Audit Report

OIG-13-017

Management Report for the Audit of the Financial Management Service's Fiscal Years 2012 and 2011 Schedules of Non-Entity Assets, Non-Entity Costs and Custodial Revenue

December 3, 2012

Office of Inspector General

Department of the Treasury

This report, originally issued in fiscal year (FY) 2013 with Sensitive but Unclassified (SBU) markings, was revised to remove the SBU markings in FY 2020.

This Page Intentionally Left Blank

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

December 3, 2012

MEMORANDUM FOR DAVID A. LEBRYK, COMMISSIONER
BUREAU OF THE FISCAL SERVICE

FROM: Michael Fitzgerald /s/
Director, Financial Audits

SUBJECT: Management Report for the Audit of the Financial Management Service's Fiscal Years 2012 and 2011 Schedules of Non-Entity Assets, Non-Entity Costs and Custodial Revenue

I am pleased to transmit the attached management report in connection with the audit of the Financial Management Service's (FMS) Fiscal Years 2012 and 2011 Schedules of Non-Entity Assets, Non-Entity Costs and Custodial Revenue (the Schedules). Under a contract monitored by the Office of Inspector General, KPMG LLP, an independent certified public accounting firm, performed an audit of the Schedules.[1] The contract required that the audit be performed in accordance with generally accepted government auditing standards; applicable provisions of Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements,* as amended; and the *GAO/PCIE Financial Audit Manual*.

As part of its audit, KPMG LLP issued its Independent Auditors' Report on Internal Control Over Financial Reporting that contained the following repeat significant deficiency on Information Technology Controls Over Systems Managed by FMS and Third Parties: "In fiscal year 2012, we noted that FMS made progress in several areas in its efforts to address this finding. Despite these improvements, our tests revealed that the necessary policies and procedures to detect and correct control and functionality weaknesses have not been consistently documented, implemented, or enforced. FMS' IT general controls do not provide reasonable assurance that: 1. An adequate security management program is in place; 2. Access to computer resources (i.e., data, equipment, and facilities) is reasonable and restricted to authorized individuals; 3. Changes to information system resources are authorized and systems are configured and operated securely and as intended; 4. Incompatible

[1] KPMG LLP's opinion on the fair presentation of the Schedules and related reports on internal control and compliance with laws and regulations were transmitted in a separate report (OIG-13-013, dated November 16, 2012).

duties are effectively segregated; and 5. Contingency planning protects information resources, minimizes the risk of unplanned interruptions, and provides for recovery of critical operations should an interruption occur. Collectively the conditions we observed and reported on could compromise FMS' ability to ensure security over sensitive financial data related to TMA and the reliability of key systems." KPMG LLP issued the accompanying sensitive but unclassified management report to provide additional details pertaining to this significant deficiency.

In connection with the contract, we reviewed KPMG LLP's reports and related documentation and inquired of its representatives. Our review disclosed no instances where KPMG LLP did not comply, in all material respects, with generally accepted government auditing standards.

Should you have any questions, please contact me at (202) 927-5789, or a member of your staff may contact Mark S. Levitt, Manager, Financial Audits at (202) 927-5076.

Attachment

cc: Richard L. Gregg
Fiscal Assistant Secretary

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

Inspector General, U.S. Department of the Treasury
Commissioner, Bureau of the Fiscal Service (formerly Financial Management Service):[1]

We have audited the Schedules of Non-Entity Assets of the U.S. Department of the Treasury's (Treasury) Financial Management Service (FMS) as of September 30, 2012 and 2011, and the related Non-Entity Costs and Custodial Revenue (collectively, Treasury Managed Accounts (TMA), hereinafter referred to as the Schedules) for the years then ended, and have issued our report thereon dated November 14, 2012.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and applicable provisions of Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*, as amended. Those standards and OMB Bulletin No. 07-04 require that we plan and perform the audits to obtain reasonable assurance about whether the Schedules are free of material misstatement.

The management of FMS is responsible for establishing and maintaining effective internal control over financial reporting related to TMA. In planning and performing our fiscal year (FY) 2012 audit, we considered FMS' internal control over financial reporting related to TMA by obtaining an understanding of the design effectiveness of FMS' internal control related to TMA, determining whether internal controls related to TMA had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures for the purpose of expressing our opinion on the Schedules, but not for the purpose of expressing an opinion on the effectiveness of FMS' internal control over financial reporting related to TMA. Accordingly, we do not express an opinion on the effectiveness of FMS' internal control over financial reporting related to TMA. 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 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. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the Schedules will not be prevented, or detected and corrected on a timely basis.

Our consideration of internal control over financial reporting related to TMA was for the limited purpose described in the third paragraph of this report and was not designed to identify all deficiencies in internal control over financial reporting related to TMA that might be deficiencies, significant

[1] Bureau of the Fiscal Service (BFS) was created on October 7, 2012, and all recommendations will, therefore, be directed to BFS.

KPMG LLP is a Delaware limited liability partnership, the U.S. member firm of KPMG International Cooperative ("KPMG International"), a Swiss entity.

deficiencies, or material weaknesses. In our FY 2012 audit, we did not identify any deficiencies in internal control over financial reporting related to TMA that we consider to be material weaknesses, as described above.

Our audit of the Schedule as of September 30, 2012 identified a significant deficiency in internal control over financial reporting related to TMA on "Information Technology Controls Over Systems Managed by FMS and Third Parties." 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. The control deficiencies summarized below and presented in the attachment for your consideration in this report were reported as part of the aforementioned significant deficiency in our *Independent Auditors' Report on Internal Control Over Financial Reporting*, dated November 14, 2012.

During our FY 2012 audit, we evaluated computer systems managed by FMS and its service providers, including the Bureau of Public Debt (BPD), the Pittsburgh National Corporation (PNC) Financial Services, and the Federal Reserve Bank (FRB). We used the Government Accountability Office's (GAO's) Federal Information Systems Controls Audit Manual (FISCAM) to guide our audit. Our audit included general controls over the following applications:

- CA$HLINK II,
- Secure Payment System (SPS),
- Central Accounting and Reporting System (CARS),
- Judgment Fund Internet Claim System (JFICS), and
- Oracle Financials.

We also assessed the status of management's corrective actions to address prior-year findings relating to the mainframe environment. The following applications run on the mainframe environment:

- Treasury's Central Accounting System (STAR),
- Regional Operations Payments System (RO Payments),
- Payment Automation Manager (PAM) System, and
- Treasury Receivable and Accounting Collection System (TRACS).

We identified 13 control deficiencies, of which 9 are new control deficiencies and 4 are control deficiencies that were reported to FMS in our prior year report, in the IT environments supporting the above applications. Although FMS has demonstrated its ability to remediate specific IT findings, we found a lack of consistent application of agency-wide security controls over all systems to ensure that:

- Access to sensitive datasets is properly controlled and restricted based on the principle of least privilege,
- Separation of duties principles is consistently implemented across FMS' applications, and
- Corrective actions are taken to consider the potential implications throughout the entity to address the deficiency systemically.

FMS continues to face ongoing challenges in managing people, processes, and technology amid budget constraints and competing initiatives as it plans to consolidate with the Bureau of Public Debt (BPD) into the Bureau of the Fiscal Service (BFS). Although management has established the high-level structures and directives for the new BFS organization, FMS management has not fully updated IT processes and controls to reflect the new environment, and FMS management has not clearly communicated updated roles and responsibilities across the new organization. A summary of the findings by general controls area follows.

Entity-wide Security Management – An entity-wide program for security planning and management represents the foundation for an entity's security control structure and a reflection of senior management's commitment to address security risks. The program should establish a framework and continuing cycle of activity assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

For the past four years, we have found weaknesses in FMS' plans of actions and milestones (POA&M) process. FMS took corrective actions to enhance its process for overseeing and tracking the status of POA&Ms. However, we identified a new weakness over FMS' lack of coordination with the BPD for the orderly transfer of POA&M items relating to UNIX Mid-Tier platform-specific weaknesses.

FMS' oversight of its systems and mission data managed by service providers needs improvement. Specifically, FMS has not implemented a process to obtain assurance that security controls at both BPD and the Pittsburgh National Corporation (PNC) Financial Services, are operating effectively, as prescribed by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*. The IT environments supporting CA$HLINK II, SPS, and JFICS are managed by these entities.

A governing structure does not exist to collect, assess, and share information relating to known weaknesses in one system with designated personnel throughout the organization to eliminate similar weaknesses in other systems.

Separation of Duties – Separation of duties controls ensure that incompatible duties are separated effectively so that users cannot control entire processes. Appropriate assignment of roles and

responsibility, according to traditional IT system functional areas, can maintain a strong internal control environment by separating incompatible sensitive IT roles, such as system administrators, database administrators (DBAs), developers, change management support, and computer operations personnel. Separation of duties deters an individual from introducing unapproved and potentially harmful code into the production environment and ensures the integrity of FMS' information. Our testing found that FMS has not identified incompatible duties for sensitive users within the UNIX Mid-Tier environment as required by the FMS Entity-Wide IT Security Standards. Although FMS has developed an approach to address prior-year mainframe separation of duties weaknesses, we found that FMS is not planning to implement corrective actions to remediate these weaknesses until 2013. The TRACS, STAR, RO Payments, and PAM applications run in the mainframe environment. Given the high volume of cash payment transaction processed through FMS' systems, emphasis should be placed on removing incompatible duties from across FMS' various applications, platforms, and environments to allow management to obtain reliance on the integrity of its financial data.

Access Controls – Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls. We found that while SPS has controls to review the business level transactions, it does not have any automated capabilities or any supporting processes to log and monitor security-relevant events. In addition, we identified weaknesses in the threat management processes to monitor security incidents over the SPS and JFICS environments. FMS should implement a comprehensive access control security program to address the administration of access controls in order to increase the reliability of data and decrease the risk of destruction or inappropriate disclosure of data.

Configuration Management – Configuration management controls ensure that only authorized changes are made to information systems and components. Establishing controls over the modification of information system components helps to ensure that only authorized systems and related program modifications are implemented. However, we found that the SPS configuration management process did not have adequate information and internal controls to address guidance from both Treasury and NIST.

Privileged programs are components of the mainframe operating system that, if not secured, could be accessed by unauthorized users to bypass mainframe security software and modify production data.[2] Privileged programs are typically operating system utilities and third-party programs that support common operating system functions such as disk management, device management, and communications. FMS IT management must know that all privileged programs are (a) safe, (b) approved by management after testing, and (c) not to be modified without management approval. In prior-year audits, we found that the Mainframe Engineering Division (MED) and Data Services Branch management could not provide a complete list of privileged programs that management had approved

[2] Privileged programs reside in Authorized Program Facility (APF) library, authorized datasets, and system libraries such as SYS1.NUCLEUS, SYS1.UADS, SYS1.LPALIB, SYS1.LINKLIB, and SYS1.SVCLIB. For simplicity, we use the term "privileged program" to refer to any program residing in these libraries and operating in supervisor state.

in accordance with NIST recommended security controls. In FY 2012, management identified seven privileged programs that management deemed necessary to monitor and review. However, hundreds of privileged programs are within the FMS mainframe environment; therefore, the list of seven privileged programs is not a complete and authoritative list. Without a complete inventory of privileged programs, FMS could not demonstrate that management performed a comprehensive analysis over all of the programs to determine whether they were approved and secure. Additionally, FMS personnel have still not implemented an automated process to inform the Enterprise Identity, Credentialing, and Access Management (E-ICAM) and Data Services Branch management when new privileged programs are added or existing privileged programs modified.

Contingency Planning – Contingency planning controls protect information resources, minimize the risk of unplanned interruptions, and provide for recovery of critical operations should interruptions occur. Such controls include the assessment of criticality and sensitivity of computerized operations and identification of supporting resources, as well as the steps taken to prevent and minimize potential damage and interruption. We found that management remediated the prior-year weaknesses relating to PAM and RO Payments' contingency plan test. However, we found that the backup controls detailed in the SPS System Security Plan (SSP) do not reflect the primary backup testing process. In addition, FMS management was unable to define who was responsible for the JFICS backup testing process.

The control deficiencies described herein have been discussed with the appropriate members of management and are intended **For Official Use Only**. Our audit procedures are designed primarily to enable us to form an opinion on the Schedules, and therefore may not identify all weaknesses in policies, procedures or controls that may exist.

Additional detailed findings and recommendations associated with these control deficiencies were included in a separate sensitive but unclassified management, dated November 14, 2012, issued in conjunction with our fiscal year 2012 audit of FMS' Schedules of Non-Entity Government-Wide Cash.

This report is intended solely for the information and use of the Bureau of the Fiscal Service management, the U.S. Department of the Treasury Office of Inspector General, OMB, the U.S. GAO, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 14, 2012

U.S. Department of the Treasury
Financial Management Service
Non-Entity Assets, Non-Entity Costs, and Custodial Revenue

Significant Deficiency in Internal Control Over Financial Reporting:
Information Technology Controls Over Systems Managed by FMS and Third Parties

Table of Contents

Appendices

BACKGROUND

The U.S. Department of the Treasury (Treasury) is authorized by Congress to borrow money backed by the full faith and credit of the United States to fund federal operations. Treasury is responsible for prescribing the debt instruments and otherwise limiting and restricting the amount and composition of the debt. The Financial Management Services (FMS), a bureau of the Treasury, provides central payment services to Federal Program Agencies, operates the federal government's collections and deposit systems, and oversees a daily cash flow of $89 billion. FMS provides government-wide accounting and reporting services, and manages the collection of delinquent debt owed to the government.

FMS has an extensive investment in its distributed IT systems to perform its primary mission efficiently. FMS' SPS and JFICS UNIX Mid-Tier support is provided by BPD, and this environment is maintained in Parkersburg, West Virginia. FMS and its customers depend on the FMS IT systems for making payments in a timely manner and for providing accurate financial information. Any disruption to this service or corruption of the information residing in the systems can potentially cause considerable harm to and/or loss of confidence in FMS. To minimize potential harm, FMS has implemented multiple levels of security controls to ensure the confidentiality, integrity, and availability of FMS information.

The Enterprise Business Information & Security Services (EBISS) group developed the Fiscal Service Baseline Security Requirements (BLSR) document that replaced the old FMS Standards Manual in May 2012. This document describes the standard baseline of controls for FMS and BPD (Fiscal Service) applications and systems.

CONCLUSION

Although we found that FMS made progress in several areas to address the prior year significant deficiency, FMS did not consistently implement NIST recommended guidance across all general IT control environments or comply with FMS' policies. Specifically, we identified 9 new control weaknesses and made 16 recommendations spanning three general IT environments, which are the FMS legacy mainframe environments; the Mid-Tier UNIX platform, which is managed by the BPD; and the CA$HLINK II system residing at the PNC Financial Services site in Riverdale, Maryland. The *Detailed Findings and Recommendations* section of this report presents the detailed findings and associated recommendations.

We evaluated prior year IT findings reported in our FY 2011 Sensitive but Unclassified Report on Non-Entity Government-wide Cash: Information Technology Controls Over Systems Managed by FMS and Third Parties, issued November 14, 2011, and determined that FMS did not implement all recommendations from our prior year audit. While FMS closed three prior year control weaknesses, we found that FMS did not fully implement corrective actions for four prior year control weaknesses. Three of the four prior year control weaknesses remain open, and one prior year control weakness was reissued in FY 2012, as FMS originally deemed it closed. See Appendix III, *Status of Prior Year Findings*, for a summary of FMS' progress in addressing prior year recommendations.

Internal controls over these operations are essential to ensure the integrity, confidentiality, and reliability of critical data while reducing the risk of errors, fraud, and other illegal acts. Overall, FMS continues to make progress at resolving identified security weaknesses, and we commend FMS for their efforts and improvements.

DETAILED FINDINGS AND RECOMMENDATIONS

The following control weaknesses were included in a separate sensitive but unclassified (SBU) management report, dated November 14, 2012, issued in conjunction with our fiscal year (FY) 2012 audit of FMS' Schedules of Non-Entity Government-Wide Cash (GWC).

1. FMS mainframe access controls have not been designed to adequately control access to all programs and datasets by those individuals with significant/system programmer privilege, affecting STAR, RO Payments, PAM, and TRACS (Repeat Condition) (see Finding 1 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

2. Separation of duties principles were violated by granting conflicting access to critical resources on the FMS IBM mainframe environment, affecting STAR, RO Payments, PAM, and TRACS (Repeat Condition) (see Finding 2 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

3. FMS did not adequately restrict access over mainframe batch job submissions, which could allow an individual to elevate his/her access privileges, update datasets, and potentially avoid detection (Repeat Condition) (see Finding 3 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

4. Separation of duties for the UNIX Mid-Tier environments, which host the SPS and JFICS applications, is not documented for sensitive users as required by the FMS Entity-Wide IT Security Standards Manual (see Finding 4 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

5. FMS does not monitor privileged programs that bypass mainframe security (Repeat Condition); therefore, FMS management cannot confirm that deployed privileged programs on FMS' mainframe are safe, approved by management, and have not been modified without managements approval (see Finding 5 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

6. The current SPS audit capabilities and functions have controls to review business level transactions, but they do not have any automated capabilities or supporting processes to log and monitor security-relevant events (see Finding 6 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

7. FMS' oversight of its systems and mission data being managed by service providers (CA$HLINK II and the UNIX Mid-Tier Environment of SPS and JFICS) needs improvement. (see Finding 7 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

8. FMS needs to improve coordination with the BPD for the orderly transfer of POA&M items relating to UNIX Mid-Tier platform-specific weaknesses (See Finding 8 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

9. SPS configuration management process lacks adequate information and robust control to address Treasury requirements (see Finding 9 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

10. FMS was unable to provide sufficient evidence of the threat management process over SPS due to changing network infrastructure (see Finding 10 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

11. SPS system security plan does not reflect the primary backup process (see Finding 11 in the "Detailed Findings and Recommendations" section of the GWC IT SBU management report).

We identified the following two control weaknesses during our fiscal year 2012 audit.

12. FMS was unable to provide sufficient evidence of the threat management process over JFICS due to changing network infrastructure.

    An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. Effective monitoring involves the entity performing tests of information system controls to evaluate or determine whether they are appropriately designed and operating effectively to achieve the entity's control objectives.

    The FMS Entity-wide IT Standards prescribes that it is management's responsibility to monitor the effectiveness of its security program over the JFICS environment, which includes the UNIX Mid-Tier platform maintained at the BPD; however, we found a lack of evidence supporting FMS' responsibility for threat management. Moreover, FMS did not document the effectiveness of their monitoring program by not confirming whether:

    1. The actual JFICS Internet Protocol (IP) addresses in production at the time of the vulnerability scans that were run from October 1, 2011 to June 30, 2012 were valid;
    2. Any vulnerabilities were identified; and
    3. Any corresponding corrective actions had been implemented.

    As a result, we were unable to test the effectiveness of the controls over FMS' threat management process for JFICS.

    As FMS plans to consolidate with BPD into the Bureau of the Fiscal Service, the threat management process has not been effectively communicated to affected field personnel. In addition, the network infrastructure across these environments has been changing to meet the IT network needs of the new organization. Therefore, the IP addresses scanned at different intervals throughout FY 2012 were different from the IP address scanned previously. Management had not documented these changes in the IT environment for JFICS.

    Weaknesses in the threat management process may result in vulnerabilities being undetected, assessed, and remediated, thereby resulting in potential downtime and limited action taken to secure the application and system. These undetected vulnerabilities could permit an attacker to compromise the system, resulting in unauthorized access, disclosure, and/modification of production data. Furthermore, the inability to correlate known vulnerabilities across the organization may result in

uncorrected, unidentified entity-wide vulnerabilities.

Additionally, entities are facing a set of emerging cyber security threats that are the result of changing sources of attacks, increasingly sophisticated social engineering techniques designed to trick the unsuspecting user into divulging sensitive information, new modes of covert compromise, and the blending of once distinct attacks into more complex and damaging exploits. It is, therefore, imperative that FMS adequately protects it systems against emerging threats based on risk.

Criteria

FMS Entity-wide IT Standards, dated April 10, 2012, prescribe the following vulnerability scanning control requirements:

> *Vulnerability Scanning Control:*
> The organization scans for vulnerabilities in the information system and hosted applications monthly, and when new vulnerabilities potentially affecting the system are identified and reported. The organization remediates legitimate vulnerabilities immediately or through the established POA&M process in accordance with an organizational assessment of risk.
>
> Threat Management shall:
> - Provide oversight for all IT system monitoring, including receipt and distribution as needed of information system security alerts

The **NIST SP 800-53 Revision 3,** states:

> *RA- Vulnerability Scanning*
> The organization:
> a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
> b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
> – Enumerating platforms, software flaws, and improper configurations;
> – Formatting and making transparent, checklists and test procedures; and
> – Measuring vulnerability impact;
> c. Analyzes vulnerability scan reports and results from security control assessments;
> d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
> e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
>
> Control Enhancements:

(1) The organization employs vulnerability-scanning tools that include the capability to update the list of information system vulnerabilities scanned.

Recommendations

We recommend that FMS management:

1. Document the vulnerability scanning processes for the new organization and communicate the processes to affected field personnel.

2. Maintain a complete listing of hosts and IP addresses for JFICS production environment and document any changes to this listing, and retain enough supporting documentation to confirm the accuracy of completed vulnerability scans.

3. Strengthen the threat management process to require the sharing of information obtained from the vulnerability scanning process and security control assessments with designated personnel through the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses).

13. JFICS Backup Processes Needs Improvement.

The JFICS application runs on the UNIX Mid-Tier environment, which is maintained and managed by the BPD in Parkersburg, West Virginia. The JFICS production environment, per FMS and BPD management, consists of application, database, and web servers.

During our FY 2012 testing, FMS management was unable to define who was responsible for the JFICS backup testing process. Through inquiry, the FMS JFICS management staff informed us that BPD performs backup test procedures for the JFICS application. However, JFICS management stated that it is not responsible for this control. Furthermore, BPD support personnel informed us that BPD does not perform backup tests unless JFICS management instructs BPD to do so. Through additional inquiry, we determined that JFICS backup tests were not performed consistently by either BPD or JFICS management on a semi-annual basis as required by the Fiscal Service BLSR and the Treasury Directive Publication (TD P) 85-01, the Treasury Information Technology Security Program.

In addition, FMS or BPD could only provide to us supporting documentation evidencing backup testing of the JFCIS application server. No evidence was available to demonstrate backup testing of the database and web servers.

The current backup processes for JFICS and the Mid-Tier environment have not been updated to reflect current roles and responsibilities. These roles and responsibilities have not been communicated to affected field-personnel; thus, this control is not being performed consistently on a semi-annual basis.

Lack of frequent, successful backups can have a significant negative effect on JFICS if a disaster (e.g., hard-drive failure, natural disaster, and national emergency) were to occur. By not testing that backups are created completely and consistently, reliance cannot be placed on them to recover a program, file, database, log, etc., for those times when such information becomes corrupted or

requires being reloaded. The result could be a loss of critical data.

Criteria

Fiscal Service BLSRs, effective May 9, 2012, provides the following control requirement regarding system backups:

> The organization:
> - Conducts backups of user-level information contained in the information system at least daily for HIGH systems and at least weekly for MODERATE and LOW systems;
> - Conducts backups of system-level information contained in the information system at least daily for HIGH systems and at least weekly for MODERATE and LOW systems;
> - Conducts backups of information system documentation including security-related documentation periodically; and
> - The organization tests backup information at least quarterly for HIGH systems and semi-annually for MODERATE systems to verify media reliability and information integrity.

The **Treasury Directive Publication 85-01, Appendix A: Minimum Standard Parameters, CM-6,** states:

> **CP-9 Information System Backup**
> - The organization: Conducts backups of user-level information contained in the information system *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]*;
> - Conducts backups of system-level information contained in the information system *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
> - Conducts backups of information system documentation including security-related documentation *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]*.
>
> *(NOTE: The minimum requirement frequency for a system or application that has a Moderate FIPS 199 rating is specified "Weekly")*

The **National Institute of Standards and Technology, Revision3,** states:

> **CP-9 INFORMATION SYSTEM BACKUP**
> The organization:
> a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
> b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
> c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protects the confidentiality and integrity of backup information at the storage location.

NIST SP 800-53, Revision 3, also requires the following:

PL-2 System Security Plan
The organization:

a. Develops a security plan for the information system that, among others:
   - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Reviews the security plan for the information system at an organization-defined frequency; and
c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Recommendations

We recommend that FMS management:

4. Update the existing JFICS and Mid-Tier UNIX backup procedures and system security plans to clarify roles and responsibilities with regards to the semi-annual testing of JFICS backups to comply with the Fiscal Service's BLSR, Treasury Directive Publication 85-01, and NIST SP 800-53.

5. Communicate the updates to JFICS and Mid-Tier UNIX backup procedures and SSPs to JFICS management staff and BPD support personnel.

6. Test backups for the JFICS production servers semi-annually as prescribed the Fiscal Service's BLSR and the Treasury Directive Publication 85-01.

APPENDIX I – AUDIT METHODOLOGY & CRITERIA

Audit Methodology

In accordance with Generally Accepted Government Auditing Standards (GAGAS), we developed an IT audit approach consistent with methodology prescribed by the Federal Information System Controls Audit Manual (FISCAM). FISCAM describes an audit methodology for assessing the effectiveness of general information systems controls. General information systems controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General information systems controls establish the environment in which application systems and controls operate. FISCAM is comprised of five general information systems controls families, security management, access controls, configuration management, segregation of duties, and contingency planning. An effective general information systems control environment:

1. Provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls to ensure that an adequate security management program is in place;
2. Limits or detects access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;
3. Prevents unauthorized changes to information system resources (for example, software programs and hardware configurations) and provides reasonable assurance that systems are configured and operating securely and as intended;
4. Includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and
5. Protects critical and sensitive data, and provides for critical operations to continue without disruption or be promptly resumed when unexpected events occur.

Criteria

The Office of Management and Budget (OMB) has directed agencies to use the NIST Federal Information Processing Standards Publication (FIPS Pub.) 199, *Security Categorization of Federal Information and Information Systems*, to apply a security categorization rating to an information system. Agencies assign this rating to an information system based on an evaluation of its confidentiality, integrity, and availability.

OMB has further directed that agencies use NIST FIPS Pub. 200, *Minimum Security Requirements for Federal Information and Information Systems*, in order to apply a security controls baseline to the information system, based on the FIPS Pub. 199 categorization. FIPS Pub. 200 specifies the minimum security requirements for the information system and provides a risk-based process for determining the minimum security controls necessary for the information system. In addition, FIPS Pub. 200 specifies 18 controls families that must be addressed when implementing security controls commensurate with the FIPS Pub. 199 security categorization of the system.

NIST Special Publication (SP) 800-53, Revision (Rev.) 3, *Recommended Security Controls for Federal Information Systems and Organizations,* further defines the 18 controls families outlined in FIPS Pub.

200, by defining the minimum set of security controls for non-national security systems of all Federal agencies.

Based on the above guidance from OMB, the U.S. Treasury and FMS have developed complementary policies and procedures that incorporated the required security policies.

We focused our audit approach using federal information security guidance developed by NIST and OMB. NIST SPs provide guidelines that are considered essential to the development and implementation of agencies' security programs.

The following is a listing of the criteria used in the performance of the FY 2012 audit:

- OMB Circular A-130, *Management of Federal Information Resources;*
- NIST FIPS Pub. 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- NIST FIPS Pub. 200, *Minimum Security Requirements for Federal Information and Information Systems;*
- NIST SPs:
  - 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*
  - 800-18 Rev. 1, *Guide for Developing Security Plans for Information Technology Systems*
  - 800-30, *Risk Management Guide for Information Technology Systems*
  - 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*
  - 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - 800-39, *Managing Risk from Information Systems: An Organizational, Mission and Information System View*
  - 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
  - 800-53A Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
  - 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-61 Rev. 1, *Computer Security Incident Handling Guide*
  - 800-70 Rev. 2, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*
- OMB Memoranda:
  - 04-04, *E-Authentication Guidance for Federal Agencies*
  - 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*
  - 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*
  - 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
  - 07-18, *Ensuring New Acquisitions Include Common Security Configurations*
  - 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*
  - 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

- Treasury Guidance:
  - Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*

APPENDIX II – RISK RATING OF DETAILED FINDINGS

Corresponding Finding in the "Detailed Findings and Recommendations" Section	**Title of Finding**	**Risk Rating**
Finding 1	FMS mainframe access controls have not been designed to adequately control access to all programs and datasets by those individuals with significant/system programmer privilege (Repeat Condition).	High
Finding 2	Separation of duties principles were violated by granting conflicting access to critical resources on the FMS IBM mainframe environment (Repeat Condition).	High
Finding 3	FMS did not adequately restrict access over mainframe batch job submission (Repeat Condition).	Moderate
Finding 4	Separation of duties for the UNIX Mid-Tier environments is not documented for sensitive users.	High
Finding 5	FMS does not monitor privileged programs that bypass mainframe security (Repeat Condition).	High
Finding 6	SPS audit and monitoring process needs improvement.	High
Finding 7	FMS' oversight of its systems and mission data being managed by service providers needs improvement.	Moderate
Finding 8	FMS needs to improve coordination with the BPD for the orderly transfer of POA&M items relating to UNIX Mid-Tier platform-specific weaknesses.	Moderate
Finding 9	SPS configuration management process lacks adequate information and robust control to address Treasury requirements.	Moderate
Finding 10	FMS was unable to provide sufficient evidence of the threat management process over SPS due to changing network infrastructure.	Moderate

Corresponding Finding in the "Detailed Findings and Recommendations" Section	**Title of Finding**	**Risk Rating**
Finding 11	SPS system security plan does not reflect the primary backup process.	Low
Finding 12	FMS was unable to provide sufficient evidence of the threat management process over JFICS due to changing network infrastructure.	Moderate
Finding 13	JFICS backup process needs improvement.	Low

APPENDIX III – STATUS OF PRIOR YEAR FINDINGS

FY 2011 Finding	**Title of Finding**	**Action Complete**	**Action in Process**
Finding 1	FMS mainframe access controls have not been designed to adequately control access to all programs and datasets by those individuals with significant/system programmer privilege.		**X**
Finding 2	Separation of duties principles were violated by granting conflicting access to critical resources on the FMS IBM mainframe environment.		**X**
Finding 3	FMS did not adequately restrict access over mainframe batch job submission.		**X**
Finding 4	FMS did not monitor privileged programs that bypass mainframe security		X Reissue from FY 2012 Finding #5.
Finding 5	The PAM and RO Payments applications were not subjected to a failover contingency plan test in FY 2010 and 2011 according to FMS and NIST standards.	X	
Finding 6	POA&Ms were not tracked and remediated in accordance with NIST and Treasury requirements at FMS (Repeat Condition).		X[3]
Finding 7	FMS did not appropriately restrict physical access to the KROC Data Center and IT Command Center.	X	

[3] FMS notified KPMG that it closed the POA&M finding during the end of FY 2012 audit period. This finding was open for most of audit period, and, due to timing of corrective action, we were unable to test the operating effectiveness of this control because a sufficient level of evidence was not available.

APPENDIX IV – LIST OF ACRONYMS

Acronym	Definition
AC	Access Control
ACID	Accessor ID
ATO	Authorization to Operate
BFS	Bureau of the Fiscal Service
BLSR	Baseline Security Requirements
BPD	Bureau of the Public Debt
CARS	Central Accounting and Reporting System
CM	Configuration Management
CP	Contingency Planning
DBA	Database Administrators
EBISS	Enterprise Business Information & Security Services
E-ICAM	Enterprise Identity, Credentialing, and Access Management
FY	Fiscal Year
FISCAM	Federal Information Systems Controls Audit Manual
FISMA	Federal Information Security Management Act
FIPS Pub.	Federal Information Processing Standards Publication
FMS	Financial Management Service
FRB	Federal Reserve Bank
FY	Fiscal Year
GAO	Government Accountability Office
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
GWC	Government-Wide Cash
ISSO	Information System Security Officer
IT	Information Technology
IP	Internet Protocol
JCL	Job Control Language
KROC	Kansas City Regional Operations Center
NIST SP	National Institute of Standards and Technology Special Publication
OMB	Office of Management and Budget
PAM	Payment Automation Manager
PNC	Pittsburgh National Corporation
POA&M	Plan of Action and Milestones
ROC	Regional Operations Center
RO Payments	Regional Operations Payments System
SBU	Sensitive But Unclassified
SOD	Segregation of Duties
SPS	Secure Payment System
SSP	System Security Plan
STAR	Treasury's Central Accounting System
TAF	Trusted Agent FISMA
TD P	Treasury Directive Publication
TMA	Treasury Managed Accounts
TRACS	Treasury Receivable and Accounting Collection System
TWAI	Treasury Web Application Infrastructure

This Page Intentionally Left Blank