Audit Report

OIG-21-021

FINANCIAL MANAGEMENT

Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2020 and 2019

February 2, 2021

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

February 2, 2021

MEMORANDUM FOR MATTHEW J. MILLER, ACTING COMMISSIONER
BUREAU OF THE FISCAL SERVICE

FROM: James Hodge /s/
Director, Financial Audit

SUBJECT: Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2020 and 2019

We hereby transmit the attached subject report. We contracted with the certified independent public accounting firm of KPMG LLP (KPMG) to audit the consolidated financial statements of the Department of the Treasury as of September 30, 2020 and 2019, and for the years then ended, to provide a report on internal control over financial reporting, to report instances in which Treasury's financial management systems did not substantially comply with the requirements of the Federal Financial Management Improvement Act of 1996 (FFMIA), and to report any reportable noncompliance with laws, regulations, contracts, and grant agreements tested. The contract required that the audit be performed in accordance with U.S. generally accepted government auditing standards, and Office of Management and Budget Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*.

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 December 30, 2020, 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-21-019; issued December 30, 2020).

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) 927-0009, or a member of your staff may contact Mark S. Levitt, Audit Manager, Financial Audit, at (202) 927-5076.

Attachment

cc: Trevor Norris
Acting Assistant Secretary for Management

Timothy E. Gribben
Acting Fiscal Assistant Secretary

Carole Y. Banks
Acting Chief Financial Officer

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

December 30, 2020

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

Mr. 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) as of and for the year ended September 30, 2020, 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. 19-03, 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 December 30, 2020 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 December 30, 2020 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. Further, Fiscal Service had newly identified control deficiencies related to its general information technology controls over its cash management systems. The unresolved and newly identified 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) changes to systems are authorized, properly configured, and secured as intended; (6) vulnerabilities identified by management were addressed timely; (7) inactive application user accounts are monitored and removed timely; (8) application backups are configured by management in accordance with policy; and (9) baseline policies and procedures for contingency planning and security configuration controls, including password and audit logging controls, were adequately documented and fully implemented for all platforms. These deficiencies resulted because Fiscal Service did not effectively verify and validate that its corrective actions remediated control deficiencies; identify and effectively confirm that the controls were properly designed, implemented, and operating effectively; identify all risks and implement controls to address such risks; establish clear responsibilities in its information technology plans, policies, and procedures; identify and evaluate sufficient compensating controls to reduce the risk of unauthorized access for instances where management accepted associated risks and focus sufficient resources to perform the controls for all platforms supporting financial systems. 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 control deficiencies—primarily unresolved control deficiencies from prior audits—related to its federal debt information systems. These continuing control deficiencies relate to information system general controls in the areas of security management, access controls, configuration management, and segregation of duties. Fiscal Service made progress toward improving its procedures to reasonably assure that (1) corrective action plans fully address information system control deficiencies and (2) new or enhanced controls established as part of the corrective actions fully resolve the control deficiencies. However, Fiscal Service continued to have instances in which the corrective actions taken by the responsible officials were not sufficient to address the control deficiencies or identify shortcomings. Specifically, Fiscal Service did not identify technical inaccuracies, inconsistencies between the documented policies and procedures, and significant control gaps in the information included in finding closure packages. Fiscal Service continued to have deficiencies where vulnerabilities and deviations from baseline security requirements were not remediated on a timely basis or adequately tracked for remediation. Additionally, Fiscal Service needs improvement in documentation describing the security architecture for the mainframe and continued to have instances in which mainframe security controls were not employed in accordance with the concept of least privilege.

Recommendation:

We recommend that the Assistant Secretary for Management (ASM) and Deputy Chief Financial Officer (DCFO) ensure that Fiscal Service implement 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.

We identified the following Fiscal Service Cash Management Information Systems control deficiencies that are further described along with recommendations in Appendix I:

1. Payment Information Repository (PIR) periodic user review needs improvement.
2. Secure Payment System (SPS) and PIR activation and deactivation of user access need improvement.
3. PIR audit events review needs improvement.
4. Judgment Fund Internet Claims System (JFICS) monitoring inactive users needs improvement.
5. Information system component inventory needs improvement.
6. UNIX Mid-Tier backups process needs improvement.
7. Vulnerability management needs improvement.
8. UNIX Mid-Tier contingency plan needs improvement.

In addition, fourteen findings from Fiscal Year (FY) 2019 remain open which are further described in 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 providers, the Federal Reserve System, manage the following government-wide cash (GWC) and Treasury managed accounts (TMA) systems that had control deficiencies:

1. Payment Automation Manager (PAM) System;[i]
2. Payments, Claims, and Enhanced Reconciliations (PACER) On-Line;[ii]
3. Secure Payment System (SPS);[iii]
4. Treasury Web Application Infrastructure (TWAI);[iv]
5. Payment Information Repository (PIR);[v]
6. Judgment Fund Internet Claims System (JFICS);[vi]
7. Mainframe environment; and
8. UNIX Mid-Tier environment.[vii]

The details of the control deficiencies are included below, which relate to GWC and TMA.

Fiscal Service management implemented corrective actions to remediate 3 of 17 FY 2019 findings related to Treasury's Oracle Financials, PIR, and SPS. However, we determined that 14 of 17 FY 2019 findings are still open as of September 30, 2020. These findings, described in appendix II, were still open because management:

- indicated in its corrective action plans that it accepted risk for some conditions but did not design and implement compensating controls to address the noted condition;
- implemented controls without consideration to the full FY and the impact to the design, implementation, and operating effectiveness of controls from October 1, 2019 to September 30, 2020; and/or
- did not complete all its corrective action milestones within FY 2020.

We assessed Fiscal Service management's closure packages and, based on the results of our follow-up testing, we present the *Status of Prior year IT Findings for Government-wide Cash and Treasury Managed Accounts* in a matrix that appears in Appendix II. Additionally, we identified new conditions in FY 2020 related to the following:

1) The FY 2020 PIR user access review was not conducted in a timely manner.

2) Fiscal Service management was unable to provide evidence to support access requests and removals for the period of October 1, 2019 to April 13, 2020.

3) For a sample of five PIR audit logs, Fiscal Service management was unable to provide evidence to support the timely review of five audit logs.

4) Fiscal Service management did not implement a control in JFICS to automatically disable application user access after a period of 120 days of inactivity.

5) Fiscal Service management did not update the Configuration Management Database (CMDB) to reflect all production servers across the UNIX Mid-Tier environment.

6) From October 1, 2019 to September 24, 2020, Fiscal Service management did not configure JFICS backups to be performed on an at least weekly basis.

7) For an identified vulnerability, Fiscal Service management did not document that it could not complete remediation within 90 days.

8) The Fiscal Service general support system contingency plan was not updated since January 15, 2017.

1) PIR periodic user review needs improvement. (GWC and TMA)

The PIR application is hosted by the UNIX Mid-Tier environment, which includes the production operating systems and databases that support this application. The PIR information technology (IT) System Owner and Resource Owners are responsible for performing an annual review of application user accounts. As a separate control, Information Security Services (ISS) management performs periodic reviews of administrative accounts established on the UNIX Mid-Tier operating systems and databases maintained in this environment.

In FY 2020, the annual review of PIR user access did not operate effectively. The PIR System Security Plan (SSP) Security Control Matrix (SCM) requires that users' access be reviewed periodically to validate that access is still needed and commensurate with job responsibilities on an annual basis. However, management did not conduct the FY 2020 periodic review within the annual timeframe, as the FY 2019 periodic review concluded on July 17, 2019, and a FY 2020 review was not concluded until September 17, 2020.

Security control AC-2 in the PIR SSP requires Fiscal Service management to perform periodic reviews, at least annually, of Fiscal Service user roles/accounts/profiles. This review includes:

- Verification of active and inactive accounts;
- Verification of business justification for multiple IDs for the same person;
- Change in user job functions;
- Compliance with least privilege and separation of duties principles;
- Coordinated review with management/data owners of access control lists; and
- Verification that accesses are removed or modified as a result of reassignments, promotions, terminations, or retirements of departing Fiscal Service employees, Federal Program Agency (FPA), fiscal agent and financial institution employees, contractors, and subcontractors.

Fiscal Service management stated that due to resource and time constraints attributable to priorities associated with the disbursement of economic impact payments for the Coronavirus Aid, Relief, and Economic Security (CARES) Act, the periodic review of PIR user access could not be completed within the annual timeframe.

Without performing a periodic review of users' access within a timely manner, users could retain unauthorized, excessive, and/or otherwise inappropriate access that could be used to alter the integrity and accuracy of the system and its data.

Recommendation:

We recommend that Fiscal Service management:

1. Complete its periodic review of PIR user access within the annual timeframe in accordance with the PIR SSP.

2. Address resource constraints and prioritize efforts to perform periodic reviews within the annual timeframe in accordance with the PIR SSP.

2) SPS and PIR activation and deactivation of user access need improvement. (GWC and TMA)

Fiscal Service management could not provide evidence for selections of 25 SPS and PIR access requests and 25 SPS access removals for the period of October 1, 2019 to April 13, 2020. Specifically, management could not provide supporting documentation relating to:

- The creation, activation, and management of SPS and PIR application users; and
- The removal of separated and/or transferred SPS application users.

In addition, due to the Coronavirus Disease 2019 (COVID-19) pandemic, Fiscal Service management developed an alternative electronic records management policy for maintaining relevant audit documentation to proactively address the above noted condition, which was finalized on July 13, 2020. Fiscal Service management provided a selected sample of one user access request form for both an SPS and PIR user, as well as evidence for a selected SPS user termination for the period of April 14, 2020 to September 30, 2020, to demonstrate the updated electronic records process was operating effectively.

Security control AC-2 in the Fiscal Service Baseline Security Requirements (BLSR) requires management to create, enable, modify, disable, and remove accounts in accordance with standard operating procedures (SOP).

Due to the COVID-19 pandemic, the Kansas City (KC) office was not accessible; thus, in FY 2020, management was unable to provide evidence of user access documentation physically maintained in the KC office until April 13, 2020, when management updated controls to support a remote environment.

Weaknesses related to the ability to readily generate and/or provide documentation evidencing the completion of PIR and SPS access controls for the period of October 1, 2019 to April 13, 2020, could inhibit Fiscal Service management's ability to properly manage, monitor and/or evaluate such processes to help ensure their ongoing effectiveness. Such activities could negatively affect the confidentiality, integrity, and availability of the PIR and SPS applications and its data.

Recommendation:

3. As Fiscal Service management has updated access controls to address the noted condition during the FY 2020 audit period, we are not including a formal recommendation.

3) PIR audit events review needs improvement. (GWC and TMA)

The PIR Security Log SOP requires that audit log reviews be performed and signed-off on a weekly basis. However, for 5 out of 5 selected PIR audit logs, management did not perform the audit log reviews on a weekly basis as directed by the SOP.

Due to a lack of management oversight, audit logs were not consistently reviewed in a timely manner.

Without proper review of auditable security events in accordance with established policy, the risk exists that unauthorized or inappropriate activity could occur in the PIR application without timely action by Fiscal Service management.

Recommendation:

We recommend that Fiscal Service management:

4. Re-enforce established audit logging policy and procedures.

5. Retain evidence to demonstrate PIR auditable events are reviewed on a weekly basis as required by the PIR Security Log SOP.

6. Consider resource constraints and prioritize efforts to perform timely audit logging reviews in accordance to policy and procedures.

4) JFICS monitoring inactive users needs improvement. (TMA)

JFICS SSP SCM requires that user accounts be automatically disabled after 120 days of inactivity. However, the control that the Fiscal Service management implemented did not disable application users' access after a period of 120 days of inactivity as required by SCM.

We were informed that JFICS management relied upon the Lightweight Directory Access Protocol (LDAP)[viii] inactivity control to remove accounts with inactivity greater than 120 days. However, JFICS management was not aware the LDAP control managed by ISS did not address user inactivity specific to JFICS application users.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 required management to create, enable, disable and remove information system accounts in accordance with organization-defined procedures or conditions.

Failure to disable inactive accounts within the JFICS environment in a timely manner, increases the risk of unauthorized access to and/or inappropriate activity in the application that may compromise the integrity of the information systems data.

Recommendation:

We recommend that Fiscal Service management:

7. Review the current population of JFICS accounts and disable application user access that has been inactive for greater than 120 days.

8. Design and implement a control to automatically disable JFICS application user accounts after 120 days of inactivity.

9. Retain evidence to demonstrate that access is disabled in a timely manner in accordance with JFICS SSP.

5) Information system component inventory was not complete and accurate. (GWC and TMA)

Fiscal Service management designed a control as documented in the Fiscal Service BLSR related to maintaining a complete and accurate inventory of information system components for agency monitoring of assets against system security risks. However, management did not update the CMDB to reflect all production servers across the UNIX Mid-Tier environment, which hosts the PIR, JFICS, and SPS applications. Specifically, three servers were not updated in the CMDB.

The Fiscal Service BLSR requires management to develop, document and review an inventory of information system components on an annual basis that:

- Accurately reflects the current information system;
- Includes all components within the authorization boundary of the information system;
- Is at the level of granularity deemed necessary for tracking and reporting; and
- Includes information deemed necessary to achieve effective information system component accountability but must include an inventory of basic input/output system (BIOS) information for workstations and laptops, to include BIOS characteristics such as manufacturer name, type, model, serial number, version or time stamp (allows organization to perform update, rollback, and recovery) and when applicable: physical location, software license information, information system/component owner, and for a networked component/device, the machine name and network address;
- Reviews and updates the information system component at least annually.

Due to human error attributable to resource constraints, management stated that CMDB administrators failed to monitor and update the CMDB to ensure that the inventory of information system components accurately reflected the UNIX Mid-Tier environment.

The lack of a complete inventory of servers, increases the risk that security controls could inadvertently or deliberately be omitted, or turned off, or that processing irregularities or unauthorized access to and modification of computing resources could be introduced, impacting the integrity of financial production data.

Recommendation:

We recommend that Fiscal Service management:

10. Perform a review of the current system environment against the CMDB to ensure that all information system components are inventoried.

11. Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for monitoring and updating the CMDB.

12. Update policy and procedures related to the above recommendations and disseminate the documentation to enforce such policy and procedures.

6) UNIX Mid-Tier backups process needs improvement. (GWC and TMA)

The Fiscal Service BLSR require backups of low and moderate risk level systems to be conducted on a weekly basis. Fiscal Service management has designated the JFICS application at the moderate risk level. For the period of October 1, 2019 to September 24, 2020, Fiscal Service management did not configure backups to be performed on an at least weekly basis for the UNIX Mid-Tier server that hosts the JFICS application.

Security control CP-9 in the Enterprise Information Technology Infrastructure (EITI) SSP requires Fiscal Service management to conduct backups of user-level information contained in the information system at least “daily” for high systems and at least “weekly” for low and moderate systems.

Management stated that it transitioned to a new process to perform backup of UNIX Mid-Tier production servers, however, due to a lack of management oversight, the backup team did not implement the control for a JFICS production server.

Without proper backups of UNIX production servers, the risk exists that Fiscal Service would be unable to resume critical operations if primary processing capabilities become unavailable.

Recommendation:

We recommend that Fiscal Service management:

13. Conduct a review of the UNIX Mid-Tier production servers to validate that backups are scheduled for all servers based on the frequency defined in the EITI SSP for the full fiscal year.

7) Vulnerability management needs improvement. (TMA)

Fiscal Service management designed a control as documented in the Vulnerability Management Plan (VMP) related to requirements for documenting a Plan of Action and Milestones (POA&M) for identified vulnerabilities. The VMP requires Fiscal Service management to remediate vulnerabilities according to a 90-day schedule and that all equipment and software not patched in accordance with policy shall be tracked in a POA&M. For a vulnerability identified on the February 2020 Historical Database (DB) Report related to vulnerability on a JFICS server, management completed its remediation of this vulnerability in excess of 90 days from when it was identified. However, management did not document a POA&M within 90 days in accordance with the VMP.

Fiscal Service management stated that due to 1) resource constraints and 2) not enforcing policy and procedures with control owners, management did not document a POA&M for vulnerabilities identified.

Weaknesses in vulnerability management, specific to the nonuse of a POA&M, increases the risk of being exposed to attacks on information systems and applications, unauthorized modification, or data being compromised.

Recommendation:

We recommend that Fiscal Service management:

14. Perform a risk assessment over the subject matter and determine the appropriate personnel to be responsible for developing POA&M or formal risk acceptance for vulnerabilities identified.

15. Disseminate policy and procedures related to the use of a POA&M or formal risk acceptance to the appropriate personnel determined above to enforce the respective vulnerability management requirements.

8) UNIX Mid-Tier contingency plan was not reviewed and updated. (GWC and TMA)

Fiscal Service's general support system EITI contingency plan includes the UNIX Mid-Tier environment, which hosts the PIR, JFICS, and SPS applications. The Fiscal Service BLSR and the EITI Security Control Matrix (SCM) require that contingency plan procedures be updated every three years or when there is a significant change. However, EITI management was unable to demonstrate that a review and/or update of the EITI Contingency Plan occurred within the three-year frequency, as the last approved update was on January 15, 2017.

Specifically, security controls CP-1 and CP-2 in the EITI SSP require that Fiscal Service management: 1) develop and approve a contingency plan for the information system; 2) review and approve the plan every three years or when there is significant change; and 3) update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing.

Management informed us that due to resource constraints caused by an organizational change, Fiscal Service management did not determine the point of contacts (POCs) responsible for EITI contingency plan reviews and updates.

Without an updated contingency plan, there is an increased risk that the Fiscal Service's ability to recover from a disaster is impaired.

Recommendation:

We recommend that Fiscal Service management:

16. Update the contingency plan at a minimum of every three years or after a major change, in accordance with BLSR and EITI SSP.

17. Assign responsible POCs to prioritize efforts to perform updates to the contingency plan every three years or when there is a significant change in accordance with the BLSR and EITI SSP.

Appendix II

Department of the Treasury

Status of Prior year IT Findings for Government-wide Cash and Treasury Managed Accounts

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
FY 2018 Finding Open in 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***
Address the mainframe operating system vulnerabilities noted in the condition as soon as possible. (FY 2019 recommendation #1)	Fiscal Service management updated mainframe security software baseline documentation with SVCs[1] and privilege programs. Further, management noted majority of the SVCs were dynamic.	Fiscal Service Management has documented the ISS mainframe Access Management Security Review and updated the Fiscal Service mainframe security software baseline document that considers mainframe security software hardening settings from the DISA STIG and that include risk categories and/or deviations from actual STIG settings. However, we determined that there were SVCs on the system that were not addressed in the baseline documentation. As such, the mainframe security software baseline appeared to be incomplete for us to determine that management has adequate protection against possibly unsecured SVCs.	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
Develop and document controls over changes and			Open

[1] In IBM mainframes, an SVC is a processor instruction that directs the processor to pass control of the computer to the operating system's supervisor program. Most SVCs are requests for a specific operating system service from an application program or another part of the operating system.

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
monitor update access to all key system datasets. (FY 2019 recommendation #4)			
Develop and document controls to prevent unauthorized, unnecessary read access to system datasets containing sensitive information. (FY 2019 recommendation #5)	Fiscal Service management has removed update access to in-scope financial datasets.	From inspection of records used by mainframe security software, we concluded that update access was removed from the in-scope financial datasets. As such, management's corrective actions taken addressed the prior year conditions.	Closed
Develop and document controls and baseline documentation of mainframe operating system options specified in the configuration files. (FY 2019 recommendation #6)	Fiscal Service management has appropriately corrected the Mainframe operating system configuration settings on 3 of 4 logical partitions (LPARs)[2] on the mainframe. Management has developed a POA&M to address the risk associated with one setting on the remaining LPAR.	Because Fiscal Service management has not completed its POA&M for last the remaining LPAR, it has not fully implemented its corrective actions to remediate this deficiency during the FY 2020 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	Fiscal Service management evaluated the prior year condition associated to users having read access to system datasets containing sensitive information and concluded that the risk was low and accepted such risk.	Fiscal Service Management has accepted the risks associated with these FY 2019 conditions 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

[2] 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 applications

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
their use. (FY 2019 recommendation #7)			
Provide for annual review of all techniques that permit a program to obtain the privileges of the operating system. (FY 2019 recommendation #8)	Fiscal Service management has updated the configuration baseline to limit read access to system datasets such as page datasets to only programmers.	Fiscal Service management has updated access to the system to limit read access to the page datasets.	Closed
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 internally determined the risk is mitigated due to the security file being encrypted.	Fiscal Service Management has accepted the risks associated with these FY 2019 conditions 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
FY 2018 Finding Open in 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***
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)	Updated policies, procedures, and Mainframe security software securing configuration baseline documentation. Supervisor Call (SVC)[3] instructions were not identified on baseline documentation but were identified within the system are due to Fiscal Service changes to and/or use of the SVCs. Lastly, management also	Fiscal Service Management has documented the ISS Mainframe Access Management Security Review and updated the Fiscal Service Mainframe security software baseline document that considers Mainframe security software hardening settings from the DISA STIGs and that include risk categories and/or deviations from	Open

[3] In IBM mainframes, an SVC is a processor instruction that directs the processor to pass control of the computer to the operating system's supervisor program. Most SVCs are requests for a specific operating system service from an application program or another part of the operating system.

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
	performed a review of the Mainframe security software settings.	actual STIG settings. However, the documentation lacked sufficient detail to determine that controls/processes were designed and implemented to fully address FY 2019 conditions. Specifically, we determined the following: • Baseline documentation did not identify all values to be set in the Mainframe security software configuration file. E.g., (1) Four SVCs identified on the system were not reflected on documentation provided. Formal Risk acceptance to include adequate compensating controls to reduce the risk of unauthorized access to and modification of mainframe computing resources, payment and production data were not documented. (2) Procedures for comparing actual Top Secret settings to the Fiscal Service Baseline or STIGs were not sufficiently	

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
		documented. • Policies and procedures and baseline documentation did not identify steps to be taken to ensure reviews against the STIGs and/or Fiscal Service's Top Secret baseline were complete and accurate such that all setting recommendations are addressed and if not, reasoning for non-inclusion to include formal risk acceptance and compensating controls.	
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 STIGs.	Fiscal Service Management did update documentation noted in the Fiscal Service Corrective Action Taken to include an annual comparison of actual Mainframe security software configurations derived from the DISA STIGs. However, management did not include formal risk acceptance and justifications for not addressing all high risk DISA STIG configuration settings, nor did management identify compensating controls associated with preventing unauthorized access and modification to computing resources and payment and production data. For example, we noted one example where the actual Mainframe security software	Open
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	Updated Fiscal Service Mainframe security software policies, procedures and baseline documentation.		Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
approving the setting. (updated FY 2019 recommendation #12)		configurations does not meet the STIG (i.e. STIG ID ACP00260). The closure package did not include respective formal risk acceptance, POA&M, and/or compensating control evidence for such variance.	
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.	Fiscal Service management has identified non-compliant Mainframe security software settings and has documented POA&Ms. As such, corrective action has not been fully implemented during the audit period to address the prior year recommendations. Further, management did not identify and/or provide compensating controls associated with preventing unauthorized access and modification to computing resources and payment and production data.	Open
Remove duplicate and excessive permissions in the mainframe security software database. (FY 2019 recommendation #14)			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)	Policies and procedures for comparing actual Mainframe security software settings to the configuration baseline and for controlling update to the Mainframe security software control file, and the Fiscal Service configuration baseline was compared to actual.	Policies, procedures and baseline documentation lacked sufficient detail, such as listing all the User SVCs on the system to include what the programs do, how management knows they are safe, and who approved them.	Open
Develop and document procedures for controlling updates to the mainframe security software control file. (FY 2019 recommendation #16)			Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
FY 2018 Finding Open in FY 2019 – 3) Excessive privileged access that violates the principle of least privilege is allowed on the Mainframe.			***Open***
Define and document the segregation of functions and privileges based on the principle of least privilege for mainframe security software and operating system. (FY2019 recommendation #17)	Fiscal Service management has updated policies, access management standards, and baseline documentation that speak to segregation of functions and privileges. For excessive privileges identified in the associated condition that has not been remediated are being addressed through five POA&Ms. Lastly, Fiscal Service management has accepted any inherent risk associated with continuing to allow programmers to have read access to system datasets containing sensitive data.	Fiscal Service management has documented the following in support of restricting access based on segregation of duties and principles of least privilege as evidenced by reviewing such access documentation on a periodic basis: • Access Management Policy; • Access Management Standards; • Access Management Security Review; and • Combined Mainframe security software baselines.docx. However, management has not fully implemented policies and procedures with respect to excessive privileged access that violates the principle of least privilege as management is in the process of addressing POA&Ms associated with excessive permissions. Lastly, management has accepted risks associated with allowing programmers to have read access to system datasets containing sensitive data and did not identify and/or provide compensating controls to reduce the risk of unauthorized disclosure of mainframe computing	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

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
		resources and payment and production data.	
Identify and document the person responsible for approving each access permission. (FY 2019 recommendation #19)	Fiscal Service management has updated policies and procedures associated with responsibilities for approving access permissions.	Fiscal Service management has documented Access Management Policy and Access Management Standards with responsibilities for approving access permissions. As such, management's corrective actions taken addressed the prior year conditions.	Closed
Review and re-assess each access permission in the mainframe security software dataset and resource rules on a periodic basis. (FY 2019 recommendation #20)	Fiscal Service management has performed a periodic review of access permission, and for areas of continued excessive permissions that could not be addressed due to the impact of remediation's, management developed POA&Ms 32327, 27005, 32333, 32329, and 32315. Lastly, from the review of programmer's access to system datasets containing sensitive data, management has accepted any inherent risk associated with allowing such users to have read access.	Fiscal Service management has documented the following in support of performing and documenting periodic reviews of privileged access: • Access Management Policy; • Access Management Standards; • Access Management Security Review; and • Combined Mainframe security software baselines.docx. However, because management has not completed its POA&Ms for restricting/limiting the remaining excessive privileges allowed on the mainframe, it has not fully implemented its corrective actions to remediate this deficiency during the FY 2020 audit period.	Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
		See KPMG determinations above regarding management's acceptance of the inherent risk of allowing system programmers to have read access to system datasets containing sensitive data.	
Develop procedures and documentation to establish the following for each dataset permission, resource permission, and mainframe security software privilege: 1. Responsibility for approving access and enforcing compliance with the principle of least privilege; 2. Actual access meets the principle of least privilege; and 3. Any discrepancy from approved access will be identified and corrected. (FY 2019 recommendation #21)	Fiscal Service management has updated policies, access management standards, and baseline documentation that speak to responsibilities for approving access. For discrepancies of approved access that have been identified with excessive privileges, management has developed the POA&Ms 32327, 27005, 32333, 32329, and 32315 to correct such access. Lastly, management has accepted any inherent risk associated with continuing to allow programmers to have read access to system datasets containing sensitive data.	Fiscal Service management has documented the following in support of approving privileged access: • Access Management Policy; • Access Management Standards; • Access Management Security Review; and • Combined Mainframe security software baselines.docx. However, because management has not completed its POA&Ms for restricting/limiting the remaining excessive privileges allowed on the mainframe, it has not fully implemented its corrective actions to remediate this deficiency during the FY 2020 audit period. See KPMG determinations above regarding management's acceptance of the inherent risk of allowing system programmers to have read access to system datasets containing sensitive data.	Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
FY 2018 Finding Open in FY 2019 – 4) Logging and monitoring controls for the Mainframe are not fully implemented to detect unauthorized activity. (GWC and TMA)			***Open***
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 informed us that due to high priority actions needed to support the CARES Act, the POA&M to address this recommendation will not be completed until October 31, 2020.	We determined that the status of this recommendation is 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 2020.	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

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 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)	Fiscal Service management updated policies and procedures.	Fiscal Service management provided documentation that outlined the following: 1. Performance tuning, 2. Problem management, 3. Capacity planning, and 4. Management of service level agreements. However, documentation provided (e.g., Log Management Policy and Information Logging Standard) were enterprise level documents, which did not sufficiently document audit and logging controls specific to the mainframe environment, such as CA Compliance Manager, Audit Tracking File (ATF), System Management Facility (SMF), DB2, and Mainframe security software. In addition, evidence of implementation of policies and procedures were not provided as recommendations 1-5 and 8 are in process of being addressed.	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)	Fiscal Service management updated policies and procedures.		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	Fiscal Service management informed us that due to high priority actions needed to support the CARES Act, the POA&M to address this recommendation will not be completed until 10/31/2020.	We determined that the status of this recommendation is 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	Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
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).		corrected control in FY 2020.	
FY 2018 Finding Open in FY 2019 – 5) Mainframe security control documentation needs improvement. (GWC and TMA)			***Open***
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	Fiscal Service management has updated access management policies, standards, and baseline documentation that speak to mainframe security controls affecting the system software. SVCs[4] were not identified on baseline documentation but were identified within the system and are due to Fiscal Service changes to and/or use of the SVCs.	Fiscal Service management has documented the following in support of mainframe security controls: • Access Management Policy; • Access Management Standards; • Access Management Security Review; and • Combined Mainframe security software baselines.docx. However, policies, procedures and baseline documentation lacked sufficient detail, such as listing all the User SVCs on the system to include what the programs do, how management knows they are safe, and who approved them. Specifically, we determined the following:	Open

[4] In IBM mainframes, an SVC is a processor instruction that directs the processor to pass control of the computer to the operating system's supervisor program. Most SVCs are requests for a specific operating system service from an application program or another part of the operating system.

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
operating system security, and 5. Standard procedures to compare actual configuration settings to baseline documents. (FY 2019 recommendation #30)		• Baseline documentation did not identify all values to be set in the Mainframe security software configuration file. E.g., (1) Four SVCs identified on the system were not reflected within documentation provided. Formal Risk acceptance to include adequate compensating controls to reduce the risk of unauthorized access to and modification of mainframe computing resources, payment and production data were not documented. • Procedures for comparing actual Top Secret Security (TSS) settings to the Fiscal Service Baseline or STIGs were not sufficiently documented. E.g., Policies and procedures and baseline documentation did not identify steps to be taken to ensure reviews against the STIGs and/or Fiscal Service's Top Secret baseline were complete and accurate such that all setting recommendations are	

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
		addressed and if not, reasoning for non-inclusion to include formal risk acceptance and compensating controls identification.	
Develop, approve, and promulgate control standards that address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance processes. (FY 2019 recommendation #31)	Fiscal Service management has updated access management policies and standards that address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance processes.	Fiscal Service management has documented an Access Management Policy and Access Management Standards that address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance processes.	Closed
Update mainframe documentation to be consistent with Fiscal Service and TD P 85-01 requirements. (FY 2019 recommendation #32)	Fiscal Service management has updated access management policies, standards, and baseline documentation that speak to mainframe security controls affecting the system software. SVCs were not identified on baseline documentation but were identified within the system are due to Fiscal Service changes to and/or use of the SVCs.	See KPMG determination above regarding all User SVCs within the system not being defined within policies, procedures and baseline documentation.	Open
Develop procedures and documentation to establish who is responsible and how effective security is achieved for controls. (FY 2019 recommendation #33)	Fiscal Service management has updated access management policies and standards that speak to who is responsible and how effective security is achieved for controls noted in the recommendation. In addition, as it relates to the following controls, management accepted risk	Fiscal Service management has documented an Access Management Policy and Access Management Standards that detail responsibility for ensuring effective security is achieved. However, management has 'accepted the risks' associated with read access to sensitive datasets as well	Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
	associated with the noted recommendations: • Read access to sensitive system datasets such as the TSS files, the spool and checkpoint datasets, and the page datasets (FY 2019 recommendation); • Control over encryption of data at rest, including the encryption function; and • Control over use of encryption keys and functions, including ICSF (Integrated Cryptologic[ix] Services Facility).	as controls over encrypted[5] data 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.	
FY 2018 Finding Open in FY 2019 – 6) UNIX periodic user access review is still not consistently performed.			***Open***
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 provided corrective actions documentation; however, management did not provide sufficient evidence to support remediation.	Fiscal Service management provided corrective actions to support the FY 2019 condition; however, we determined that management did not provide sufficient evidence to address the periodic user review weakness identified in FY 2018 due to the following:	Open
Configure the systems-management software agents to include all UNIX			

[5] We concluded that this responsibility applies to the page files, the spool dataset, the checkpoint dataset, the Mainframe security software database containing userids and passwords (which can be learned by means of a password cracker program, even though they are encrypted), the SMF datasets (which occasionally contain a password in the event users confuse their userids with their passwords), and others.

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
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) 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)		• For one server, documentation was not maintained to confirm the users on the production webserver were appropriate for the recertification. • For three servers, approval of user accounts for appropriate access was given prior to the review of each user account for appropriate access and privileges. • The semi-annual review was not completed in a timely manner. The bureau defines a semi-annual review as January-June and July-December. However, the semi-annual review was initiated in Jul 2019 and did not conclude until April 2020.	
FY 2018 Finding Open in 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***
Finalize policies and procedures to review audit logs of production IBM Database 2 (DB2) servers. (FY 2019 recommendation #37) Implement an oversight process to ensure that designated Fiscal Service personnel: 1. Reviews the security logs for the UNIX and DB2 servers hosting	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2020.	We determined that the status of this recommendation is 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 2020.	Open

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
the PIR, JFICS, and SPS applications on a pre-defined frequency, as indicated in the BLSR. 2. Formally documents completion of their reviews and any escalations to the Information System Security Office (ISSO), and 3. Retains the audit logs and documentation of its reviews for 18 months, as required by the BLSR. (FY 2019 recommendation #38)			
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)			
Establish an effective enforcement process or mechanism to ensure that (a) UNIX and DB2 events and monitoring controls are			

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
followed, and (b) Fiscal Service management has confidence it consistently reviews for potential unauthorized or inappropriate activity. (FY 2019 recommendation #40)			
FY 2019 Finding – 8) Improvements are needed in controls over management's semi-annual review and recertification of PIR developers' access.			***Open***
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's corrective actions are planned to be implemented after September 30, 2020.	We determined that the status of this recommendation is 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 2020.	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)			
Ensure that developers do not have the ability to make changes to the PIR production environment. (FY 2019 Recommendation #43)			

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
FY 2019 Finding – 9) Secure Payment System (SPS) periodic user access review needs improvement.			***Open***
Remove users' access once validated by the FPA, during the SPS annual user access review. (FY 2019 Recommendation #44)	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2020.	We determined that the status of this recommendation is 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 2020.	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)			
FY 2019 Finding – 10) TWAI users' access recertification needs improvement.			***Open***
Review and enhance the manual processes and procedures to ensure that user access to all resources as defined for TWAI users are accurately and completely identified and evaluated during the course of the GSS1 and GSS2 TWAI User Privilege Recertification cycles. (FY 2019 Recommendation #47)	Fiscal Service management provided corrective actions documentation; however, management did not provide sufficient evidence to support remediation.	Fiscal Service management provided a corrective action closure package. However, evidence of the GSS2 review was not provided and we were informed it would not be completed until January 2021.	Open
Complete the GSS1 TWAI User Access Recertification cycle within the time intervals set by BLSR requirements. (FY 2019 Recommendation #48)			

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
FY 2019 Finding – 11) Treasury's Oracle[x] Financials separation of duties policies, processes, and procedures for Departmental Offices (DO), GWC, and TMA users need improvement.			***Closed***
FY 2019 Finding – 12) PIR user termination control needs improvement.			***Open***
Remove and disable the two users' access accounts that were inactive for over 120 days, immediately. (FY 2019 Recommendation #53)	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2020.	We determined that the status of this recommendation is 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 2020.	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)			
FY 2019 Finding – 13) Unix password control needs improvement.			***Open***
Review and update the EITI SSP, Attachment A–SCM, to be consistent with the BLSR and the Chief Information Officer (CIO) Publication ISS Internal SOP 8.3.6.60 UNIX/LINUX Account Management. (FY 2019 Recommendation #55)	Fiscal Service management provided corrective action documentation; however, management did not address the implementation of the remediation since October 1, 2019.	Fiscal Service management provided corrective action documentation that demonstrated an update to password configurations to a minimum character length of 12 characters on February 20, 2020; however, password configuration settings were not remediated during October 1, 2019 to February 20, 2020 of the audit period.	Open
Configure the six UNIX servers to enforce the minimum password as stated in the Fiscal Service BLSR and ensure that the default password configuration settings for the production Unix environments comply with the minimum			

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
requirements specified in the BLSR. (FY 2019 Recommendation #56)			
FY 2019 Finding – 14) Completeness and accuracy of user data transfer from the Identity and Access Management (IDAM)[xi] system to LDAP application servers needs improvement.			***Closed***
FY 2019 Finding – 15) Weekly review and retention of SPS audit logging needs improvement.			***Closed***
FY 2019 Finding – 16) Lack of approval for PIR emergency changes.			***Open***
Develop and implement a quality control process to ensure that PIR emergency change approvals are consistently obtained, documented, and retained by the configuration control board (CCB) prior to implementing changes into the PIR production environment. (FY 2019 Recommendation #61)	Fiscal Service management's corrective actions are planned to be implemented after September 30, 2020.	We determined that the status of this recommendation is 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 2020.	Open
FY 2019 Finding – 17) Baseline Process over the UNIX environment needs improvement.			***Open***
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, 2020.	We determined that the status of this recommendation is 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 2020.	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			

Findings Included in the FY 2019 Fiscal Service IT Management Report			
FY 2019 Recommendations	**Fiscal Service Corrective Action Taken**	**Determination of Action Taken**	**FY 2020 Status**
compensating controls that mitigate the security risk to an acceptable level. (FY 2019 Recommendation #63)			
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)			
Provide logging and monitoring of security related events to include the retention of evidence of reviews performed. (FY 2019 Recommendation #65)			
Develop a baseline of essential security settings and specifying that baseline as the standard to be observed. (FY 2019 Recommendation #66)			
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)			

List of Abbreviations

Abbreviations	Definition
AC-2	Account management
ATF	Audit Tracking File
ASM	Assistant Secretary for Management
BIOS	basic input/output system
BLSR	Baseline Security Requirements
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CARS	Central Accounting Reporting System
CCB	Configuration Control Board
CIO	Chief Information Officer
CMDB	Configuration Management Database
CP-1/CP-2	Contingency Planning
CP-9	Backup and Recovery
DB	Database
DB2	IBM Database 2
DCFO	Deputy Chief Financial Officer
DISA	Defense Information Systems Agency
DO	Departmental Offices
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
ISSO	Information System Security Officer
IT	Information Technology
JFICS	Judgment Fund Internet Claim System
KC	Kansas City
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
POC	Point of Contact
PY	Prior Year
Rev.	Revision
RBAC	Role Based Access Control
RFC	Regional Field Centers
SCM	Security Control Matrix
SGL	Standard General Ledger

Abbreviations	Definition
SMF	System Management Facility
SOP	Standard Operating Procedures
SP	Special Publication
SPS	Secure Payment System
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SVC	Supervisor Call
TMA	Treasury Managed Accounts
Department or Treasury	Department of the Treasury
TSS	Top Secret Security
TWAI	Treasury Web Application Infrastructure
VMP	Vulnerability Management Plan

End Notes

[i] 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.

[ii] 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.

[iii] 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.

[iv] 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).

[v] PIR is a centralized information repository for Federal payment transactions.

[vi] JFICS allows for web-based submission and tracking of claims for payment from the Judgment Fund Permanent and Indefinite Appropriation. The Judgment Fund Claims are submitted over the Internet by federal agencies. The submitted claims are for court judgments and Justice Department compromise settlements of actual or imminent lawsuits against the Government.

[vii] 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.

[viii] 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.

[ix] Crypt is the library function which is used to compute a password hash that can be used to store user account passwords while keeping them relatively secure (a password file).

[x] 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

[xi] 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/