Audit Report

OIG-22-026

FINANCIAL MANAGEMENT

Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2021 and 2020

December 22, 2021

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D. C. 20220

OFFICE OF
INSPECTOR GENERAL

December 22, 2021

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

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

SUBJECT: Management Report for the Audit of the Department of the Treasury’s Consolidated Financial Statements for Fiscal Years 2021 and 2020

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, 2021 and 2020, 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. 21-04, *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 information systems and the related noncompliance with FFMIA's Federal financial management systems requirements at the Bureau of the Fiscal Service.[1] KPMG also issued the accompanying management report to provide the specific findings 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, 2021, 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-22-012; issued November 15, 2021).

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: J. Trevor Norris
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, 2021

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

Mr. J. Trevor Norris
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, 2021, 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. 21-04, *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, 2021 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.

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, 2021 is as follows:

Significant Deficiency in Internal Control over Information 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 Office of Management and Budget (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 and the federal debt. Although Fiscal Service made progress in addressing prior year deficiencies, Fiscal Service did not consistently implement adequate controls over the government-wide cash and the federal debt information systems and controls did not operate effectively as follows:

1. Cash Management Information Systems

Fiscal Service had not fully implemented remediation relative to corrective action plans and, in situations where Fiscal Service accepted associated risks, did not 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) separated user accounts are disabled and removed in a timely manner; (4) security events are logged and monitored, and potential vulnerabilities are investigated and resolved; (5) vulnerabilities identified by management were addressed timely; (6) inactive application user accounts are monitored and removed timely; (7) application backups are configured by management in accordance with policy; (8) baseline policies and procedures for security configuration controls, including audit logging controls, were adequately documented and fully implemented for all platforms; (9) a complete and accurate inventory of information system components is maintained; and (10) 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.

2. Federal Debt Information Systems

Fiscal Service continued to have information system general control deficiencies—primarily unresolved control deficiencies from prior audits—related to its federal debt information systems. These control deficiencies relate to information system general controls in the areas of security management, access controls and configuration management. Fiscal Service made some progress by strengthening segregation of duties controls over certain administrator accounts and took steps toward remediating other previously reported control deficiencies. However, Fiscal Service continued to have deficiencies where known information system vulnerabilities and deviations from baseline security requirements were not remediated on a timely basis. Additionally, Fiscal Service's controls for an information system did not properly restrict access to individuals requiring access and documentation describing the security architecture of the system needs improvement. Further, control deficiencies within Fiscal Service's change management process continue to exist.

Recommendation:

We recommend that the Acting Assistant Secretary for Management (Acting ASM) and Acting Chief Financial Officer (Acting CFO) ensure that Fiscal Service implements corrective actions to resolve control deficiencies over its cash management and debt information 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. A management report with additional details and recommendations for corrective actions on the Fiscal Service Debt Management Systems control deficiencies noted above will be provided separately to Fiscal Service management.

In Fiscal Year (FY) 2021, we determined that Fiscal Service closed 5 findings from the prior year (3 from FY 2019 and 2 from FY 2020). However, we identified 11 Cash Management Information System deficiencies from FY 2019 and 6 deficiencies from FY 2020 that remain open. The status of the deficiencies are 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

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 2021 control deficiencies.

Fiscal Service management implemented corrective actions to remediate 3 of 14 FY 2019 and 2 of 8 FY 2020 deficiencies related to the Treasury's UNIX Mid-Tier environment, Payment Information Repository (PIR), Secure Payment System (SPS), Judgement Fund Internet Claims System (JFICS) and the Treasury Web Application Infrastructure (TWAI). However, we determined that 11 of 14 FY 2019 and 6 of 8 FY 2020 deficiencies were unresolved and, as such, are still open as of September 30, 2021. 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 Appendix II for descriptions of these systems). These prior-year (PY) deficiencies 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 2021.

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.

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 2021 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 2021 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.	Corrective actions for the deficiency are still in process. Based on this, we determined the deficiency to remain open. We performed limited testing at the policy level and did not identify any further issues based on the below 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 Baseline for the production logical partition (LPAR).[1]	Open
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)			Open
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)			Open

[1] 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	FY 2021 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 2021 Status
Develop and document controls over changes and monitor update access to all key system datasets. (FY 2019 recommendation #4)		• 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.	Open
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 2021 audit period.	Open
Establish which techniques are to be used to control update access to key system datasets and to control read access to 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)		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	FY 2021 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 2021 Status
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	**FY 2021 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 2021 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.	We performed limited testing at the policy level and did not identify any further issues based on the below updated documentation received. a. 8.3.12.60 Mainframe Security Access Management Baseline. See deficiency 2019-01 b. 8.3.12.61 Mainframe Security – Top Secret Security (TSS) Access Management Baseline – • 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.	Open
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	**FY 2021 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 2021 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.	• 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 on the mainframe that will be logged and reviewed	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		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)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	FY 2021 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 2021 Status
	configuration baseline was compared to actual.		
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.		Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 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 2021 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. See deficiency 2019-01. b. 8.3.12.60 Mainframe Security Access Management Baseline. See deficiency 2019-01.	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	FY 2021 Status
FY 2019 – 4) Logging and monitoring controls for the Mainframe are not fully implemented to detect unauthorized activity. (GWC and TMA)	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 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 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.	We determined that as Fiscal Service has not formally documented the corrective action plan, this finding will remain open for the FY 2021 audit.	Open
Review and determine which profiles, applications, databases, and other processes on the mainframe will be logged and reviewed. (FY 2019 recommendation #23)			Open
Assess all mainframe logs to determine which logs should be evaluated by the incident management tool. (FY 2019 recommendation #24)			Open
Establish appropriate alerts and event thresholds for those mainframe logs required to be evaluated by the external tracking tool. (FY 2019 recommendation #25)			Open
Develop and implement data and analysis tools and processes for identifying event trends, patterns, spikes, and exceptions. (FY 2019 recommendation #26)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding
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 2021 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)			Open
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)			Open
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).			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	FY 2021 Status
FY 2018 Finding Open in FY 2019 – 5) Mainframe security control documentation needs improvement. (GWC and TMA)	***Open***

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 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, but are not expected to be implemented until fiscal year 2023.	We performed limited testing at the policy level and did not identify any further issues based on the below updated documentation received. a. 8.3.12.60 Mainframe Security Access Management Baseline. See deficiency-2019-01 b. 8.3.6.31 Mainframe Operating System Integrity - This internal standard provides an auditable procedure for maintaining and reviewing various aspects of mainframe operating system integrity. c. 8.3.6.48 Audit System Testing - This Information Security Services (ISS) Internal SOP establishes the process for the random testing of the audit system. d. 8.3.6.94 Mainframe Baseline Audit Reports - This ISS Internal SOP provides guidance for reviewing reports related to mainframe baseline configuration. The monitoring of report(s) is to ensure that the approved Fiscal Service mainframe configuration has not been altered. Although Fiscal Service management has significantly updated their policies, procedures, and other remediation related documentation for this issue, we determined the 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 2025.	Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding
FY 2018 Finding Open in FY 2019 – 5) Mainframe security control documentation needs improvement. (GWC and TMA)

FY 2019 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 Status
Update mainframe documentation to be consistent with Fiscal Service and TD P 85-01 requirements. (FY 2019 recommendation #32)			Open
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	**FY 2021 Status**
FY 2018 Finding Open in FY 2019 – 6) UNIX periodic user access review is still not consistently performed.	***Open***

FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Implement an oversight process to determine that designated Fiscal Service personnel reviews and reevaluates privileges associated with the UNIX production environment semi-annually for privileged accounts. (FY 2019 recommendation #34)	Fiscal Service management is looking to implement a new Enterprise Service Management (ESM) Configuration Management Database (CMDB) by ServiceNow to better automate and document the review and recertification process, increasing both accuracy and timeliness. To ensure no users or servers are missed in the review, a second and third review of servers identified, plus verification through Excel macros against a master list is being performed. Additionally, management will require all reviewers to document their review of users and attach an Excel file when responding to record their completion of the review. Furthermore, to ensure a timelier review, management has been moving the review process earlier into the calendar period to allow additional time for the process to be completed within the established timeframe.	As corrective actions are in process and under internal management review, this deficiency for FY 2021 audit remains open. Additionally, we performed a limited assessment over the one semi-annual review that was conducted; however, we determined that evidence demonstrating the period of review covered as well as evidence demonstrating Segregation of Duties were checked for accounts reviewed was not available. However, as the closure package was under internal review and we did not assess the completed closure package, this will be revisited in FY 2022 and/or during the audit period where the package is through internal management review.	Open
Configure the systems-management software agents to include all UNIX servers, databases, and users' accounts within the UNIX environment when generating the users' lists for the semi-annual review and recertification process so that all privileged and non-privileged users' access is reviewed. (FY 2019 recommendation #35)			Open
Update UNIX semi-annual account review and recertification procedures to include quality control steps to validate that systems-management software is generating complete and accurate account listings for all UNIX servers and databases privileged and non-privileged user accounts within the UNIX environment prior to completing the review and recertification process. (FY 2019 recommendation #36)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 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 2021 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 at the end of FY22. Specifically, management had approved the use of the SPLUNK audit log management tool and is in the process of obtaining licensing for using the tool moving forward. The new tool will impact the local environment along with the Unix and DB2 servers hosting both PIR and SPS applications. Funding for SPLUNK licensing was recently approved for initial steps to take effect October 2021, with implementation projected for the end of FY 2022.	We determined that the status 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 2021.	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	**FY 2021 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 2021 Status**
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	**FY 2021 Status**
FY 2019 Finding – 8) Improvements are needed in controls over management's semi-annual review and recertification of PIR developers' access.	***Open***

FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Update its current PIR security procedures to require that management obtain current PIR developer access requirement listings from the service provider and use them when validating the appropriateness of PIR developer access during the semi-annual access reviews and recertification of the PIR and UNIX environments. (FY 2019 recommendation #41)	Fiscal Service management is working to ensure the PIR team has processes in place to control developer access to the application and the production environment. We also noted communications between PIR management and the Federal Reserve Bank (FRB) and ISS developers will be retained, and a cadence will be formalized to ensure that developer access is reviewed twice per year. Additionally, management is anticipating the new process and procedures to be implemented by August 31, 2021.	We determined that corrective actions are in process and under internal management review. This deficiency for FY 2021 audit remains open. Additionally, we performed limited testing over the semi-annual evidence provided by management and noted that the accounts reviewed were a subset of PIR developers, thus not demonstrating access was appropriate for all accounts and were free of incompatible user access between the development, test, and production environments. Additionally, evidence provided did not demonstrate a review over any test environment accounts or production environments accounts.	Open
Maintain the documentation used to review and recertify the access of the known PIR service provider developers evidencing that their access to the UNIX environments is commensurate with their job functions and responsibilities. (FY 2019 recommendation #42)			Open
Ensure that developers do not have the ability to make changes to the PIR production environment. (FY 2019 recommendation #43)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2019 Finding – 9) Secure Payment System (SPS) periodic user access review needs improvement.	***Open***

FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Remove users' access once validated by the Federal Program Agency (FPA), during the SPS annual user access review. (FY 2019 Recommendation #44)	Fiscal Service management reviewed and updated the Annual User Access Review SOP to highlight documentation retention and the need to remove users in a timely manner. Additionally, as a part of the user access review process going forward, management will provide evidence of the following: 1) all users are reviewed, 2) only appropriate users are recertified and all others removed, and 3) management will oversee all aspects of the user review and that user access actions were taken within a reasonable timeframe after validation.	Although Fiscal Service management was able to provide a closure package related to the PY finding, we determined that evidence of the initial system-generated listing was not available to confirm all users reviewed and demonstrate all required changes were 1) made and 2) changes made timely during the FY 2021 SPS Recertification. Therefore, this finding will remain open.	Open
Retain evidence of recertification of all users. (FY 2019 Recommendation #45)			
Oversee the recertification process and ensure that access corrections are processed once received from the FPA. (FY 2019 Recommendation #46)			

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2019 Finding – 10) TWAI users' access recertification needs improvement.	***Closed***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2019 Finding – 12) PIR user termination control needs improvement.	***Open***

FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Remove and disable the two users' access accounts that were inactive for over 120 days, immediately. (FY 2019 Recommendation #53)	Fiscal Service management removed the two users identified as a part of the FY 2020 deficiency. Additionally, a quality control process was implemented to automatically generate email notifications about user inactivity. Rather than rely on a manual system, help desk support staff can rely on system-generated emails. PIR management also receives the system-generated email, they know to expect the confirmation that the activity has been completed.	We determined that the Corrective Action Closure Package (CAC) was submitted internally and not to us timely due to internal review. As such, the CAC will be assessed in future audit following internal management review and will then be made available to auditor. This deficiency will remain open accordingly.	Open
Implement a quality control process to ensure that PIR application accounts defined to the PIR production environment that have been inactive for over 120 days are disabled. (FY 2019 Recommendation #54)			

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2019 Finding – 13) Unix password control needs improvement.	***Closed***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2019 Finding – 16) Lack of approval for PIR emergency changes.	***Closed***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 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 2021 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, 2021.	We determined that the status 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 2021.	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	FY 2021 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 2021 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

Appendix II

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	FY 2021 Status
FY 2020– 1) PIR periodic user review needs improvement	***Open***

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 Status
Complete its periodic review of PIR user access within the annual timeframe in accordance with the PIR System Security Plan (SSP). (FY 2020 recommendation #1)	Fiscal Service management will work to complete the annual recertification in a timely manner going forward. Additionally, shared inboxes and carbon copy emails will be utilized to ensure backup support when key staff are on leave or consumed by higher priority activities.	Although the recertification was complete for FY 2021, a closure package was not provided to evidence full remediation and closure of this finding. Thus, this deficiency will be re-issued for FY 2021.	Open
Consider resource constraints and prioritize efforts to perform periodic reviews within the annual timeframe in accordance with the PIR SSP. (FY 2020 recommendation #2)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	FY 2021 Status
FY 2020 – 2) SPS and PIR activation and deactivation of user access need improvement	***Closed***

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 – 3) PIR audit events review needs improvement	***Open***

FY 2020 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Re-enforce established audit logging policy and procedures (FY 2020 recommendation #4)	Fiscal Service Management provided instruction to management and staff to reinforce importance of maintaining controls in accordance with established procedures and to escalate any issues related to resource constraints.	We determined that Fiscal Service Management has updated policies and procedures to include delegation and backup resources to support timely reviews of the SOP. However, from a random sample of 5 weeks of audit log reviews (January 23, 2021, March 13, 2021, May 01, 2021, June 12, 2021, and August 14, 2021), reviews for 2 logs were not conducted in a timely manner (i.e., weekly) in accordance with policies and procedures and the control as designed.	Closed
Retain evidence to demonstrate PIR auditable events are reviewed timely in accordance to policy and procedures. (FY 2020 recommendation #5)			Open
Consider resource constraints and prioritize efforts to perform timely audit logging reviews in accordance to policy and procedures (FY 2020 recommendation #6)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 Finding Open in FY 2021 – 4) Judgement Fund Internet Claims System (JFICS) monitoring inactive users' needs improvements.	***Open***

FY 2020 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2021 Status**
Review the population of JFICS accounts and disable application user access that has been inactive for greater than 120 days (FY 2020 recommendation #7)	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2021.	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 2021. Additionally, JFICS was not in scope for FY 2021, as such no further testing was conducted or reported within this period.	Open
Design and implement a control to disable JFICS application user accounts after 120 days of inactivity. (FY 2020 recommendation #8)			Open
Retain evidence to demonstrate that access is disabled in a timely manner in accordance with the above recommendations. (FY 2020 recommendation #9)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 Finding Open in FY 2021 – 5) Information System Component Inventory Needs Improvement (UNIX Mid-Tier)	***Open***

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 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, 2021.	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 2021.	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

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 Finding Open in FY 2021 – 6) UNIX Mid-Tier backups process needs improvement	***Open***

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 Status
Conduct a review of production servers to ensure backups are scheduled on all servers in accordance with established policies and procedures across the full fiscal year. (FY 2020 recommendation #13)	Fiscal service management conducted a full review of servers and configurations to identify issues from the FY20 deficiency. Additionally, procedures were implemented to validate that backups are scheduled for all servers based on the frequency defined in the System Security Plan (SSP).	As a part of the closure package, we were provided screenshot evidence of one SPS server that we determined demonstrated that the SPS server was configured to perform daily incremental backups, as well as demonstrated weekly backup results for the server via the 'NetBackUp' tool. However, as the closure package was under internal review and we did not assess completed closure package, this will be revisited in FY22 and/or during the audit period where the package has gone through internal management review.	Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 Finding Open in FY 2021 – 7) Vulnerability management needs improvement (UNIX Mid-Tier)	***Open***

FY 2020 Recommendations	Fiscal Service Corrective Action Taken	Determination of Action Taken	FY 2021 Status
Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for developing a POA&M or formal risk acceptance for vulnerabilities identified. (FY 2020 recommendation #14)	Fiscal Service management performed an assessment to determine the appropriate personnel for remediation, developing POA&Ms, or formal risk assessments for vulnerabilities identified. Additionally, Fiscal service will update procedures to ensure identified vulnerabilities are addressed accordingly.	Although Fiscal Service provided an example PIR vulnerability Database (DB) report and an operating system (OS) vulnerability report to demonstrate that vulnerability scans are being performed, management's corrective action closure package is under internal review and as such we were unable to review the specific corrective actions noted above, nor were we able to review the supporting plan of action and milestones for the vulnerability reports received. As such, we determined based on the above, this finding will remain open.	Open
Disseminate policy and procedures related to the use of a POA&M or formal risk acceptance to the appropriate personnel determined. (FY 2020 recommendation #15)			Open

Deficiencies Included in the FY 2020 Fiscal Service IT Management Report Finding	**FY 2021 Status**
FY 2020 Finding Open in FY 2021 – 8) UNIX Mid-Tier Contingency Plan needs improvement	***Closed***

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.

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/