Audit Report

OIG-20-022

FINANCIAL MANAGEMENT

Management Report for the Audit of the Department of the Treasury's Consolidated Financial Statements for Fiscal Years 2019 and 2018

December 16, 2019

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 16, 2019

MEMORANDUM FOR TIMOTHY E. GRIBBEN, 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 2019 and 2018

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, 2019 and 2018, 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 November 15, 2019, 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-20-012; issued November 15, 2019).

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: David F. Eisner
Assistant Secretary for Management

David A. Lebryk
Fiscal Assistant Secretary

Carole Y. Banks
Deputy Chief Financial Officer

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

Acting Inspector General
Department of the Treasury:

We have audited, in accordance with auditing standards generally accepted in the United States of America, in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget Bulletin No. 19-03, *Audit Requirements for Federal Financial Statements*, the *consolidated* financial statements of the Department of the Treasury (Department), which comprise the consolidated balance sheets as of September 30, 2019 and 2018, and the related consolidated statements of net cost, consolidated statements of changes in net position, combined statements of budgetary resources and statements of custodial activity for the years then ended, and the related notes to the consolidated financial statements (hereinafter referred to as “consolidated financial statements”), and have issued our report thereon dated November 15, 2019.

In planning and performing our audit of the consolidated financial statements as of and for the year ended September 30, 2019, we considered the Department’s internal control over financial reporting (internal control) to determine the 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. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers’ Financial Integrity Act of 1982*.

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.

Our consideration of internal control was for the limited purpose described in the second paragraph above 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 have not been identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, as discussed in our auditors’ report dated November 15, 2019 on the consolidated financial statements, 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, 2019 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 OMB Circular No. A-130, *Managing Information as a Strategic Resource*. The Bureau of the Fiscal Service (Fiscal Service) relies on a number of 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 or controls did not operate effectively as follows:

1. Cash Management Information Systems

Fiscal Service had unresolved and newly identified control deficiencies related to its general information technology controls over its cash management systems and 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 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) responsibilities are properly segregated; (6) changes to systems are authorized, properly configured, and secured as intended; and (7) baseline policies and procedures for security configuration controls, including password 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; 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, and configuration management. Fiscal Service's corrective action plans for addressing the prior year deficiencies did not include sufficient detail to facilitate a common understanding of the deficiencies and the root causes or the steps and resources needed to fully resolve them. As a result, Fiscal Service's corrective actions did not consistently resolve the underlying causes of the control deficiencies and many of the deficiencies that contributed to the significant deficiency reported in the prior year—all of which, according to Fiscal Service, had been remediated—remained unresolved as of September 30, 2019. Specifically, Fiscal Service continued to have instances in which known information system vulnerabilities and deviations from baseline security requirements were not being remediated on a timely basis and or adequately tracked for remediation. Additionally, Fiscal Service 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. Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources (Repeat Condition).

2. Mainframe security software configuration baseline settings for the mainframe have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access (Repeat Condition).
3. Excessive privileged access that violates the principle of least privilege is allowed on the mainframe (Repeat Condition).
4. Logging and monitoring controls for the mainframe are not fully implemented to detect unauthorized activity (Repeat Condition).
5. Mainframe security control documentation needs improvement (Repeat Condition).
6. UNIX periodic user access review is still not consistently performed (Repeat Condition).
7. Lack of audit log policies and procedures for payment system production database and production UNIX servers and lack of production database security audit log reviews (Repeat Condition).
8. Improvements are needed in controls over management’s semi-annual review and recertification of Payment Information Repository (PIR) developers’ access.
9. Secure Payment System (SPS) periodic user access review needs improvement.
10. Treasury Web Application Infrastructure (TWAI) users’ access recertification needs improvement.
11. Treasury’s Oracle Financials separation of duties polices, processes, and procedures for Departmental Offices (DO), Government Wide Cash (GWC), and Treasury Managed Assets (TMA) users need improvement.
12. PIR user termination control needs improvement.
13. UNIX password control needs improvement.
14. Completeness and accuracy of user data transfer from the Identity and Access Management system to the Lightweight Directory Access Protocol (LDAP) application servers needs improvement.
15. Weekly review and retention of SPS audit logging needs improvement.
16. Lack of approval for PIR emergency changes.
17. Configuration security baseline process over the UNIX and payment system production database environments needs improvement.

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

Very truly yours,

KPMG LLP

Washington, DC
November 15, 2019

APPENDIX I

Department of the Treasury

Cash Management Information Systems Control Deficiencies

The Bureau of the Fiscal Service (Fiscal Service) and its service provider, the Federal Reserve System, manage the following government-wide cash (GWC) and Treasury managed accounts (TMA) systems that had control deficiencies:

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

The details of the control deficiencies are included below and the title of each control deficiency indicates whether it is a repeat condition; all control deficiencies relate to GWC and TMA.

Eight findings are repeat control deficiencies from the Fiscal Year (FY) 2018 audit.[1] For the first five repeated control deficiencies, management created closure packages that involved developing or updating various enterprise policies and procedures to provide documentation to address specific weaknesses noted in the five mainframe findings reported in FY 2018[2].

The Fiscal Service Identity, Credential, and Access Management (ICAM) organization reviewed the entire Access Management Matrix (formerly the role-based access control [RBAC] matrix) for each application supported by the security software and the mainframe environment. Finally, management initiated an Information System Security (ISS) Project to manage the formal review and remediation of all existing security software permissions.

Fiscal Service management closed these 2018 findings in Treasury's Joint Audit Management Enterprise System (JAMES) Financial Analysis and Reporting System;[viii] however, we noted in the closure packages that management had "partial completion" markings for its status to implement corrective actions to remediate these control deficiencies. We assessed the closure packages and identified new conditions in 2019:

- The Access Management Policy contained a list of rules to be followed, but it did not specify how these rules are to be enforced and who is responsible for the enforcement.
- The ICAM Mainframe Access Management Standard did not explicitly outline responsibilities for execution and oversight and was vague. For example, this policy did not specify:
  - How resource access permissions are to be attributed to a business area and correspond with a documented and approved access management document;
  - How system access will be attributed to business areas and correspond with a documented and approved access management baseline; and
  - Terms and definitions, e.g., defining what is meant by "access" and "periodically."
- The Fiscal Service Mainframe User Authenticator Recertification Standard did not indicate how to:

[1] Refer to OIG Report Number OIG-19-024.
[2] Findings #1 - #5 in OIG Report Number OIG-19-024.

  - Determine the user accounts associated with a given application, nor how assurance is provided that all user accounts are addressed during the recertification;
  - Perform recertification of access permissions to datasets and resources;
  - Address user account for started tasks;
  - Provide for and assign responsibility for granting of privileges in the security software; and
- Provide specific steps to address Multiple Virtual Storage vulnerabilities noted in the FY 2018 conditions.

As a result, we reissued the five mainframe control deficiencies.

1) *Controls over the mainframe operating system security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources (Repeat Condition).*

In FY 2018, we reported that the Fiscal Service Baseline Security Requirements (BLSR) and the Treasury Directive Publication 85-01 (TD P 85-01), which incorporate the guidance contained the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, require Fiscal Service management to configure the mainframe operating system security to prevent unauthorized access to the mainframe system software and resources. However, Fiscal Service management did not fully document procedures related to mainframe operating system security, and needs to improve access controls over key system datasets.

Fiscal Service management did not demonstrate that such programs are: secure, approved by management, and protected from unauthorized modification. Fiscal Service procedures, System Security Plans (SSPs), and baseline documents did not provide sufficient assignment of responsibility and authority for determining and documenting how access permissions and configuration options for the mainframe operating system security are to be set. Fiscal Service did not periodically compare actual settings to approved settings and periodically review and evaluate settings and access permissions granted. Furthermore, Fiscal Service had not fully established a robust internal audit function to identify weaknesses.

FY 2019 Status:

The BLSR and the TD P 85-01 security control Baseline Configuration (CM-2) require Fiscal Service management to: 1) develop, document, and maintain under configuration control, a current mainframe baseline configuration; 2) review and update the mainframe baseline configuration annually; 3) employ automated mechanisms to maintain a current, complete and accurate mainframe baseline configuration; and 4) maintain a mainframe operating system baseline configuration for development and test environments that is managed separately from the operation baseline configuration.

Fiscal Service management closed the finding in JAMES without fully completing its closure package and subsequently verifying and validating that the mainframe operating system security baseline follows a benchmark, such as Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIGs), and is implemented effectively in the production mainframe environment. An ineffective mainframe operating system configuration security baseline to support effective information security increases the risk for unauthorized access to and modification of the mainframe system software and production data, and increases the likelihood that security configuration controls, which are approved to be implemented for security purposes (e.g., address vulnerabilities), may not be effectively enforced on mainframe systems.

By assessing the closure packages, we noted the following:

- The closure package described the eight privileged programs noted in the FY 2018 conditions but did not describe the actions to be taken to verify and ensure that these programs do not introduce security exposures.
- The closure package described specific steps to change one of the noted vulnerabilities; however, the closure package did not explain how management will ensure the correction would be maintained going forward.

- The closure package did not address how sensitive authorized datasets are to be protected from unauthorized updates and what approval, review, recertification, logging, or monitoring is to be performed over the security software rules protecting these datasets.
- The closure package included a listing of dataset rules from the security software included in the FY 2018 condition, but did not include an explanation of the nature of these datasets, who approved them, and who reviewed and recertified them. The closure package documents did not provide controls for the identification, protection, and monitoring of key system datasets and sensitive datasets.
- The closure package did not specifically address the mainframe security configuration baseline conditions in the FY 2018 control deficiency, which are still open.

Recommendations:

We recommend that Fiscal Service management:

1. Address the mainframe operating system vulnerabilities noted in the condition as soon as possible (FY 2018 recommendation #1).
2. 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 2018 recommendation #2).
3. Ensure that the chief information security officer assign specific responsibility for providing controls over operating system security, including access permissions to all system datasets and all security-related option settings (FY 2018 recommendation #3).
4. Develop and document controls over changes and monitor update access to all key system datasets (FY 2018 recommendation #4).
5. Develop and document controls to prevent unauthorized, unnecessary read access to system datasets containing sensitive information (FY 2018 recommendation #5).
6. Develop and document controls and baseline documentation of mainframe operating system options specified in the configuration files (FY 2018 recommendation #6).
7. 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).
8. Provide for annual review of all techniques that permit a program to obtain the privileges of the operating system (FY 2019 recommendation).
9. 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).

2) *Mainframe security software configuration baseline settings for the mainframe have not been established consistent with the DISA STIG requirements to prevent unauthorized access (Repeat Condition).*

In FY 2018, we reported that the BLSR and TD P 85-01 require Fiscal Service management to establish mainframe security software configuration baseline to prevent and detect unauthorized access to the mainframe system software; its resources; and PAM and PACER data sets. Fiscal Service management indicated that it configured the security software settings based on the DISA STIG, the configuration standards for Department of Defense (DOD) Information Assurance (IA) and IA-enabled devices/systems. However the current security software configuration settings are not consistent with the STIG. In addition, Fiscal Service management did not develop, document and implement policies, procedures, and controls to approve, recertify, or monitor logs for each of the resource classes that can be used in the security software.

FY 2019 Status:

The BLSR and TD P 85-01 security control CM-2 require Fiscal Service management to: 1) develop, document and maintain under configuration control, a current mainframe baseline configuration; 2) review and update the mainframe baseline configuration annually; 3) employ automated mechanisms to maintain a current, complete and accurate mainframe baseline configuration; and 4) maintain a mainframe baseline configuration for development and test environments that is managed separately from the operation baseline configuration. Additionally, security Least Privilege (AC-6) from the BLSR, TD P 85-01, and the NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires Fiscal Service management to employ the principle of least privilege, allowing only authorized access for users which are necessary to accomplish assigned tasks in accordance with Fiscal Service mission and business functions.

Fiscal Service management closed the finding in JAMES without fully completing its closure package and subsequently verifying and validating that mainframe security software configuration security baselines were consistent with the DISA STIGs and implemented effectively in the production mainframe environment. Not configuring the security software settings in a way that supports effective information security could result in unauthorized access to and modification of the mainframe system software and PAM and PACER production data. Additionally, the lack of a tailored baseline increases the likelihood that security configuration controls, which are approved to be implemented for security purposes (e.g., address vulnerabilities), may not be effectively enforced on mainframe systems.

By assessing the closure packages, we determined that Fiscal Service management did not demonstrate that the programs are: secure, approved by management, and protected from unauthorized modification. We also noted following weaknesses:

- The closure package did not address actual security software settings, which are specified in the security software configuration file, to be enforced.
- The closure package did not provide for development and maintenance of a baseline document specifying how all the security software options are to be set, and it did not address specific conditions mentioned as part of the FY 2018 finding. From an inspection of select actual settings in place in security software, many of the mainframe security software configuration baseline conditions reported in the FY 2018 control deficiency had not been addressed.

Recommendations:

We recommend that Fiscal Service management:

10. Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual mainframe security software settings against the security baseline (FY 2018 recommendation #7).
11. Develop a mainframe security software risk assessment process using the DISA STIG as a guideline (FY 2018 recommendation #8).
12. 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 2018 recommendation #9).
13. Use the mainframe security software configuration baseline to harden the mainframe environment, including the PAM and PACER production (FY 2018 recommendation #10).
14. Remove duplicate and excessive permissions in the mainframe security software database (FY 2018 recommendation #11).
15. 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).
16. Develop and document procedures for controlling updates to the mainframe security software control file (FY 2019 recommendation).

3) *Excessive privileged access that violates the principle of least privilege is allowed on the mainframe (Repeat Condition).*

In FY 2018, we reported that the BLSR and TD P 85-01 require Fiscal Service management to only grant access to mainframe users who are assigned responsibilities in accordance with the organization's missions and business functions. Although, Fiscal Service established a RBAC document for mainframe users with approved access, privileges, and roles, Fiscal Service management had allowed excessive privileged access on the mainframe, including the PAM and PACER logical partitions (LPARs),[ix] which is not consistent with the principle of least privilege access.

Fiscal Service management had not fully defined and documented segregation of functions and privileges based on the principle of least privileges for mainframe security software and operating system. Also, Fiscal Service policy, standards, procedures, SSPs, and baseline documents did not provide sufficient assignment of specific responsibility and authority for determining and reviewing access permissions consistent with the principle of least privilege.

FY 2019 Status:

BLSR security control AC-6 and TD P 85-01 require Fiscal Service management to employ the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Fiscal Service management closed the finding in JAMES without fully completing its closure package and subsequently verifying and validating that system and application privileges assigned to users, datasets and mainframe computing resources were commensurate with job functions and follow the principle of least privilege. Therefore, Fiscal Service may not be able to rely on the security controls provided by the mainframe security software alone, and unauthorized access to and modification of production mainframe, PAM, and PACER data may occur.

By assessing the closure packages, we determined that Fiscal Service management did not demonstrate that it effectively limited access within the mainframe environment based on the principle of least privilege, as the closure packages did not address the excessive privileged access conditions detailed in the FY 2018 control deficiency, which is still open.

Recommendations:

We recommend that Fiscal Service management:

17. Define and document the segregation of functions and privileges based on the principle of least privilege for mainframe security software and operating system (FY 2018 recommendation #12).
18. Review and establish access permissions to the mainframe system and security software based on the principle of least privilege access (FY 2018 recommendation #13).
19. Identify and document the person responsible for approving each access permission (FY 2018 recommendation #14).
20. Review and re-assess each access permission in the mainframe security software dataset and resource rules on a periodic basis (FY 2018 Recommendation).
21. 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; and
    c. Any discrepancy from approved access will be identified and corrected (FY 2019 recommendation).

4) *Logging and monitoring controls for the mainframe are not fully implemented to detect unauthorized activity (Repeat Condition).*

In FY 2018, we tested Fiscal Service's security controls to log and monitor events and reported that they were not sufficient to detect and respond to unauthorized activity on the mainframe operating system, PAM and PACER LPARs, and databases in accordance with the BLSR and the TD P 85-01.

Fiscal Service's policies, standards, procedures, and SSPs did not provide sufficient assignment of responsibility and authority for determining and documenting logging of events, monitoring of mainframe datasets and resources, and review and evaluation of settings to be performed. Moreover, Fiscal Service had not fully established detailed procedures and standards for logging and monitoring accesses to mainframe datasets and resources that follow acceptable industry guidance, such as the DISA STIG, and that is tailored to Fiscal Service's risk profile when specifying how security options are to be set. In addition, Fiscal Service's management security policies did not include procedures to perform periodic reviews of the mainframe security software audit settings against a detailed security configuration baseline.

FY 2019 Status:

BLSR security controls Audit and Accountability Policy and Procedure (AU-1), Audit Events (AU-2), Content of Audit Records (AU-3), and Audit Review, Analysis, and Reporting (AU-6) and TD P 85-01 require Fiscal Service management to:

- Develop, document, and disseminate procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls;
- Review and update the audit and accountability procedures to keep them current;
- Monitor the user of information system accounts;
- Review and analyze information system audit records for indications of inappropriate or unusual activity;
- Report findings to designated organizational officials;
- Integrate its analysis of audit records with analysis of vulnerability scanning information, performance data, information system monitoring information, and data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity;
- Capture security-related events in audit logs; and
- Generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs.

Fiscal Service management closed the finding in JAMES without fully completing its closure package and subsequently verifying and validating that its logging and monitoring controls over users, sensitive datasets, privileged programs, and transactions are effective to detect and respond to unauthorized actions. Fiscal Service does not have the necessary information or reporting to tools and procedures in place to log, identify, and react to unauthorized access to mainframe datasets and resources. Fiscal Service also does not have the means to identify exceptional accesses nor significant changes in patterns of access to mainframe datasets and resources.

By assessing the closure package, we determined that Fiscal Service management did not demonstrate that it logs and monitor security events effectively within the mainframe environment in a manner that adheres to the BLSR and TD P 85-01. Also, we noted following weaknesses:

- The closure package made no reference to use of Fiscal Services external tracking tool used for security audit logging and monitoring.
- The documents included in the closure package did not provide any description of how alerts and events are to be evaluated in its external tracking tool. This tool still did not:
  - Log resource access or log in a format suitable for identification of trends and exceptions;
  - Monitor updates to sensitive datasets and resources; and

  - Monitor execution of powerful programs.
- The closure package did not have controls to enforce the auditing in the mainframe security software, which is the only function in the security software that is comprehensive to determine that a given type of access is reliably logged. Additionally, the mainframe security software still did not log dataset accesses, sensitive IBM resource rules, execution of powerful programs, and resource classes.
- The closure package did not fully address the specific security logging and monitoring conditions identified in the FY 2018 control deficiency, which is still open.

Recommendations:

We recommend that Fiscal Service management:

22. 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 2018 recommendation #16).
23. Review and determine which profiles, applications, databases, and other processes on the mainframe will be logged and reviewed (FY 2018 recommendation #17).
24. Assess all mainframe logs to determine which logs should be evaluated by the incident management tool (FY 2018 recommendation #18).
25. Establish appropriate alerts and event thresholds for those mainframe logs required to be evaluated by the external tracking tool (FY 2018 recommendation #19).
26. Develop and implement data and analysis tools and processes for identifying event trends, patterns, spikes, and exceptions (FY 2018 recommendation #20).
27. 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).
28. 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).
29. 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).

5) Mainframe security control documentation needs improvement (Repeat Condition).

In FY 2018, we reported that the BLSR and the TD P 85-01 require Fiscal Service to identify, document, and assess security controls over its mainframe to prevent and detect security risks. For the mainframe, including the system software and the PAM and PACER, Fiscal Service did not have comprehensive documentation describing how mainframe security is provided and reviewed.

FY 2019 Status:

BLSR security control Services Acquisition (SA-5) and TD P 85 requires Fiscal Service management to obtain:

- Administrator documentation for mainframe operating system, security software, and system software and programs that describes:
  - Secure configuration, installation, and operation of the system, component, or service;
  - Effective use and maintenance of security functions/mechanisms; and
  - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

- User documentation for the mainframe operating system, security software, and system software and programs that describes:
  - User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
  - Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
  - User responsibilities in maintaining the security of the system, component, or service.

Fiscal Service management closed the finding in JAMES without fully completing its closure package and subsequently verifying and validating it adequately documented the design and operation of mainframe security controls in place. Without comprehensive documentation describing how mainframe security is provided, Fiscal Service mainframe system software may not be configured in a way that supports effective information security. As a result, there may be unauthorized access to, and modification of, production data.

By assessing the closure packages, we determined that Fiscal Service management did not demonstrate that it fully documented its mainframe security controls in a manner that adheres to the BLSR and TD P 85-01. Specifically, the closure packages did not address the specific mainframe security documentation conditions detailed in the FY 2018 control deficiency, which is still open.

Recommendations:

We recommend that Fiscal Services management:

30. 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:
    a. Specific assignment of responsibility for maintaining operating security,
    b. Skill assessment and remediation for operating system security maintenance,
    c. Baseline documents for mainframe configuration files,
    d. Standard procedures for review and maintenance of operating system security, and
    e. Standard procedures to compare actual configuration settings to baseline documents (FY 2018 recommendation #21).
31. Develop, approve, and promulgate control standards that address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance processes (FY 2018 recommendation #22).
32. Update mainframe documentation to be consistent with Fiscal Service and TD P 85-01 requirements (FY 2018 recommendation #23).
33. Develop procedures and documentation to establish who is responsible and how effective security is achieved for controls (FY 2019 recommendation).

6) UNIX periodic user access review is still not consistently performed (Repeat Condition).

In FY 2018, we reported that the Fiscal Service BLSR and Enterprise Information Technology Infrastructure (EITI) [x] Security Control Matrix (SCM) require Fiscal Service management to perform a semi-annual periodic user review in accordance with implemented policies and procedures to review and reevaluate privileges associated with changes to the information system. Although Fiscal Service Management performed an annual user review, Fiscal Service management did not perform a semi-annual periodic user review of privileged UNIX users in accordance with established policies.

FY 2019 Status:

Fiscal Service management established policies and procedures to perform semi-annual user access review and recertification for the UNIX environment. Additionally, management completed the semi-annual reviews of user accounts and privileges for the production UNIX servers and payment system databases and retained evidence. However, Fiscal Service management did not perform the semi-annual review and recertification for accounts on one sampled UNIX server. Consequently, management did not review and recertify all privileged production UNIX and database accounts as required by the Information Security Services (ISS) Internal Standard 8.3.4.9, BLSR, and the NIST SP 800-53, Rev. 4.

Security control Account management (AC-2) and EITI SCM requires Fiscal Service management to monitor the user of information system accounts and review accounts for compliance with account management requirements on a semi-annual basis.

Management stated that one UNIX server was omitted because Fiscal Service relies on systems-management software to generate the listings of UNIX and payment system production databases accounts to be reviewed for the semi-annual review and the systems-management software agent failed to generate the listing of users across all UNIX servers and databases. Although the systems-management software agent is installed on each server and database in the UNIX environment, issues related to the systems-management software tool and the recertification script used for the periodic user review prevented the generation of complete and accurate listings of UNIX system administrators, database administrators (DBAs), and users to be used for semi-annual access reviews and recertification.

In addition, Fiscal Service had implemented a systems-management software that provides system administrators with remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory functionality. Fiscal Service used this systems-management software to generate current lists of users to facilitate its annual and semi-annual access reviews. Fiscal Service procedures did not include steps to validate periodically that the systems-management software agents include all UNIX servers, payment system production databases, and user accounts and privileges when generating user listings for the UNIX semi-annual access review and recertification.

When management does not first perform validation steps to confirm the completeness and accuracy of the UNIX access listings generated by systems-management software, the risk exists that unauthorized or invalid accounts may be omitted from being detected and subsequently removed or adjusted in a manner that is consistent with the concept of least privilege. Therefore, the control as performed may not cover the intended risk and will not be accurate and comprehensive.

Recommendation:

We recommend that Fiscal Service management:

34. 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 (2018 recommendation #24).
35. 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 (2019 Recommendation).
36. 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 (2019 Recommendation).

7) Lack of audit log policies and procedures for payment system production database and production UNIX server and lack of database audit log reviews (Repeat Condition).

In FY 2018, we reported that the Fiscal Service BLSR and EITI SCM require Fiscal Service management to develop policies and procedures over the monitoring and retention of security audit logs for the production

UNIX and the DB2 production servers that host and maintain PIR, JFICS, and SPS applications and production data, and to subsequently conduct a review of those logs. However, the Fiscal Service management had not:

- Developed policies and procedures for the security audit logging and monitoring of activities and events over the DB2 production servers that maintain PIR, SPS, and JFICS production data; and
- Defined the frequency of the use of Fiscal Service's established security tools to support the logging, reviewing, and monitoring of security audit logs on a consistent basis.

FY 2019 Status:

BLSR security controls Access Control Policy and Procedures (AC-1), AC-2, AU-1, AU-2, AU-6, and Audit Record Retention (AU-11) in the EITI SCM require Fiscal Service management to:

- Develop, document, and disseminate procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls;
- Review and update the audit and accountability procedures to keep them current;
- Monitor the user of information system accounts;
- Review and analyze information system audit records for indications of inappropriate or unusual activity;
- Report findings to designated organizational officials;
- Integrate its analysis of audit records with analysis of vulnerability scanning information, performance data, information system monitoring information, and data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity; and
- Retain audit logs and records for 18 months to provide support for after-the-fact investigations for security incidents and to meet regulatory and organizational information retention requirements.

Fiscal Service’s management represented that they implemented corrective actions to remediate the prior-year security audit logging and monitoring control weakness. However, many of these corrective actions were implemented late in FY 2019. Fiscal Service management also closed our recommendations in JAMES on September 30, 2019. As a result, there was not sufficient time for us to determine if the policies and procedures were consistently being followed and the corresponding controls performed correctly to conclude that the overall control deficiency was remediated during FY 2019.

Fiscal Service management had not finalized policies and procedures to review audit logs of the production database and server hosting the PIR, JFICS, and SPS UNIX applications, document the review, and investigate any abnormal events and activities. Fiscal Service management had not implemented an oversight process to ensure adherence to policy and procedures over audit logging. In order to determine if management has properly addressed the root cause of this control deficiency, we will have to perform relevant audit procedures, which would typically include inquiry, examination, observation, and/or re-performance of the effectiveness of the control in operation throughout the year. The four recommendations will be formally reassessed during our FY 2020 audit.

Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. By not establishing procedures and performing log reviews for PIR, JFICS, and SPS production UNIX server and DB2 server, security-related incidents could go unnoticed and uninvestigated, thus increasing the possibility for unauthorized users to continue attempting to access system resources.

<u>Recommendations:</u>

We recommend that Fiscal Service management:

37. Finalize policies and procedures to review audit logs of production DB2 servers.

38. 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 Office (ISSO), and
    c. Retains the audit logs and documentation of its reviews for 18 months, as required by the BLSR.
39. 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.
40. 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.

8) *Improvements are needed in controls over management's semi-annual review and recertification of PIR developers' access.*

The BLSR, EITI SSP, and the 8.3.6.70 Unix Account Recertification Procedures, require management to review and recertify privileged PIR user access on a semi-annual basis. NIST SP 800-53, Rev. 4, requires management to review developers[3] and programmers[4] access. Although management performs this review during the UNIX recertification, they did not retain documentation of its compliance with these requirements. Specifically, we noted the following control deficiencies:

- Although management has obtained an organizational chart identifying the PIR developers from the service provider, its formal PIR and UNIX security procedures do not require management to utilize a system-generated listing of PIR Federal Reserve System developers to validate the appropriateness of developers' access to the PIR production environment.
- Management did not retain supporting documentation, such as a system-generated listing from the UNIX operating system, used to review and recertify the access of the known PIR Federal Reserve System developers.
- During field testing, management was unable to identify personnel with knowledge and ability to provide a system-generated listing of the PIR Federal Reserve System developers and the privileges assigned to the PIR Federal Reserve System developers within the application and UNIX.
- Although management had granted the developers access to the PIR production operating system environment (i.e. PIR production server), management was unable to provide supporting documentation detailing the privileges assigned (e.g., update, read, or promote changes into the PIR production environment) within the production environment to them. As a result, we were unable to determine if the developers' access was assigned commensurate with their job responsibilities.

Security controls AC-2 and Access Restrictions for Change (CM-5) and EITI SSP require Fiscal Service management to: 1) monitor the user of information system accounts, 2) review accounts for compliance with account management requirements, and 3) review and reevaluate privileges.

Fiscal Service established an arrangement with the Federal Reserve System to provide program development support for PIR; however, PIR security policies and procedures do not completely address the risks of incompatible developer access to production related to utilizing a third-party service provider for such support services. Additionally, during the audit, management did not have personnel with knowledge and ability to provide

[3] NIST SP 800-53 states: "A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; vendors; and product resellers. Development of systems, components, or services can occur internally within organizations or through external entities."

[4] The Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) defines a programmer as "A person who designs, codes, tests, debugs, and documents computer programs."

a system-generated listing of the PIR Federal Reserve System developers and the privileges assigned to the PIR Federal Reserve System developers within the application and UNIX.

The PIR Federal Reserve System developers' access and assigned privileges may not be properly reevaluated and recertified as developers during the semi-annual review for UNIX recertification. Therefore, developers could have update access to the production environment, which is not commensurate with their job duties. Unauthorized access to and modification of the PIR system and production data may occur.

Recommendation:

We recommend that Fiscal Service management:

41. 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.
42. 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.
43. Ensure that developers do not have the ability to make changes to the PIR production environment.

9) SPS periodic user access review needs improvement.

Although the management performed the SPS annual user review during FY 2019 and users were validated by the Federal Program Agency (FPA), the recertification package did not include evidence that management reviewed and approved 44 of the 2267 user accounts. In addition, management did not remove 2 of the 2267 user accounts that management determined to be removed as part of the SPS annual periodic user access review process.

BLSR security control AC-2 and SPS SCM security requires Fiscal Service management to: 1) monitor the user of information system accounts, 2) review accounts for compliance with account management requirements, and 3) reevaluate privileges with users with privileges and functions that support system changes.

Due to lack of management oversight, some of the users' access reviews were not retained and removed as identified during the SPS annual user review.

By not effectively reviewing and adjusting, as necessary, SPS user access and privileges on the frequency specified in the SSP, unauthorized access to and modification of the SPS application and modification of production data could occur.

Recommendation:

We recommend that Fiscal Service management:

44. Remove users' access once validated by the FPA, during the SPS annual user access review.
45. Retain evidence of recertification of all users.
46. Oversee the recertification process and ensure that access corrections are processed once received from the FPA.

10) **TWAI users' access recertification needs improvement.**

The BLSR requires management to complete semi-annual reviews of privileged users (e.g., administrators) and an annual review of non-privileged users. To comply with this requirement, Fiscal Service performs the following TWAI account reviews:

1. General Support System 1 (GSS1) recertification – Fiscal Service management performs an annual review and recertification of all TWAI privileged and non-privileged users.
2. GSS2 recertification – Fiscal Service management performs an annual review and recertification of privileged users only (therefore, reviewing the privileged users semi-annually).

However, Fiscal Service management only completed one of the two required TWAI user privilege reviews when it completed the GSS2 recertification cycle in November 2018. As noted above, these users are to be recertified again during the GSS1 recertification and that one was last completed in August 2018 and has not been completed within 12 months from that date as required by Fiscal Service.

The BLSR and TWAI SCM security control number AC-2 require Fiscal Service management to review accounts for compliance with account management requirements. This review should include:

- Verification of active and inactive accounts;
- Verification of business justification for multiple accounts 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 access is removed or modified as a result of reassignments, promotions, terminations, or retirements of departing Fiscal Service employees, FPA, fiscal agent and financial institution employees, contractors, and subcontractors.

Although the GSS1 TWAI IT Infrastructure User Privilege Review Recertification cycle for all TWAI users, including privileged users, was initiated consistent with the requirement, the semi-annual review of privileged users' recertification cycle was delayed because of the reassignment of the recertifiers. As a result unauthorized access to and modification of the TWAI environment and modification of production data could occur.

Recommendation:

We recommend that Fiscal Service management:

47. 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.
48. Complete the GSS1 TWAI User Access Recertification cycle within the time intervals set by BLSR requirements.

11) Treasury's Oracle Financials separation of duties polices, processes, and procedures for Departmental Offices (DO), GWC, and TMA users need improvement.

The Segregation of Duties (SD) policy for Oracle Federal Financials is in the Oracle e-Business Suite (OeBS) SSP SCM for OeBS users. These policies and procedures should be implemented in accordance with the NISTSP 800-53, Rev. 4, family of security controls, including Separation of Duties (AC-5). However, we found that:

- Management had not formally documented the TMA SD responsibilities for Fiscal Accounting Operations and does not have a formal review and retention process documented;

- Evidence of annual reviews of the DO, GWC, and TMA responsibility matrices was not available; and
- The DO, GWC, and TMA responsibilities matrices do not define which roles and privileges have conflicting responsibilities and should not be assigned to a user.

Therefore, we determined that management did not have a formal review and retention process documented—in accordance with its OeBS SSP and NIST SP 800-53—for the existing DO, GWC, and TMA SD responsibility matrices.

Security controls AC-1, AC-2, and AC-5 in the OeBS SSP security control number require Fiscal Service management to:

- Develop, document, and disseminate an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance;
- Review and update the access control policy and procedures; and
- Document separation of duties of individuals and define information system access authorizations to support separation of duties.

Management was not aware that it had to:

- Document the TMA Oracle Financials SD responsibilities for Fiscal Accounting Operations and document its formal review and retention process; and
- Retain evidence of annual reviews of the DO, GWC, and TMA responsibility matrices.

Separation of duties helps prevent fraud, waste, and abuse in the entity by considering the need to separate authority, custody, and accounting in the organizational structure. Therefore, by not formally documenting the TMA SD responsibilities for Fiscal Accounting Operations and not properly reviewing the DO, GWC, and TMA responsibility matrices on a periodic basis, management may grant user access to Oracle Financials' menus, screens, and transactions that is not commensurate with the users' job duties. In addition, not having fully documented processes may lead to lack of continuity of operations in the event of personnel turnover.

Recommendations:

We recommend that Fiscal Service management:

49. Create a policy to require a formal review, approval, and documentation of the results for the SD matrix review on an annual basis or when there is a significant change.
50. Document in a SD or Access Management Matrix the TMA SD responsibilities for Fiscal Accounting Operations and maintain the supporting documentation used to review and approve the SD matrix in accordance with the policy.
51. Maintain the supporting documentation used to review and document the results, as well as approve SD responsibility matrices for DO and GWC, TMA in accordance with the policy.
52. Identify conflicting roles and privileges in the DO, GWC, and TMA responsibilities matrices that should not be assigned to an Oracle Financials user when access is granted and reviewed on an annual basis.

12) PIR user termination control needs improvement.

The PIR SSP SCM requires that users' access be terminated after 120 days of inactivity. However, we noted that two users were inactive for over 120 days without access being terminated.

Security control AC-2 in the PIR SCM requires Fiscal Service management to disable inactive PAR user accounts after 120 days of inactivity and removing accounts during recertification process annually (365 days).

Due to the lack of management's oversight, the PIR Helpdesk did not suspend two inactive users' accounts after being notified. Without disabling inactive accounts within the PIR environment in a timely manner, there is an increased risk that Fiscal Service's ability to prevent or detect inappropriate activity is impaired.

Recommendations:

We recommend that Fiscal Service management:

53. Remove and disable the two users' access immediately.
54. 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.

13) UNIX password control needs improvement.

The BLSR Identification and Authentication (IA-5) security control and the Chief Information Officer (CIO) Publication Information Security Services (ISS) Internal Standard Operating Procedure (SOP) 8.3.6.60 require that passwords have a minimum length of 12 characters.

Management informed us that a 'crypt'[xi] function that was installed on payment system production UNIX servers for password hashing only recognized the first eight characters of a password. When the hashing algorithm changed to Secure Hash Algorithms (SHA), it did not update all policies to state that longer passwords of 12 characters could be hashed. In addition, they did not update the associated default password setting on the systems to comply with Fiscal Service management's policies. Weaknesses in password configuration settings over applications, operating systems, and databases increase the risk of unauthorized access to an environment, and may compromise the confidentiality, integrity, and availability of the data residing on the information system.

We also noted the following weaknesses with Fiscal Service's password controls:

- EITI SSP, Attachment A –SCM, UNIX Control Implementation, dated July 9, 2018, defines the implemented minimum password length to a less restrictive minimum 8 character length.
- Six servers within the UNIX environment, which supports the PIR, JFICS and SPS financial systems, had a default password configuration set at a minimum of eight characters.

Recommendations:

We recommend that Fiscal Service management:

55. Review and update the EITI SSP, Attachment A– SCM, to be consistent with the BLSR and the CIO Publication ISS Internal Standard Operating Procedure (SOP) 8.3.6.60 UNIX/LINUX Account Management.
56. 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 requirements specified in the BLSR.

14) Completeness and accuracy of user data transfer from IDAM to LDAP needs improvement.

Security controls AC-2, Access Enforcement (AC-3), and Information Flow Enforcement (AC-4) from NIST SP 800-53, Rev. 4, require management to 1) create, enable, modify, disable, and remove information system accounts, 2) review accounts for compliance with account management requirements, 3) enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies, and (4) enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.

Fiscal Service management has implemented IDAM[xii] to manage user access to information systems and LDAP[xiii] for authorization to certain applications and general support systems across the TWAI and UNIX environments. Upon account creation, modification, or deletion in IDAM, user account information is transferred to LDAP in order to provision or de-provision access to the systems. However, we found that Fiscal Service management has not implemented a control to verify and ensure the complete and accurate transfer of user account information from IDAM to LDAP as required by NIST SP 800-53 Rev 4. Within the TWAI and UNIX environments, the following systems are affected for user authentication: the CIR, TCIS, and JFICS applications.

Fiscal Service management stated that there is an issue where certain applications with heavy customization are not compatible with the built-in reconciliation functionality of IDAM, which management had planned to rely on to ensure that user account information was transferred from IDAM to LDAP in a complete and accurate manner. Without controls to ensure the complete and accurate transfer of user account information between IDAM and the LDAP for the CIR, TCIS, and JFICS applications, the risk of individuals having inappropriate access to these systems and their data increases. This access could allow an individual to use various system functions advertently or inadvertently, to alter the accuracy, integrity, and availability of these systems and their data.

Recommendation:

We recommend that Fiscal Service management:

57. Develop and implement a policy and a control to ensure the complete and accurate transfer of user account information from IDAM to LDAP on an ongoing basis for CIR, TCIS, and JFICS.
58. Perform an analysis for all financial system, mixed systems, and supporting general support systems to identify instances where user account information in IDAM and LDAP do not match and implement corrective actions to remediate these instances.

15) Weekly review and retention of SPS audit logging needs improvement.

The SPS Audit Report SOP requires management to monitor, review, and retain security audit logs for the SPS application on a weekly basis. Although the SPS application has developed procedures to outline a process to implement audit monitoring over the SPS application, management did not perform its review and retention of the SPS audit logging for one of the sampled weeks.

Security controls AC-1, AC-2, AU-1, AU-2, AU-6, and AU-11 of the SPS Audit Report SOP and SPS SCM require Fiscal Service management to:

- Develop, document, and disseminate procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls;
- Review and update the audit and accountability procedures to keep them current;
- Monitor the users of information system accounts;
- Review and analyze information system audit records for indications of inappropriate or unusual activity;
- Report findings to designated organizational officials;
- Integrate its analysis of audit records with analysis of vulnerability scanning information, performance data, information system monitoring information, and data/information collected from other sources to further enhance the ability to identify inappropriate or unusual activity; and
- Retain audit logs and records for 18 months to provide support for after-the-fact investigations for security incidents and to meet regulatory and organizational information retention requirements.

Fiscal Service users that are assigned the “Auditor” role within the SPS application are responsible for the review and retention of the audit logs. However, personnel with the ‘Auditor’ role were unavailable to conduct the review of audit logs and document potential findings for the noted week. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems. By not performing log reviews, SPS security-related incidents could go unnoticed and uninvestigated, thus increasing the possibility for unauthorized users to continue attempting to access system resources.

Recommendations:

We recommend that Fiscal Service Management:

59. Prioritize and reevaluate its procedures to outline a process to complete the application security log reviews over the SPS application and establish a process to perform the review at a defined frequency and update the procedures when changes occur.
60. Include provisions in their process oversight so that at no time the weekly SPS log reviews are not assigned.

16) Lack of approval for PIR emergency changes.

Security control Configuration Change Control (CM-3) in the the BLSR and the PIR CMP require that Fiscal Service management 1) review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analysis, 2) implement approved configuration-controlled changes to the information systems, 3) document configuration change decisions associated with the information system, and 4) retain records of configuration-controlled changes to the information system.

Fiscal Service management obtained verbal approvals for one of the four PIR emergency changes to migrate into the PIR production environment. However, it did not document and retain the Change Control Board's (CCB) approval within the Fiscal Service's change management tool prior to the completion of these system migrations, which did not adhere to the PIR Configuration Management Plan (CMP), the BLSR, and the NIST SP 800-53, Rev. 4.

Due to lack of management's oversight, it did not obtain and retain supporting documentation evidencing formal approval prior to migrating the one emergency change into the production environment. Therefore, unauthorized changes to the PIR production environment or data may occur without management's awareness, thereby affecting the functionality of the application or the integrity of its production data.

Recommendation:

We recommend that Fiscal Service management:

61. Develop and implement a quality control process to ensure that PIR emergency change approvals are consistently obtained, documented, and retained by the CCB prior to implementing changes into the PIR production environment.

17) Baseline Process over the UNIX environment needs improvement.

The BLSR, EITI SCM, and NIST SP 800-53, Rev. 4, require Fiscal Service management to establish security configuration baseline to serve as a basis for current builds, future builds, releases, and/or changes to the information system. Fiscal Service management informed us that it configured the UNIX baseline settings based on the DISA STIG, the configuration standards for DOD IA and IA-enabled devices/systems. The BLSR and EITI SSP SCM security control Baseline Configuration (CM-2) requires Fiscal Service management to 1) develop, document, and maintain under configuration control, a current baseline configuration of the information system; and 2) review and update the baseline configuration of the information system.

In addition, NIST SP 800-53, Rev. 4, security control CM-2 contains guidance for Fiscal Service to 1) develop, document, and maintain under configuration control, a current baseline configuration of the information system, and 2) review and update the baseline configuration of the information system on an organization-defined frequency or circumstances and as an integral part of information system component installations and upgrades.

However, the current baseline configuration policies and settings are not consistent with the STIG and Fiscal Service established policies and procedures. Fiscal Service management has not provided effective security configuration baselines of UNIX operating systems and production databases supporting payment systems. Specifically, we noted the following:

1. Security configuration baseline documentation provided, which did not:
    a. Provide for comparison of actual settings to the recommended specifications;
    b. Specify who is accountable to ensure that the settings are properly set and maintained;
    c. Provide verifiable description of the settings necessary to provide reasonable security control over the payment system production and payment system production databases instances, or the means to compare the actual settings to the documented baseline; and
    d. Define the frequency of periodic comparison of actual system settings currently enforced to the baselines and the follow-up actions to be conducted after such comparison.

2. We were unable to determine in the documentation provided whether the UNIX operating system and payment system production database baseline configurations documentation are periodically reviewed in accordance with established policies.

3. We noted that three selected servers had default user accounts that should have been removed in accordance with current UNIX security configuration baseline.

4. We obtained output from select payment system databases commands to test compliance with the STIGS and noted that the current payment system production databases security configuration settings did not:
    a. Limit the number of concurrent sessions to an organization-defined number per user for all accounts and/or account types;
    b. Enforce non-repudiation of privileged actions (e.g., create, modify, or deleting data items or collections of data in the database);
    c. Provide security audit record generation capability for DOD-defined auditable events within all database management system (DBMS) components;
    d. Allow only the ISSO (or individuals or roles appointed by the ISSO) to select which audible events are to be audited; and
    e. Generate security audit records when privileges/permissions are retrieved.

In the security configuration baseline documentation, Fiscal Service management has not assigned personnel responsible for developing, maintaining, and enforcing UNIX operating system and database security baselines consistently within the UNIX environment. Further, when developing the UNIX operating system and database security configuration baseline documentation and procedures, Fiscal Service management did not ensure that these documents fully incorporate and enforce the components of the DISA STIGs. The lack of assigning personnel responsible for developing, maintaining, and enforcing tailored baseline security policies and procedures increases the likelihood that security configuration controls, which are approved to be implemented for security purposes (e.g., address vulnerabilities), are not effectively enforced on UNIX systems, and contain auditable standards.

<u>Recommendation:</u>

We recommend that Fiscal Service management:

62. Develop and implement documentation to assign responsibility for ensuring adequacy of UNIX and database security and baseline settings.

63. 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.
64. Develop, document, and implement policies, procedures, and controls to conduct periodic reviews of actual UNIX and database settings against the security configuration baselines.
65. Provide logging and monitoring of security related events to include the retention of evidence of reviews performed.
66. Develop a baseline of essential security settings and specifying that baseline as the standard to be observed.
67. Implement corrective actions to address all vulnerabilities associated with the baseline enforcement to include removing the three default user accounts on UNIX servers.

Findings Included in the FY 2018 Fiscal Service IT Management Report	**FY 2019 Status**
1) Controls over the Multiple Virtual Storage (MVS) security configuration settings are not restrictive to prevent unauthorized access to the mainframe production data and resources. (GWC & TMA)	Re-issued, Finding #1
2) CA Top Secret configuration baseline settings for the mainframe have not been established consistent with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) requirements to prevent unauthorized access. (GWC & TMA)	Re-issued, Finding #2
3) Excessive privileged access that violates the principle of least privilege is allowed on the mainframe.	Re-issued, Finding #3
4) Logging and monitoring controls for the mainframe are not fully implemented to detect unauthorized activity. (GWC & TMA)	Re-issued, Finding #4
5) Mainframe security control documentation needs improvement. (GWC & TMA)	Re-issued, Finding #5
6) UNIX periodic user access review is not consistently performed. (GWC & TMA)	Re-issued, Finding #6
7) Fiscal Service is currently not completing a review over JFICS developers and users with access to migrate changes to the production environment. (TMA)	Closed
8) Fiscal Service is currently not completing a review over SPS developers and users with access to migrate changes to the production environment. (TMA)	Closed
9) Improvements are needed in controls over the segregation of duties between individuals that create and manage Agency Locator Codes (ALCs) for agencies and individuals who initiate SPS payments. (GWC & TMA)	Closed
10) UNIX Configuration Change Management Controls Needs Improvement. (GWC & TMA)	Closed
11) JFICS configuration change policies and procedures do not provide sufficient detail over the process. (TMA)	Closed
12) Security patches to JFICS database server were not consistently applied. (TMA)	Closed
13) JFICS controls for disabling of inactive accounts need improvement. (TMA)	Closed
14) JFICS security event monitoring controls need improvement. (TMA)	Closed
15) SPS security event monitoring controls need improvement. (GWC & TMA)	Closed
16) PIR, JFICS, and SPS audit logging policies and procedures were not present for DB2 server, and neither production UNIX servers nor DB2 servers had logs that were reviewed consistently. (GWC & TMA)	Re-issued, Finding #7
17) PIR was not locking out sessions automatically in accordance with the PIR SSP and BLSR SSP. (GWC & TMA)	Closed
18) PIR vulnerability scans are not performed consistently. (GWC & TMA)	Closed

LIST OF ABBREVIATIONS

Abbreviations	Definition
AC-1	Access Control Policy and Procedures
AC-2	Account management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
ALCs	Agency Locator Codes
AU-1	Audit and Accountability Policy and Procedures
AU-2	Audit Events
AU-6	Audit Review, Analysis, and Reporting
AU-11	Audit Record Retention
BLSR	Baseline Security Requirements
CARS	Central Accounting and Reporting System
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-5	Access Restrictions for Change
DISA	Defense Information Systems Agency
DOD	Department of the Defense
EITI	Enterprise Information Technology Infrastructure
Fiscal Service	Bureau of the Fiscal Service
FY	Fiscal Year
GITC	General Information Technology Controls
GWC	Government-Wide Cash
ISSO	Information System Security Officer
IP	Internet Protocol
IT	Information Technology
JFICS	Judgment Fund Internet Claim System
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
RBAC	Role-Based Access Control (RBAC)
Rev.	Revision
SA-5	System and Service Acquisition
SCM	Security Control Matrix
SP	Special Publication
SPS	Secure Payment System
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TMA	Treasury Managed Accounts
Treasury	Department of the Treasury

END NOTES

[i] 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 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.

[ii] 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.

[iii] 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.

[iv] 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.

[v] Treasury Web Application Infrastructure (TWAI) is an environment that houses Treasury Web applications, including TCIS and 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).

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

[vii] 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.

[viii] JAMES is the system that the Fiscal Service uses to track, report progress on, and close audit findings and recommendations.
[ix] 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.

[x] 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.

[xi] 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).

[xii] 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.

[xiii] 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.

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Treasury OIG Hotline: 1-800-359-3898
Hotline@oig.treas.gov

Gulf Coast Restoration Hotline: 1-855-584.GULF (4853)
gulfcoastrestorationhotline@oig.treas.gov

Access Treasury OIG reports and other information online:
www.treasury.gov/about/organizational-structure/ig