Audit Report

OIG-23-019

FINANCIAL MANAGEMENT

Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2022 and 2021

December 21, 2022

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

December 21, 2022

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

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

SUBJECT: Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2022 and 2021

We hereby transmit the attached subject report. Under a contract monitored by our office, KPMG LLP (KPMG), a certified independent public accounting firm, audited the consolidated financial statements of the Department of the Treasury as of September 30, 2022 and 2021, and for the years then ended. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, Office of Management and Budget Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements,* and the Government Accountability Office/Council of the Inspectors General on Integrity and Efficiency, *Financial Audit Manual*.

As part of its audit, KPMG issued its independent auditors' report that contained a significant deficiency in internal control over cash management systems and the related noncompliance with Federal Financial Management Improvement Act of 1996 related to Federal financial management systems requirements at the Bureau of the Fiscal Service.[1] KPMG also issued the accompanying management report to provide additional details and recommendations pertaining to this significant deficiency.

In connection with the contract, we reviewed KPMG's management report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with U.S. generally accepted government auditing standards, was not intended to enable us to express, and we do not express, a conclusion about the effectiveness of internal control. KPMG is responsible for the attached management report dated November 15, 2022, and

[1] KPMG's opinion on the fair presentation of Treasury's consolidated financial statements, and its reports on internal control over financial reporting, and compliance and other matters were transmitted in a separate report (OIG-23-007; issued November 15, 2022).

the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply, in all material respects, with U.S. generally accepted government auditing standards.

If you wish to discuss this report, please contact me at (202) 927-5329, or a member of your staff may contact Mark S. Levitt, Audit Manager, Financial Statement Audits, at (202) 927-5076.

Attachment

cc: Anna Canfield Roth
Acting Assistant Secretary for Management

David Lebryk
Fiscal Assistant Secretary

Carole Y. Banks
Deputy Chief Financial Officer

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

November 15, 2022

Mr. Richard K. Delmar
Deputy Inspector General
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Ms. Anna Canfield Roth
Acting Assistant Secretary for Management
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

In planning and performing our audit of the consolidated financial statements of the Department of the Treasury (the "Department" or "Treasury") as of and for the year ended September 30, 2022, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with the Office of Management and Budget (OMB) Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*, we considered the Department's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our auditors' report dated November 15, 2022 on our consideration, and the consideration of the other auditors, which are reported separately by those other auditors, of the Department's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be material weaknesses or significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. During our audit, we identified certain deficiencies in internal control that we consider to be significant deficiencies. One of the significant deficiencies included in our auditors' report dated November 15, 2022 is as follows:

Significant Deficiency in Internal Control over Cash Management Systems at the Bureau of the Fiscal Service

Effective information system controls and security programs over financial systems are essential to protecting information resources in accordance with OMB Circular No. A-130, *Managing Information as a Strategic Resource.* The Bureau of the Fiscal Service (Fiscal Service) relies on many information systems to manage government-wide cash.

While Fiscal Service remediated several control deficiencies identified in prior audits, Fiscal Service had partially unresolved control deficiencies primarily related to its general information technology controls over the government-wide cash management systems as follows:

Fiscal Service had not fully implemented remediation relative to corrective action plans and, in situations where Fiscal Service accepted associated risks, did not initially design and implement compensating controls to reduce such risks to an acceptable level. The unresolved control deficiencies did not provide reasonable assurance that: (1) the concept of least privilege is employed to prevent significant security exposures; (2) accounts were reviewed for compliance with account management requirements and that access to systems is protected against unauthorized modification, loss, or disclosure; (3) security events are logged, monitored, investigated and resolved; (4) baseline policies and procedures for security configuration controls were adequately documented and fully implemented for all platforms; (5) a complete and accurate inventory of information system components is maintained; and (6) incompatible duties are separated effectively so that users cannot control entire processes. Fiscal Service continues to prioritize the remediation of unresolved control deficiencies and until these control deficiencies are fully addressed, there is an increased risk of inadequate security controls in financial systems; unauthorized access to, modification of, or disclosure of sensitive financial data and programs; and unauthorized changes to financial systems.

Recommendation:

We recommend that the Acting Assistant Secretary for Management (Acting ASM) and Deputy Chief Financial Officer (DCFO) ensure that Fiscal Service implements corrective actions to resolve control deficiencies over its cash management systems.

This management report presents additional details and recommendations for corrective actions related to the Fiscal Service Cash Management Information Systems deficiencies in internal control noted within the above significant deficiency.

In Fiscal Year (FY) 2022, we determined that Fiscal Service closed 10 findings from the prior year (5 from FY 2019 and 5 from FY 2020). However, we identified 6 Cash Management Information System findings from FY 2019 and 1 finding from FY 2020 that remain open. The status of the findings is further described in Appendix I and Appendix II.

The purpose of this management report is solely to describe the Fiscal Service Cash Management Information Systems deficiencies in internal control identified during our audit. Accordingly, this report is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Washington, DC

Appendix I

DEPARTMENT OF THE TREASURY

Cash Management Information Systems Control Deficiencies

The Bureau of Fiscal Service (Fiscal Service) and its service provider, the Federal Reserve System who has responsibility for managing the below-noted government-wide cash (GWC) and Treasury managed accounts (TMA) systems, did not have newly identified FY 2022 control deficiencies.

Fiscal Service management implemented corrective actions to remediate 5 of 11 FY 2019 and 5 of 6 FY 2020 findings related to the UNIX Mid-Tier environment: Payment Information Repository (PIR), Secure Payment System (SPS), and Judgment Fund Internet Claims System (JFICS); as well as Treasury's Mainframe. However, we determined that 6 of 11 FY 2019 and 1 of 6 FY 2020 findings were unresolved and, as such, are still open as of September 30, 2022. The open findings related to the Treasury's Mainframe, which hosts Payment Claims and Enhanced Reconciliation (PACER) and Payment Automation Management (PAM), and the UNIX Mid-Tier, which hosts PIR, SPS, and JFICS (refer to notes section for descriptions of these systems). These prior-year (PY) findings were still open because management:

- Did not provide evidence to demonstrate full remediation and closure, or
- Did not complete all corrective action milestones within FY 2022.

We assessed Fiscal Service management's corrective action plans, closure packages, supplemental information system general control evidence, and, based on the results of our follow-up testing, we present the *Status of Prior-Year IT Deficiencies for Government-wide Cash and Treasury Managed Accounts* in a matrix that appears in Appendix II.

Appendix II

DEPARTMENT OF THE TREASURY

Status of Prior-Year IT Deficiencies for Government-wide Cash and Treasury Managed Accounts

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2022 Status**
FY 2019 – 1) Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources. (GWC and TMA)	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Address the mainframe operating system vulnerabilities noted in the condition as soon as possible. (FY 2019 recommendation #1)	Fiscal Service management is evaluating mainframe maintenance/improvement cost needed to address the PY deficiency and have determined that cost of system improvement outweighs the benefit. As such, since management is intending to transition off the mainframe environment, alternative corrective actions that will be more cost effective have been identified but are not expected to be implemented until fiscal year 2023. During the current year, OSSD/MD conducted research and corrected documentation over various existing supervisor calls (SVCs) as well as other SOPs such as the Base line Deviation Approval SOP.	Corrective actions for the deficiency are still in process for some recommendations as documented below. Based on this, we determined the deficiency to remain open. However, for these recommendations we performed limited testing at the policy level and determined these recommendations were closed based on the updated documentation received. a. 1.1.6.3 Baseline Deviation Approval Standard Operating Procedure (SOP) - This standard operating procedure outlines the process to prepare baseline deviations from the NIST approved checklists for submission to the Vulnerability Management Board (VMB) and the evaluation criteria used by the VMB voting members for approval/disapproval. b. 8.3.12.60 Mainframe Security Access Management Baseline - this document serves these purposes: • Details on Mainframe Security Configuration	Closed
Develop a tailored mainframe operating system security configuration baseline that specifies how security configuration options are to be set based on the selected industry guidance. (FY 2019 recommendation #2)			Closed
Ensure that the chief information security officer assigns specific responsibility for providing controls over operating system security, including access permissions to all system datasets and all security-related option settings. (FY 2019 recommendation #3)			Closed
Develop and document controls over changes and monitor update access to all key system datasets. (FY 2019 recommendation #4)			Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)			**FY 2022 Status**
FY 2019 – 1) Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources. (GWC and TMA)			***Open***
		Baseline for the production logical partition (LPAR).[1] • Provides a single point of reference for configuration settings for the z/OS operating system. • Assigns specific responsibility for providing controls over operating systems security. • Develops requirements and documents controls over changes and monitors update access to all key system data sets. • Develops requirements and documents controls to approve operating systems configurations.	
Develop and document controls and baseline documentation of mainframe operating system options specified in the configuration files. (FY 2019 recommendation #6)		Because Fiscal Service management has not completed its Plan of Action and Milestone (POA&M) for the last remaining LPAR, it has not fully implemented its corrective actions to remediate this deficiency during the FY 2022 audit period.	Open
Establish which techniques are to be used to control update access to key system datasets and to control read access to		Fiscal Service Management has accepted the risks associated with these FY 2019 deficiencies over unauthorized access to the mainframe and did not identify	Open

[1] A logical partition (LPAR) is the division of the mainframe's processors, memory, and storage into multiple sets of resources so that each set of resources can be operated independently with its own operating system instance and application

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 1) Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources. (GWC and TMA)	***Open***

sensitive system datasets (such as the security software database and the page files), whether a third-party tool is to be used, or tailored change control mechanisms, and develop procedures and documentation to support their use. (FY 2019 recommendation #7)		and/or provide compensating controls to reduce the risk of unauthorized access to and modification of mainframe computing resources and payment and production data.	
Develop procedures to provide assurance that programs installed with the privileges of the operating system (whether purchased from software vendors or internally developed) do not introduce security weaknesses. (FY 2019 recommendation #9)		Fiscal Service Management has accepted the risks associated with these FY 2019 deficiencies over unauthorized access to the mainframe and did not identify and/or provide compensating controls to reduce the risk of unauthorized access to and modification of mainframe computing resources and payment and production data.	Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	FY 2022 Status
FY 2019 – 2) Mainframe security software configuration baseline settings have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual mainframe security software settings against the security baseline. (FY 2019 recommendation #10)	Fiscal Service management is evaluating mainframe maintenance/improvement cost needed to address the PY deficiency and have determined that cost of system improvement outweighs the benefit. As such, since management is intending to transition off the mainframe environment, alternative corrective actions that will be more cost effective have been identified but are not expected to be implemented until fiscal year 2023. However, for some recommendations, in the current year Fiscal Service did update policies and procedures to include evidencing an annual comparison to the baseline through various SOPs (8.3.6.35, FITMF MVS Configuration Baseline, 12.6.1.1, and 8.3.4.16) to expand upon roles and responsibilities as well as to document the annual comparison.	Corrective actions for the deficiency are still in process for some recommendations as documented below. Based on this, we determined the deficiency to remain open. However, for these recommendations we performed limited testing at the policy level and determined these recommendations were closed based on the updated documentation received. Specifically, we reviewed the STIG results provided by Fiscal Service, as well as reviewed the following updated policies and procedures to determine certain recommendations as having been closed: a. SVC policies b. 1.1.6.3 Base line Deviation Approval SO c. 8.3.4.16 OSD Baseline Management d. 8.3.6.35 z/OS Combined ACF2 and TSS Baselines e. FITMF MVS Configuration Baseline f. 8.3.12.5 Fiscal Service ACF2-TSS Baseline g. 8.3.12.60 Mainframe Security Access Management Baseline. h. 8.3.12.61 Mainframe Security – Top Secret Security (TSS)	Closed
Develop a mainframe security software risk assessment process using the DISA STIG as a guideline. (FY 2019 recommendation #11)	Fiscal Service Management updated Fiscal Service mainframe security software policies and procedures for performing Mainframe security software risk assessments and updated configuration baseline derived from DISA Security Technical Implementation Guides (STIGs).		Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	FY 2022 Status
FY 2019 – 2) Mainframe security software configuration baseline settings have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop a tailored mainframe security software configuration baseline that specifies how security configuration options should be set based on the industry guidance. As part of this action, management should develop and document a baseline specifying for each possible setting in the security software control file how the option should be set and who is responsible for approving the setting. (updated FY 2019 recommendation #12)	Updated Fiscal Service Mainframe security software policies, procedures, and baseline documentation.	Access Management Baseline (AMB) which: • Details the Access Management Baseline for all LPARS using CA TSS. TSS uses the Command Propagation Facility (CPF) facility. • Assigns specific responsibility for providing controls over operating system security, including access permissions to all system data sets and all security-related option settings. • Develops requirements and documents controls over changes and monitors update access to all key system data sets. • Develops requirements and documents controls to prevent unauthorized, unnecessary access to system data sets containing sensitive information. • Develops requirements and documents controls and baseline documentation of TSS options • Assists the data owner during recertification • Develops requirements and documents controls for roles and other critical processes	Open
Use the mainframe security software configuration baseline to harden the mainframe environment, including the PAM and PACER production. (FY 2019 recommendation #13)	Mainframe security software risk assessment was performed and corresponding POA&Ms created for non-compliance.		Open
Remove duplicate and excessive permissions in the mainframe security software database. (FY 2019 recommendation #14)	Mainframe security software risk assessment was performed and corresponding POA&Ms created for non-compliance. Policies and procedures for comparing actual mainframe security software settings to the configuration baseline were updated to the mainframe security software control file, and the Fiscal Service configuration baseline was compared to actual.		Open
Perform an annual comparison of each actual setting in the mainframe security software control file to each setting specified in the baseline to verify compliance with the baseline. (FY 2019 recommendation #15)			Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 2) Mainframe security software configuration baseline settings have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop and document procedures for controlling updates to the mainframe security software control file. (FY 2019 recommendation #16)	Policies and procedures for comparing actual Mainframe security software settings to the configuration baseline and for controlling updates to the Mainframe security software control file, and the Fiscal Service configuration baseline was compared to actual.	on the mainframe that will be logged and reviewed.	Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 3) Excessive privileged access that violates the principle of least privilege is allowed on the Mainframe.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Define and document the segregation of functions and privileges based on the principle of least privilege for mainframe security software and operating system. (FY 2019 recommendation #17)	Fiscal Service management is evaluating mainframe maintenance/improvement cost needed to address the PY deficiency and have determined that cost of system improvement outweighs the benefit. As such, since management is intending to transition off the mainframe environment, alternative corrective actions that will be more cost effective have been identified, but are not expected to be implemented until fiscal year 2023.	Although we determined the PY deficiency is not planned to be remediated, we performed limited testing related to updated policy and procedures to determine management's progress in remediating this issue. We obtained and inspected the following documents: a. 1.1.6.3 Baseline Deviation Approval SOP. b. 8.3.12.60 Mainframe Security Access Management Baseline.	Open
Review and establish access permissions to the mainframe system and security software based on the principle of least privilege access. (FY 2019 recommendation #18)			Open
Review and re-assess each access permission in the mainframe security software dataset and resource rules on a periodic basis (FY 2019 recommendation #20)			Open
Develop procedures and documentation to establish the following for each dataset permission, resource permission, and mainframe security software privilege: a. Responsibility for approving access and enforcing compliance with the principle of least privilege; b. Actual access meets the principle of least privilege; c. Any discrepancy from approved access will be identified and corrected. (FY 2019 recommendation #21)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 4) Logging and monitoring controls for the Mainframe are not fully implemented to detect unauthorized activity. (GWC and TMA)	***Closed***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop, document and implement policies, procedures, and controls for comprehensive logging and monitoring of events. Procedures and controls should include an annual re-assessment of whether logging and reporting is adequate. (FY 2019 recommendation #22)	Fiscal Service management reviewed existing policies and standards, as well as internal SOPs and updated them during the current year as well as implemented new processes as part of these new policies, procedures and controls.	We performed limited testing at the policy level, reviewing updated policies and procedures and did not identify any further issues based on the below updated documentation received, and determined the recommendation was closed: a. 11.1.1.4 Log Management Policy b. 11.1.3.19 Information Logging Standard c. 11.1.3.20 Application Logging Standard d. 11.1.6.77 Mainframe Monitoring and Logging e. 8.3.12.60 FITMF MVS Access Management Baseline f. 8.3.12.61 TSS AMB g. CEM policy Sets h. 8.3.6.129 Mainframe Log and Audit Management i. 8.4.6.24 Network Operators Compliance (NOC) Procedures for Compliance Manager Alerts j. 9.0.3.5 MACB FITMF Access Management Standard k. 9.0.6.74 ISS Mainframe Access Management l. Reviewed sample alerts from CEM- Alert June/July	Closed
Review and determine which profiles, applications, databases, and other processes on the mainframe will be logged and reviewed. (FY 2019 recommendation #23)			Closed
Assess all mainframe logs to determine which logs should be evaluated by the incident management tool. (FY 2019 recommendation #24)			Closed
Establish appropriate alerts and event thresholds for those mainframe logs required to be evaluated by the external tracking tool. (FY 2019 recommendation #25)			Closed
Develop and implement data and analysis tools and processes for identifying event trends, patterns, spikes, and exceptions. (FY 2019 recommendation #26)			Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)
FY 2019 – 4) Logging and monitoring controls for the Mainframe are not fully implemented to detect unauthorized activity. (GWC and TMA)

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Identify non-security related purposes for logging and monitoring (including performance tuning, problem management, capacity planning, management of service level agreements); assign responsibility for addressing them and for integrating them with security uses of logging and monitoring. (FY 2019 recommendation # 27)		as well as the TSS access failures trend analysis. m. We reviewed 11.1.1.4 Log Management Policy and 11.1.3.19 Information Logging Standard and noted both provide guidance and establish responsibility for audit logs.	Closed
Identify the possible sources of log information; determine how each is to be used for security monitoring; and develop procedures to ensure that each type of logging which is necessary for effective security monitoring is activated. (FY 2019 recommendation #28)			Closed
Annually assess the effectiveness of security logging and monitoring, ensuring that the volume of logged events is limited to just those that are needed for security, and ensuring that monitoring results include effective identification and response for any violations and for any significant trends (such as an increase in the number of password resets for a given group of users or repetition of the same attempted but failed attempt to access a productions dataset or resource). (FY 2019 recommendation #29).			Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	FY 2022 Status
FY 2019 Finding– 5) Mainframe security control documentation needs improvement. (GWC and TMA)	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Identify, document, and assess the mainframe security controls affecting the system software, to fully describe how mainframe security is provided. These Fiscal Service management controls should include: 1. Specific assignment of responsibility for maintaining operating security, 2. Skill assessment and remediation for operating system security maintenance, 3. Baseline documents for mainframe configuration files, 4. Standard procedures for review and maintenance of operating system security, and 5. Standard procedures to compare actual configuration settings to baseline documents. (FY 2019 recommendation #30)	Fiscal Service management is evaluating mainframe maintenance/improvement cost needed to address the PY deficiency and have determined that cost of system improvement outweighs the benefit. As such, since management is intending to transition off the mainframe environment, alternative corrective actions that will be more cost effective have been identified. During FY 2022, OSSD/MB researched and corrected documentation of controls through various updates to SOPs and additional documentation.	We performed limited testing at the policy level and did not identify any further issues based on the below updated documentation received, and determined two of the three recommendations were closed: n. SVC Analysis o. z/OS MVS Diagnosis p. 11.0.1.2 – Access Management Policy q. 8.3.6.35 z/OS Combined ACF2 and TSS Baselines. r. 1.1.6.3 Base line Deviation Approval SOP s. 8.3.12.5 Fiscal Service ACF2-TSS Baseline t. FITMF MVS Configuration Baseline u. 9.0.3.5 MACB FITMF Access Management Standard Although Fiscal Service management has significantly updated their policies, procedures, and other remediation related documentation for this issue, we determined the overall deficiency has not been fully remediated and as such remains open. Specifically, as management is planning to transition from the mainframe environment by the end of calendar year 2025. As a result, this remaining recommendation and the deficiency remains open.	Closed

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	FY 2022 Status
FY 2019 Finding– 5) Mainframe security control documentation needs improvement. (GWC and TMA)	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Update mainframe documentation to be consistent with Fiscal Service and TD P 85-01 requirements. (FY 2019 recommendation #32)			Closed
Develop procedures and documentation to establish who is responsible and how effective security is achieved for controls. (FY 2019 recommendation #33)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 7) Lack of audit log policies and procedures for payment system production database and production UNIX servers and lack of database security audit log reviews.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Finalize policies and procedures to review audit logs of production IBM Database 2 (DB2) servers. (FY 2019 recommendation #37)	Fiscal Service management's corrective actions are planned to be implemented after FY 2022.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management has not 1) implemented its corrective actions and 2) verified and validated the design and implementation of the corrected control in FY 2022.	Open
Implement an oversight process to ensure that designated Fiscal Service personnel: a. Reviews the security logs for the UNIX and DB2 servers hosting the PIR, JFICS, and SPS applications on a pre-defined frequency, as indicated in the BLSR. b. Formally documents completion of their reviews and any escalations to the Information System Security Officer (ISS), and c. Retains the audit logs and documentation of its reviews for 18 months, as required by the BLSR. FY19 Rec #38			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 – 7) Lack of audit log policies and procedures for payment system production database and production UNIX servers and lack of database security audit log reviews.	***Open***

Periodically review Fiscal Service management's implementation and operation of the review the security audit logs for the UNIX and DB2 servers hosting the PIR, JFICS, and SPS applications to determine that Fiscal Service management completes the reviews on a pre-defined basis, documents completion of the reviews and escalations, and maintains such documentation. (FY 2019 recommendation #39)			Open
Establish an effective enforcement process or mechanism to ensure that (a) UNIX and DB2 events and monitoring controls are followed, and (b) Fiscal Service management has confidence it consistently reviews for potential unauthorized or inappropriate activity. (FY 2019 recommendation #40)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 Finding – 6) UNIX periodic user access review is still not consistently performed.	***Closed***
FY 2019 Finding – 8) Improvements are needed in controls over management's semi-annual review and recertification of PIR developers' access.	***Closed***
FY 2019 Finding – 9) Secure Payment System (SPS) periodic user access review needs improvement.	***Closed***
FY 2019 Finding – 12) PIR user termination control needs improvement.	***Closed***
FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.	***Open***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop and implement documentation to assign responsibility for ensuring adequacy of UNIX and database security and baseline settings. (FY 2019 Recommendation #62)	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2022.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management has not 1) implemented its corrective actions and 2) verified and validated the design and implementation of the corrected control in FY 2022.	Open
Update existing UNIX and database configuration security baseline documents to ensure that these documents fully incorporate and enforce the components of the DISA STIGs. Management should document any deviations from the STIGs, and note compensating controls that mitigate the security risk to an acceptable level. (FY 2019 Recommendation #63)			Open
Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual UNIX and database settings against the security configuration baselines. (FY 2019 Recommendation #64)			Open
Provide logging and monitoring of security related events to include the retention of evidence of reviews performed. (FY 2019 Recommendation #65)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding (continued)	**FY 2022 Status**
FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2022 Status
Develop a baseline of essential security settings and specify that baseline as the standard to be observed. (FY 2019 Recommendation #66)			Open
Implement corrective actions to address all vulnerabilities associated with the baseline enforcement to include removing the three default user accounts on UNIX servers. (FY 2019 Recommendation #67)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding – UNIX Mid-Tier systems	**FY 2022 Status**
FY 2020 Finding – 1) PIR periodic user review needs improvement	***Closed***
FY 2020 Finding – 3) PIR audit events review needs improvement	***Closed***
FY 2020 Finding – 4) Judgment Fund Internet Claims System (JFICS) monitoring inactive users' needs improvements.	***Closed***
FY 2020 Finding – 5) Information System Component Inventory Needs Improvement (UNIX Mid-Tier)	***Open, see below for details***
FY 2020 Finding – 6) UNIX Mid-Tier backups process needs improvement	***Closed***
FY 2020 Finding – 7) Vulnerability management needs improvement (UNIX Mid-Tier)	***Closed***

FY 2020 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2022 Status**
Perform a review of the current system environment against the CMDB. (FY 2020 recommendation #10)	Fiscal service is preparing a new service management platform called Enterprise Service Management (ESM) that will replace the existing IT service management platform. A new CMDB utilizing new data model will be established as a part of this effort. Additionally, Fiscal Service management's corrective actions are planned to be implemented after September 30, 2022.	We determined that the statuses of these recommendations are open based on our assessment that Fiscal Service management has not 1) implemented its corrective actions and 2) verified and validated the design and implementation of the corrected control in FY 2022.	Open
Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for monitoring and updating the CMDB. (FY 2020 recommendation #11)			Open
Update policy and procedures related to the above recommendations and disseminate the documentation to enforce such policy and procedures. (FY 2020 recommendation #12)			Open

LIST OF ABBREVIATIONS

Abbreviations	Definition
ASM	Assistant Secretary for Management
BLSR	Baseline Security Requirements
CARS	Central Accounting Reporting System
CMDB	Configuration Management Database
DB	Database
DB2	IBM Database 2
CFO	Chief Financial Officer
DISA	Defense Information Systems Agency
EFT	Electronic Funds Transfer
EITI	Enterprise Information Technology Infrastructure
EROC	East Rutherford Operations Center
Fiscal Service	Bureau of the Fiscal Service
FPA	Federal Program Agency
FRIT	Federal Reserve Information Technology
FY	Fiscal Year
GWC	Government-Wide Cash
IDAM	Identity and Access Management
ISS	Information Security Services
IT	Information Technology
JFICS	Judgment Fund Internet Claim System
LDAP	Lightweight Directory Access Protocol
LPAR	Logical Partition
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PACER On-line	Payments, Claims and Enhanced Reconciliation
PAM	Payment Automation Manager
PIR	Payment Information Repository
POA&M	Plan of Action and Milestones
PY	Prior Year
RBAC	Role Based Access Control
RFC	Regional Field Centers
SGL	Standard General Ledger
SOP	Standard Operating Procedures
SPS	Secure Payment System
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TMA	Treasury Managed Accounts
Department or Treasury	Department of the Treasury
TSS	Top Secret Security
TWAI	Treasury Web Application Infrastructure

Notes

PAM will disburse payments via Electronic Funds Transfer (EFT) and checks on behalf of Federal agencies in the Executive Branch, except for the Department of Defense and independent agencies.

PACER On-Line facilitates the daily processing of Claims, Cancellations and Accounting at Regional Field Centers (RFCs). PACER On-Line stores all payments generated by the RFCs and is the data warehouse for payment, claims, cancellations, and accounting data. PACER On-line is composed of two major subsystems: the Claims sub-system and the Accounting subsystem.

SPS is an automated system for payment schedule preparation and certification. The system provides positive identification of the certifying officer, who authorizes the voucher, and ensures the authenticity and certification of data. The SPS application provides a mechanism by which government agencies can create payment schedules in a secure fashion.

TWAI is an environment that houses Treasury Web applications, including TCIS and Central Accounting Reporting System (CARS), and is hosted and operated by the Federal Reserve's Federal Reserve Information Technology (FRIT) group. TWAI production sites are located at the Federal Reserve Bank (Federal Reserve System) of Dallas, TX, and the Federal Reserve System of East Rutherford Operations Center (EROC) in East Rutherford, NJ. TWAI manages the infrastructure (database and operating system).

PIR is a centralized information repository for Federal payment transactions.

UNIX operating system is included in the EITI boundary, also PIR application resides within the UNIX. Therefore, the EITI SSP is also applicable to UNIX and PIR.

LDAP is a client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

Oracle is a summary level general ledger accounting system and the system of record for the components listed above. Oracle uses a two-tier web-based infrastructure with a front-end Internet user interface and a database on the secure network. Oracle produces the TIER file for Treasury's financial statements, which shows the US Standard General Ledger (SGL) balances. Oracle also produces the SF-224, Statement of Transactions, as necessary.

Oracle Financials sets up each agency/operating unit as its own ledger. GWC and SGF transactions are under the GWC ledger. TMA is set up with its own TMA ledger. User access is set up using role-based access control (RBAC), thereby a user must be assigned a GWC/SGF role to access GWC data, and to access TMA data a user must be assigned a TMA role

An IDAM software is used to manage user access across IT environments, by using roles, accounts, and access permissions. It helps automate the creation, modification, and termination of user privileges throughout the entire user lifecycle.

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/