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	For a selection of customer agencies and months, inspected the corresponding reconciliation of revenue and expense accrual balances in the general ledger to the subledger detail to determine whether CFM accountants prepared the	No exceptions noted. With respect to the difference resolution aspect of this control, no differences were

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.	reconciliation, a supervisor reviewed the reconciliation, and any differences noted were corrected by an accounting technician or accountant in a subsequent accounting period.	identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
8.04	Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. The system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. 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 CFM, CFM reviewed them with customer agencies within the past year, they were approved by a secondary user, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
8.05	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	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 CFM 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 a CFM 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 a CFM supervisor/manager or customer agency representative, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
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 and months, inspected the corresponding TIER Submission Checklists to determine whether TIER submissions were reviewed by a CFM supervisor before being processed by TIER, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
9.03	CFM prepares monthly Prompt Payment reports for its customer agencies following Treasury guidelines. Independent accountants or analysts	For a selection of customer agencies and months, inspected the corresponding review of the Prompt Payment reports to determine whether they were	No exceptions noted. With respect to the discrepancy resolution

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	review all reports. If discrepancies arise, they are investigated and corrective actions are taken as needed.	reviewed before submission by an independent accountant, and any discrepancies identified were corrected.	aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
9.04	CFM accountants compare TFM financial statement crosswalks to CFM's internally prepared financial statements or OneStream XF table to help ensure compliance with the reporting requirements. CFM investigates and resolves any differences between TFM crosswalks and CFM's internally prepared financial statements.	For a selection of customer agencies and quarters, inspected the corresponding reconciliation of customer agencies' TFM financial statement crosswalks to CFM'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. With respect to the difference resolution aspect of this control, no differences were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
9.05	For Treasury and DHS customer agencies, CFM accountants compare the quarterly financial statements to CFM's internally prepared financial statements and resolve any differences. The comparison is reviewed by a supervisor.	For a selection of customer agencies and quarters, inspected the corresponding results of CFM's comparison of the TFM financial statement crosswalk and internally prepared financial statements to determine whether CFM performed the reconciliations, the reconciliations were reviewed by a supervisor, and any differences noted were investigated and resolved.	No exceptions noted.
9.06	If applicable for non-Treasury customer agencies, CFM accountants prepare the BS, SNC, and SCNP during the third and fourth quarters for review by a	For a selection of customer agencies and quarters, inspected the corresponding results of CFM's comparison of the TFM financial statement	No exceptions noted. With respect to the difference resolution

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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. If discrepancies arise, they are investigated and corrective actions are taken as needed.	crosswalk and internally prepared financial statements to determine whether CFM accountants prepared the BS, SNC, and SCNP during the third and fourth quarters, and in the fourth quarter, the SBR and SCA are included, CFM accountants compared the OneStream XF Trail Balance to the Oracle trial balance and GTAS balance, comparisons were reviewed by a supervisor, and CFM investigated and resolved any differences.	aspect of this control, no differences were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
9.07	For Treasury and DHS customer agencies, accountants were required to prepare third and fourth quarter financial statement variance analyses in FY 2026, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by a CFM supervisory accountant and approved by the bureau CFO or designee prior to submission to Treasury.	For a selection of customer agencies and quarters, inspected the corresponding financial statement variance analysis to determine whether CFM accountants prepared fourth quarter financial statement variance analyzes, such analyses were performed and reviewed by a CFM supervisor accountant and approved by the bureau CFO prior to submission to Treasury.	No exceptions noted.
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 2026, in accordance with guidance in OMB Circular A-136. These analyses were reviewed by a CFM supervisory accountant prior to submission to OMB.	For a selection of customer agencies and quarters, inspected the corresponding financial statement variance analysis to determine whether CFM accountants prepared fourth quarter financial statement variance analyses, and such analyses were reviewed by a CFM supervisor accountant prior to submission to OMB.	No exceptions noted.
9.09	CFM accountants prepare and submit a quarterly TROR and Debt Collection Activities report for all customer agencies. These reports are reviewed by a CFM supervisory accountant prior to submission to Treasury. If discrepancies arise, they are	For a selection of customer agencies and quarters, inspected the corresponding TROR and Debt Collection Activities Reports to determine whether the reports were prepared by a CFM accountant, reviewed by a CFM supervisory accountant and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	investigated and corrective actions are taken as needed.		selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
9.10	For non-Treasury and non-Homeland Security customer agencies, DATA Act reporting is performed monthly. For those customer agencies, three files are submitted to the governmentwide DATA Act Broker system (Broker) monthly. The Broker has validation checks with the GTAS submissions. The accountants review the reports produced by 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's monthly attestation statement, CFM 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. CFM updates the status of the three monthly DATA Act File submissions to "Certified" on behalf of the customer agency.	For a selection of non-Treasury and non-Homeland Security customer agencies and 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. For a selection of non-Treasury and non-Homeland Security customer agencies and quarters, inspected the corresponding DATA act submissions to determine whether the customer agencies certified the three monthly DATA Act submissions for the selected quarter.	No exceptions noted.

Control Objective 10 – Budget

Controls provide reasonable assurance that budget entries are complete, accurate, timely processed, and documented in accordance with CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
10.01	Budget execution system control settings, beyond the legal level, are determined by the customer agency and configured in Oracle by USB CFM staff. These system settings undergo an annual review with the customer agency, followed by input into Oracle by USB staff and a subsequent secondary review to ensure completeness and accuracy in Oracle. 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 CFM and CFM reviewed them with customer agencies within the past year, they were approved by a secondary user, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
10.02	CFM accountants prepare budgetary to proprietary account relationship reconciliations monthly, 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 and months, inspected the corresponding budgetary-to-proprietary account relationship reconciliations completed by CFM 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 a CFM supervisor.	No exceptions noted.
10.03	CFM accountants perform monthly reconciliations of CARS Account Statement balances to general ledger FBWT balances which are reviewed by CFM staff other than the individual performing the	For a selection of customer agencies and months, inspected the corresponding reconciliations to determine whether accountants performed reconciliations of the CARS Account Statements	No exceptions noted. With respect to the discrepancy resolution

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	reconciliation. If differences are identified during the reconciliations, CFM 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.	and general ledger FBWT balances, reviews were completed, and any discrepancies noted were resolved.	aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
10.04	For appropriations subject to annual enactment, CFM verifies the approved amount against the annual appropriations process, continuing resolution calculations, enacted legislation, or Treasury documentation before entry, and carefully documents and retains evidence of this verification. Apportionments are entered in Oracle only after confirming the accuracy of the customer agency's SF 132, Apportionment and Reapportionment Schedule, with records maintained for each review and entry. Upon receiving the customer agency's budget plan or reprogramming guidance, CFM allocates funding to the agency's accounting values, ensuring that allocations are consistent with the provided details. All allocations are thoroughly documented and subject to supervisory review, supporting transparency and compliance throughout the process.	For a selection of customer agencies who perform annual enactments, inspected the corresponding continuing resolution (CR), enacted appropriation legislation, or Treasury documentation, SF132 and Oracle entry to determine CFM reviewed and allocated funding after approval.	No exceptions noted.
10.05	For sources of funds not subject to annual appropriations (e.g., reimbursable or revolving accounts), CFM enters appropriations and apportionments based on the customer agency's SF	For a selection of customer agencies who do not perform annual enactments, inspected the corresponding SF132, recorded reimbursable activity, and Oracle entry to determine CFM	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	132 and recorded reimbursable activity. CFM reviews and documents the supporting activity prior to allocation and retains evidence of compliance.	reviewed and allocated funding based on the budget plan or recorded reimbursable activity.	
10.06	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	No exceptions noted.

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 CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
11.01	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.	For a selection of customer agencies and 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 and 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.
11.03	In coordination with Oracle, CFM has developed and implemented a standard document-numbering scheme to avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	Inspected the standard document numbering scheme to determine that it would avoid duplicate document processing and to enable readers of CFM reports to better identify and/or determine the nature of transactions processed by CFM.	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	CFM 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 CFM accountant then enters the request into FedInvest and generates a buy request confirmation report for the entered transaction. Buy requests are prepared by a CFM accountant and a daily work package is then created with all the supporting documents and then two additional CFM accountants review the entered information for accuracy. Each CFM 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).	For a selection of investment purchases, inspected the corresponding investment purchase review documentation to determine whether the investment purchases were reviewed by CFM staff other than the individual who processed the investment purchase, and any discrepancies identified were followed up on and resolved.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.
12.02	CFM accountants perform a daily reconciliation which compares the investment account transactions within FedInvest to the dollar amounts recorded in Oracle to verify the systems reconcile.	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	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	If discrepancies arise, they are investigated and corrective actions are taken as needed.	discrepancies noted during the reconciliation were addressed.	
12.03	CFM accountants perform 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 CFM accountant. If discrepancies exist with either reconciliation, research is conducted to determine the cause, adjust investments if necessary and document corrective actions.	For a selection of customer agencies and months, inspected the corresponding investment reconciliations to determine whether investment activity was reconciled, reviewed by a supervisory CFM accountant, and any discrepancies noted during the reconciliation were addressed.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

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 CFM policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
13.01	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.	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.	No exceptions noted.
13.02	Daily, 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.	For a selection of days, inspected the corresponding audit reports signed by the reviewing CFM staff to determine whether the Supplier and Bank record changes were reviewed and approved, and any discrepancies identified were corrected.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

PROCUREMENT PROCESSING CONTROLS

Control Objective 14 – Acquisitions and Contracts

Controls provide reasonable assurance that contract awards are executed by a warranted Contracting Officer who certifies that the award is complete, accurate, and documented in accordance with TCSC policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
14.01	The Contracting Officer reviews the contract file to ensure it is complete, accurate, and compliant with the Federal Acquisition Regulation (FAR) and applicable TCSC requirements. To ensure compliance, identified discrepancies are investigated, and appropriate corrective actions are taken. Only a warranted Contracting Officer has the authority to sign a contract award that obligates the Government. The Contracting Officer's signature certifies that the contract is complete, accurate, and supported by the required acquisition documentation and that the award complies with applicable legal and regulatory requirements.	For a selection of acquisitions awarded, inspected the corresponding award document, 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 legal and regulatory requirements, and any discrepancies identified were resolved.	No exceptions noted. With respect to the discrepancy resolution aspect of this control, no discrepancies were identified in our selection. As a result, we were unable to determine the operating effectiveness of this aspect of the control.

Control Objective 15 – Sufficiently Funded Requisitions

Controls provide reasonable assurance that award requisitions are approved by a warranted Contracting Officer acting within their delegated warrant authority and supported by sufficient funding.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
15.01	TCSC management has configured the automated contract writing system, PRISM, to enforce a Contracting Officer warrant authority by restricting award approvals to each Contracting Officer's authorized dollar threshold, thereby preventing awards that exceed delegated warrant authority.	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.	No exceptions noted.
15.02	To avoid deficiencies, PRISM also includes controls that prevent contract awards from being executed without sufficient funding.	Observed a TCSC 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 and allowed the award when the amount was equal to or less than the funding provided.	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	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. 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. 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, resolves any issues that stopped the action from applying or applying properly. 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.	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 by the appropriate personnel.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
16.02	Employee separations actions are authorized by TCSC HR staff in EBB, WRB, or PAPB. 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.	Inspected the corresponding HR separation listing and the TCSC HRConnect active employee listing to determine whether there were separated employees who retained access to HRConnect. For a selection of separating employee personnel actions in HRConnect, inspected the corresponding separation request documentation to determine whether the requested actions were reviewed, approved, and carried out by the appropriate personnel.	No exceptions noted.
16.03	TCSC 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. Depending on the type of personnel action, TCSC HR staff in 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 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,	For a selection of customer agencies and 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
	resolves any issues that stopped the action from applying or applying properly.		
16.04	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 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 the information in NFC is correct.	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 HR Assistant/Specialist, and the action was correctly applied.	No exceptions noted.

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 FEHB and TSP 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. 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 the information in NFC is correct.	For a selection of customer agencies and 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 HR Assistant/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: • Separation from federal service. • Transfer to a Public International Organization. • Military reservists who are activated to military duty and elect to receive a lump sum payment for annual leave or have a balance of restored annual leave or compensatory time. • Employee's compensatory time balance expired, depending on the employee's Fair Labor Standards Act (FLSA) status and the	For a selection of customer agencies and employees who received payment for unused annual leave or compensatory time, inspected the corresponding approval forms, payment reports, timecards, verification payments, and NFC screenshots to determine whether approvals were obtained, criteria were met, and the employee was appropriately paid.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	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.		
17.03	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.	For a selection of customer agencies and written employee requests for payroll changes and/or deductions submitted to PAPB, inspected the corresponding approval forms, HRC screenshots and NFC screenshots to determine whether the request was submitted, approved (if needed) and correctly applied.	The following exception was noted: For two (2) out of 25 written requests for payroll changes requested by a customer agency, TCSC management incorrectly processed the changes in HRConnect. For the same two (2) out of the 25 written requests for payroll changes requested by a customer agency, the secondary reviews failed to detect the incorrectly processed change in HRConnect.

Management's Response

Management concurs with the exception. Upon notification of the exception, Management corrected the two payroll change document requests in HRConnect to accurately reflect the requested change. Further, Management completed a review of all payroll change document requests submitted for processing during the examination period and determined that all other requested payroll change documents were processed appropriately. Finally, for one of the noted exceptions, the payroll change document request related to professional liability insurance (PLI) is an infrequent payroll change request document and is not typically associated with customer agency requests.

KPMG inquired of Management and inspected Management's analysis of payroll change document requests submitted and processed during the examination period to determine that no inappropriate payroll document change requests were identified.

GENERAL COMPUTER CONTROLS

Control Objective 18 – System Access

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

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
Oracle and OBI			
18.01	Access to Oracle and OBI are restricted to users using multifactor authentication (MFA). MFA is accomplished utilizing 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 and OBI users must complete, sign, and submit an approved 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 the Bureau of the Fiscal Service and CFM. 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 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.	For a selection of changes to Oracle user profiles, inspected the corresponding authorizing documentation to determine whether updates to access rights were authorized, and access was granted as authorized.	No exceptions noted.
18.04	Customer agencies are required to submit a formal request for account termination to revoke a user's	For a selection of requests for the termination of customer agency employees' Oracle access,	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	access. At that time, Oracle user access is end-dated in the system to remove their access within two business days.	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.	
18.05	Oracle end users' access is monitored and end dated after 90 days of inactivity by an external automated tool. CFM Oracle system administrator access is also monitored and end-dated after 30 days of inactivity by an external automation tool.	For a selection of days, inspect the corresponding daily Oracle inactivity reports to determine whether the reports were reviewed and users were removed as appropriate.	No exceptions noted.
18.06	Annually, CFM generates a report listing Oracle system users to validate system users across CFM and each customer agency. User access is updated according to the responses received from the customer agencies.	For a selection of customer agencies, inspected the corresponding annual Oracle user access review to determine whether the annual reviews were performed and changes provided by the customer agencies were applied. Inspected the corresponding CFM/Bureau of the Fiscal Service annual Oracle user recertification and the system-generated user access list to determine whether CFM completed Oracle user recertification and modifications were made as needed.	No exceptions noted.
18.07	The Customer Support Division (CSD) employees are assigned Oracle application administrator responsibility in the Oracle application. These individuals occasionally require temporary access privileges as functional users to address user inquiries.	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.

PRISM			
18.08	Access to PRISM is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, 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.
18.09	Prospective PRISM users must complete, sign, and submit an approved 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 the Bureau of the Fiscal Service and CFM. 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.	No exceptions noted.
18.10	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. Updates to a user's PRISM responsibilities are audited by independent employees. 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.	For a selection of changes to PRISM user accounts, inspected the corresponding authorizing documentation to determine whether updates to the accounts were authorized, access was granted as authorized, and access was audited by independent employees for appropriateness.	No exceptions noted.
18.11	Customer agencies are required to submit a formal request for account termination to revoke a user's access. At that time, PRISM user access is end-dated in the system to remove their access within two 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	No exceptions noted.

		were completed and removal of access was performed in a timely manner.	
18.12	PRISM end users' access is monitored and end dated after 90 days of inactivity by an RPA. CFM PRISM system administrator access is also monitored and end-dated after 30 days of inactivity by an RPA. On a daily basis, PRISM inactivity reports are reviewed by a technician	For a selection of days, inspect the corresponding daily PRISM inactivity reports to determine whether the reports were reviewed and users were removed as appropriate.	No exceptions noted.
18.13	Annually, CFM generates an OBI report listing users for CFM and each customer agency for review. Included for review are requisitioner and buyer approval limits by user. User access is updated according to the responses received from the customer agencies.	For a selection of customer agencies and 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 review and changes provided by the Customer Agencies were applied. Inspected the corresponding CFM/Bureau of the Fiscal Service annual PRISM user recertification and the system-generated user access list to determine whether CFM completed PRISM user recertification and modifications were made as needed.	No exceptions noted.
18.14	The system administrator responsibility in PRISM is limited to CSD employees requiring access for the performance of job duties.	Inspected the corresponding PRISM user listing to determine whether individuals with the system administrator responsibility were appropriate and from the group that were allowed to have this role.	No exceptions noted.

GovTA			
18.15	Access to GovTA is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials, derived PIV, ID.me or Login.gov.	Observed a GovTA logon session to note whether the user was required to use CAIA.	
18.16	Users that require new or modified elevated access (e.g., timekeeper, supervisor) are given that level of access following receipt of a supervisor-approved 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 GovTA.	For a selection of new/modified GovTA users with elevated privileges, inspected the corresponding System Access Form for End User Applications 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.
18.17	Upon receipt of a 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.	For a selection of removed GovTA users, inspected the corresponding emails or System Access Form for End User Applications forms to determine whether a HR administrator from the HR Systems Help Desk removed any access.	No exceptions noted.
18.18	Annually, an HR administrator from the HR Systems Help Desk distributes a list of GovTA timekeepers and supervisors to every customer agency, including TCSC, to support their annual access review process. The list is limited to those timekeepers and supervisors who are not currently	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	No exceptions noted.

	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. Updates are made to the users permissions based on the responses received.	changes identified by customer agencies were applied. Inspected the corresponding TCSC annual GovTA user recertification and the system-generated user access list to determine whether TCSC completed a GovTA user recertification and modifications were made as needed.	
18.19	The HR Systems Help Desk also conducts a semi-annual review of GovTA users with Administrator and HR Administrator access. This review is to ensure that only authorized users in LAB and HRSD have these roles.	For a selection of semi-annual reviews of privileged users, inspected the corresponding evidence of the review to determine whether semi-annual access reviews were completed and that only authorized users in LAB and HRSD have privileged access.	The following exception was noted: For one out of two semi-annual reviews selected for testing, TCSC management was unable to validate that (1) the review listing was complete and accurate, (2) the reviewer was an authorized individual independent of the population being reviewed, (3) the review was performed in a timely manner, and (4) access modifications requested during the review were applied.
<u>Management's Response</u> Management concurs with the exception and will initiate appropriate corrective actions.			
18.20	The system administrator and HR administrator roles in GovTA are limited to the GovTA support team within TCSC.	Inspected the corresponding GovTA user listing to determine whether only users in the GovTA	No exceptions noted.

		support team are assigned the HR administrator or system administrator roles.	
18.21	Administrative access to the underlying GovTA servers and databases is limited to server and database administrators within the OCIO.	Inspected the corresponding listing of GovTA user accounts with the listing of users with administrative access to the GovTA servers and databases and organizational chart to determine whether administrative access was limited to server administrators within OCIO.	No exceptions noted.
ConcurGov			
18.22	Access to ConcurGov is restricted to users using MFA. MFA is accomplished utilizing CAIA that includes 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.
18.23	All ConcurGov users must complete the registration process. After verifying that the traveler is not already in ConcurGov, or set up in Oracle, TCSC sends the 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 TCSC 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 TCSC. The form defines the user's access specifications, which will allow the user to perform his/her duties in ConcurGov.	For a selection of new ConcurGov users, inspected the corresponding New User Registration Worksheet and Supplier Entry Form to determine whether the forms were completed, and access was granted as requested. For a selection of new Budget Reviewers or Approving Officials ConcurGov users, inspected the corresponding System Access Form or email from an Approving Official to determine whether the forms or e-mails were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as requested.	No exceptions noted.

18.24	Changes to a user's identification (i.e., name change) or to the user's role in ConcurGov requires a TCSC System Access Form to be resubmitted; or 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.	For a selection of changes to ConcurGov users, inspected the corresponding System Access Form or email request to determine whether access changes were documented, access was authorized, and authorized access matched that which was configured in ConcurGov.	No exceptions noted.
18.25	Upon TCSC'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.	For a selection of removed ConcurGov users, inspected the corresponding Exit Clearance form or email request and the ConcurGov access list to determine whether ConcurGov access was removed.	No exceptions noted.
18.26	On an annual basis, TCSC staff create reports of ConcurGov users and distribute the reports to customer agency Travel contacts (including TCSC) 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. Inspected the corresponding TCSC annual ConcurGov user recertification and the system-generated user access list to determine whether TCSC completed ConcurGov user recertification and modifications were made as needed.	No exceptions noted.
GO.gov			
18.27	Access to GO.gov is restricted to users using MFA. MFA is accomplished utilizing CAIA that includes PIV credentials or ID.me.	Observed a user access the GO.gov system to note whether the user was required to use CAIA in order to authenticate.	No exceptions noted.
18.28	All GO.gov users must complete the registration process. After verifying that the traveler is not already in GO.gov, or set up in Oracle, TCSC sends	For a selection of new GO.gov users, inspected the corresponding New User Registration Worksheet and Supplier Entry Form to determine whether the	No exceptions noted.

	the traveler a GO.gov 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 TCSC 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 Departmental Offices and TCSC. The form defines the user's access specifications, which will allow the user to perform his/her duties in GO.gov. TCSC must complete a Profile Template and submit it to IBM via SFTP to create/update user profiles.	forms were completed, and access was granted as requested. For a selection of new Budget Reviewers or Approving Officials GO.gov users, inspected the corresponding System Access Form or email from an Approving Official to determine whether the forms or e-mails were completed, employees acknowledged that they understood the Privacy Act requirements, access was authorized, and access was granted as requested.	
18.29	Changes to a user's identification (i.e., name change) or to the user's role in GO.gov requires a TCSC System Access Form to be resubmitted; or 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. TCSC must complete a Profile Template and submit it to IBM via SFTP to update user profiles.	For a selection of changes to GO.gov users, inspected the corresponding System Access Form or email request to determine whether access changes were documented, access was authorized, and authorized access matched that which was configured in GO.gov.	No exceptions noted.
18.30	Upon TCSC's receipt of an Exit Clearance form or e-mail request, TCSC must complete a Profile Template and submit it to IBM via SFTP to disable the profile and terminate GO.gov access.	For a selection of removed GO.gov users, inspected the corresponding Exit Clearance form or email request and the GO.gov access list to determine whether GO.gov access was removed.	No exceptions noted.

moveLINQ – Employee Portal			
18.31	Access to moveLINQ Employee Portal is restricted to users using CAIA/SailPoint MFA that includes PIV credential 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.
18.32	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 Employee Portal users, inspected the corresponding Request for Relocation forms to determine whether the requests were documented and access was configured as authorized.	No exceptions noted.
18.33	moveLINQ Employee Portal access is removed once all relocation records have been deleted from the system.	For a selection of removed moveLINQ Employee Portal users, inspected the corresponding moveLINQ System User Audit Report to determine whether the removal of access was documented and performed.	No exceptions noted.
moveLINQ – Agency Contract/Approval Portal			
18.34	Access to moveLINQ Approval Portal is restricted to users using CAIA/SailPoint MFA that includes PIV credentials or ID.me.	Observed a user login to moveLINQ's web-based Approval Portal to note if they were required to authenticate via MFA.	No exceptions noted.
18.35	New/modified moveLINQ Approval Portal user accounts are processed with the receipt of a moveLINQ System Access Form designed for either customer agency or third-party vendors that has been signed by the user acknowledging acceptance of the requirements to use the system. The document also must be signed by the customer agency or third-party vendor contact, the moveLINQ administrator that added or modified the user and the reviewing moveLINQ administrator/RSB Manager.	For a selection of new/modified moveLINQ Approval Portal users, inspected the corresponding moveLINQ System Access Forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.

18.36	To remove/disable a user's moveLINQ Approval Portal account, customer agencies or third-party vendors submit a request for account termination via a moveLINQ System Access Form or email that is signed by the preparer/first reviewer and by a second reviewer. At that time, the moveLINQ Approval Portal user account is disabled in the system.	For a selection of removed moveLINQ Approval Portal users, inspected the corresponding moveLINQ System Access Forms or email requests and moveLINQ System User Audit Report to determine whether the removal/disablement of access was documented, performed, and reviewed.	No exceptions noted.
moveLINQ – Expense Management Portal			
18.37	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.
18.38	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/manager, the moveLINQ administrator that added or modified the user, and the reviewing moveLINQ Branch Manager, System Owner (SO), or appointed backup. These user roles/permissions are granted based on the principle of separation of duties through assigned access authorizations and the least privilege principle.	For a selection of new/modified moveLINQ Expense Management Portal users, inspected the corresponding moveLINQ System Access Forms to determine whether the requests were documented, approved, and access was configured as authorized.	No exceptions noted.
18.39	A user's moveLINQ Expense Management Portal account is removed/disabled upon receipt of a moveLINQ System Access Form. The document must be signed by a supervisor/manager, the moveLINQ administrator that disabled the user, and the reviewing moveLINQ Branch Manager,	For a selection of removed moveLINQ Expense Management Portal users, inspected the corresponding moveLINQ System Access Forms and moveLINQ System User Audit Report to determine whether the removal of access was documented, performed, and reviewed.	No exceptions noted.

	System Owner (SO), or appointed backup. At that time, the moveLINQ Expense Management Portal user account is disabled in the system.		
IPP			
18.40	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.
18.41	Internal and external users must complete, sign, and submit an approved 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 CFM 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 the Bureau of the Fiscal Service and CFM. The form defines the user's access specifications, which allows 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.	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.
18.42	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 CFM.	For a selection of employee termination requests made from customer agencies and for Bureau of the Fiscal Service users, inspected the corresponding user access termination requests to determine	No exceptions noted.

		whether employees did not retain access to IPP after their termination date.	
18.43	Annually, FRB St. Louis sends a list of all IPP users in the Bureau of the Fiscal Service Admin Disburser Account for recertification. CFM reaches out to the customer agency IPP contact to confirm the ongoing appropriateness of the customer agency's IPP users. Updates are made by CFM to user permissions based on the responses received. Then CFM certifies the results in the Shared Document with Secured Access (SDSA) that is operated by FRB St. Louis. Lastly, CFM returns the certified results to FRB St. Louis.	For a selection of customer agencies, inspected the corresponding annual account recertification for IPP supporting documentation to determine whether CFM contacted customer agencies to initiate the recertifications, and results were returned to FRB St. Louis so that access changes could be applied as necessary. Inspected the corresponding CFM/Bureau of the Fiscal Service IPP user recertification to determine whether it was completed and sent to FRB St. Louis.	No exceptions noted.
OneStream XF			
18.44	Access to OneStream XF is restricted to users using MFA. MFA is accomplished utilizing CAIA mechanisms PIV credentials or ID.me.	Observed an OneStream XF user log in to note whether the user was required to use CAIA.	No exceptions noted.
18.45	Prospective OneStream XF users must complete, sign, and submit an approved 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 the Bureau of the Fiscal Service and CFM. The form defines the user's access specifications, which will allow the user to perform his/her duties in OneStream XF.	For a selection of new 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.
18.46	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,	For a selection of employee changes to OneStream XF users, inspected the corresponding user access request forms to determine whether the requests	No exceptions noted.

	requesting the change, and defining what access should be added/deleted/changed.	were documented, employees acknowledged that they understood the Privacy Act requirements, access was approved, and access was configured as authorized.	
18.47	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.	For a selection of employee termination requests made from customer agencies and Bureau of the Fiscal Service, inspected the corresponding email requests and inactivity reports to determine whether the termination of OneStream access were completed and removal of access was performed in a timely manner.	No exceptions noted.
18.48	OneStream XF end users' access is monitored, and end dated after 60 days of inactivity by an external automation tool. CFM 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 by a technician.	For a selection of days, inspected the corresponding OneStream XF inactivity reports to determine whether the reports were reviewed and users were removed as appropriate.	No exceptions noted.
18.49	Annually, CFM generates a report listing system users for each customer agency for review. User access is updated according to the responses received from the customer agencies.	For a selection of customer agencies, inspected the corresponding annual account recertification and the system-generated user access list to determine whether CFM contacted customer agencies to initiate the recertification and made related changes to access permissions in OneStream XF as necessary, based on the customer agency's response. Inspected the corresponding CFM/Bureau of the Fiscal Service OneStream XF user recertification to determine whether CFM Service Branch Desk completed OneStream XF user recertification and modifications were made as needed.	No exceptions noted.

18.50	The system administrator responsibility in OneStream XF is limited to certain CSD and FSID employees requiring access for the performance of job duties. Administrator duties include user set up and cube/role/workflow creation and assignment.	Inspect the corresponding listing of OneStream XF administrators and the Bureau of the Fiscal Service personnel listing to determine whether all administrators were CSD or FSID employees.	No exceptions noted.
HRConnect			
18.51	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.
18.52	Users that require new or modified elevated access (e.g., admin, HR and PDS roles) are given that level of access following receipt of a 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/modified HRConnect users with elevated privileges, inspected the corresponding System Access Forms for End User Application 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.
18.53	Upon receipt of a 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.	For a selection of removed HRConnect users, inspected the corresponding System Access Forms for End User Application or email requests and HRConnect access list to determine whether the removal of access was documented and performed.	No exceptions noted.
18.54	Semi-annually, an HR Specialist on the HR Systems Help Desk sends out a list of users with privileged roles to each customer agency for the agency to use in performing a review of access. The HR Systems Help Desk updates the permissions for users based on the responses	For a selection of customer agencies and semi-annual instances, inspected the corresponding customer agencies semi-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	No exceptions noted.

	received from the customer agencies. The Specialist on the HR Systems Help Desk also performs a similar semi-annual review for users with administrative roles to ensure that only authorized users in TCSC have those roles.	changes provided by the Customer Agencies were applied. For a selection of TCSC semi-annual HRConnect user recertification instances, inspected the corresponding reviews and the system-generated user access list to determine whether TCSC completed HRConnect user recertification and modifications were made as needed.	
USA Staffing Onboarding			
18.55	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 Onboarding to note whether the user was required to use CAIA.	No exceptions noted.
18.56	Users that require new or modified elevated access (e.g., admin, and HR roles) are given that level of access following receipt of a 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.	For a selection of new/modified USA Staffing Onboarding users with elevated privileges, inspected the corresponding System Access Forms for End User Application 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.
18.57	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 a review of access. The HR Systems Help Desk updates the permissions for users based on the responses received from the customer agencies.	For a selection of customer agencies and semi-annual instances, inspected the corresponding USA Staffing Onboarding semi-annual account recertifications and user access list to determine whether the lists were provided to Customer Agencies for review and changes provided by the Customer Agencies were applied. For a selection of TCSC semi-annual USA Staffing Onboarding user recertification instances,	No exceptions noted.

		inspected the corresponding reviews and system-generated user access list to determine whether the HR Systems Help Desk completed the user recertification and modifications were made as needed.	
18.58	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 removed USA Staffing Onboarding users, inspected the corresponding email requests and USA Staffing Onboarding Account records to determine whether the removal of access was documented and performed.	The following exception was noted: TCSC management was unable to provide a complete and accurate population of USA Staffing terminated accounts for the audit period of July 1, 2025, to June 30, 2026. As a result, we were unable to conclude on the operating effectiveness of this control.
Management's Response Management concurs with the exception and will initiate appropriate corrective actions.			
oneARC			
18.59	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.
18.60	New oneARC users must complete, sign, and submit an approved 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	For a selection of new oneARC users, inspected the corresponding System Access Forms for End User Application to determine whether access was documented, employees acknowledged that they understood the Privacy Act requirements, access	No exceptions noted.

	security requirements and will comply with computer security requirements established by the Bureau of the Fiscal Service and CFM. The form defines the user's access specifications, which will allow the user to perform his/her duties in oneARC.	was approved, and access was configured as authorized.	
18.61	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. 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 email, Self-Service authorization, or FS Form 5409 to determine whether updates to access rights were authorized and access was configured as authorized.	No exceptions noted.
18.62	To remove a 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 and access request forms, email request, or Self-Service Authorization to determine whether termination of oneARC access was completed and access was removed.	No exceptions noted.
18.63	oneARC load sheets are prepared from lists provided from the accounting area. Customer agencies or internal management then do a	For a selection of recertified users, inspected the corresponding oneARC user access reviews to determine if review of user access was performed	No exceptions noted.

	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.	and any users not on the list completed a System Access Form.	
18.64	oneARC authorization officials cannot approve their own access (so each agency has a minimum of two authorization officials).	Inspected evidence of a oneARC authorization official attempt to approve their own access to determine if the system prevented the user from approving their own access.	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 policies and procedures.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
Oracle, OBI, and PRSIM			
19.01	CFM 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. FSID staff develop customizations in a separate development instance. CSD staff test changes by running test scripts and analyzing the results in a separate test environment. Upon successful completion of testing, CSD 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, CFM requires verbal approval from a designated on-call manager (for all production instances). CFM application administrators document the emergency change in My Oracle Support on the next business day.	For a selection of emergency changes processed in My Oracle Support for Oracle and PRISM, inspected the corresponding ESM/ServiceNow tickets to determine whether the emergency changes were approved by a CFM Oracle or PRISM application administrator in My Oracle Support the next business day.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
		GovTA	
19.03	When a new GovTA release is received from UKG, TCSC 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 OCIO. The new GovTA release is not applied to production until it has been successfully tested and then approved by the HRSD Director.	For a selection of GovTA changes, inspected the corresponding change management records to determine whether changes were tested in a separate non-production environment using testing scripts and were only released to production by authorized GovTA applications administrators after successful testing and appropriate approvals were obtained.	No exceptions noted.
		OneStream XF	
19.04	When a new OneStream XF release is received, OneStream Support provides notification to CFM 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. CFM and FSID test the new release in a separate test environment by running test scripts and analyzing the results. CFM 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	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
	developed in a separate development environment with staff from CFM, FSID, and ARAD running test scripts and analyzing the results. Upon successful completion of testing, CFM 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.		
		RPA	
19.05	Changes to RPAs are initiated by a Change Request Form submitted by the business area responsible for the process (Process Owner). Automation Platform Configuration & Management Branch (APCMB) 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. Changes requiring a Security Impact Analysis (to include those that leverage existing Enterprise SIA's) are submitted to the security program and Policy and Risk Management Branch (PRMB) within the OCIO for analysis. SIA's must be submitted by the ISSO or are routed to the ISSO	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. If the change could have a security impact or create a new business process, inspect the corresponding change management records to determine whether the RPAs were approved prior to production implementation.	No exceptions noted.

Control #	Description of Controls	Testing Performed by KPMG LLP	Results of Tests
	for approval prior to being submitted for analysis by PRMB. Upon completion (implementation) of the SIA, the security posture must be evaluated in accordance with the SIA, which is either a self or 3rd party assessment. The results are then recorded in the Bureau's Governance, Risk and Compliance platform (ServiceNow GRC). Once the IV form is signed by both the ISSO and System Owner, a non-developer resource within the APCMB uploads the bot code to the production Management Console, schedules the RPA, and closes the JIRA ticket.		
oneARC			
19.06	Once the developer completes the initial development, the change is tested in the non-production region of oneARC. 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 DevForce ticket is then closed.	For a selection of oneARC workflow changes, inspected the corresponding change documentation to determine whether the changes were tested in a non-production environment and approved prior to being implemented to production.	No exceptions noted.

V. OTHER INFORMATION PROVIDED BY THE MANAGEMENT OF BUREAU OF THE FISCAL SERVICE CENTER FOR FINANCIAL MANAGEMENT AND TREASURY COMMON SERVICES CENTER

Continuity of Operations

If the main building becomes inoperable, network operations will be transferred to the Kansas City Data Center facility in alignment with the OCIO data center's Disaster Recovery Plan (DRP). This facility utilizes a "warm site" strategy to ensure operational recovery. Meanwhile, the Bureau of the 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 OCIO personnel, Fiscal Agents, Financial Agents, and contractor support teams.

As part of the CFM Business Continuity Plan (BCP), should CFM facilities become unavailable, essential CFM 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 CFM, ensuring that all essential functions continue smoothly with CFM employees' support. Disaster recovery testing is conducted annually in coordination with the Bureau of the Fiscal Service's OCIO 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 the Bureau of the Fiscal Service's access to the moveLINQ system within the MHS environment, as well as the availability of support tools hosted at the Bureau of the 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/