



governmentattic.org

"Rummaging in the government's attic"

Description of document: Seven Department of the Treasury Inspector General (OIG) Audit Reports, 2008-2013

Request date: October 2014

Released date: 14-November-2014

Posted date: 26-January-2015

Source of document: FOIA and Transparency
FOIA Request
Department of the Treasury
Washington, DC 20220
Fax: 202-622-3895
[FOIA Online Request Form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

From: "Delmar, Richard K."
Date: Nov 14, 2014 5:11:56 PM
Subject: Your FOIA request 2014-10-080 - Treasury OIG audit reports

This is a partial response to your FOIA request for Treasury OIG audit reports. Following emails will attach further reports. Our overall explanation of what is produced is contained herein:

CA-14-001-Referral memo to OFAC of SARs – produced with redactions of bank names and details of the SARs – per FOIA Exemption 3 and 31 C.F.R. 1010.960

CA-14-002- Referral memo to OFAC of SARs – produced with redactions of bank names and details of the SARs – per Exemption 3 and 31 C.F.R. 1010.960

CA-14-009 – CLASSIFIED PROGRAM REPORT – withheld per FOIA Exemption 1

13-016 – SBU – FMS Non-entity government-wide cash – produced

13-017 – SBU - FMS non-entity costs – produced

13-041 – contract audit – Crane Paper price proposal – withheld per FOIA Exemption 4 - consists of proprietary bid and cost information

CA-09-001- Management Challenges memo to Secretary - produced

CA-09-004 – Memo re IndyMac capital infusion – produced

CA-09-008 – SBU – memo to Secretary re OTS/Failed Bank – produced

If you disagree with this resolution of your FOIA request, you can appeal the matter pursuant to 5 U.S.C. section 552(a)(6)(A)(i). Pursuant to the Department's FOIA appeal process set forth in 31 C.F.R. section 1.5(i), an appeal must be submitted within 35 days from the date of this response to your request, signed by you and addressed to: Freedom of Information Act Appeal, DO, Disclosure Services, Department of the Treasury, Washington, D.C. 20220. The appeal should reasonably describe your basis for believing that Treasury OIG possesses records to which access has been wrongly denied, that the redactions are improper, or that we have otherwise violated applicable FOIA law or policy.

Rich Delmar
Counsel to the Inspector General
Department of the Treasury



OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Sensitive But Unclassified

CA-14-001/002.

October 17, 2013

MEMORANDUM FOR JENNIFER SHASKY CALVERY
DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK

FROM: Marla A. Freedman
Assistant Inspector General for Audit

SUBJECT: Referral of Potential OFAC Violations by Three Banks to
OFAC and OCC

The purpose of this memorandum is to advise your office that we provided certain Suspicious Activity Reports (SAR) to the Office of Foreign Assets Control (OFAC) and the Office of the Comptroller of the Currency (OCC). As background, during our ongoing audit of the Financial Crimes Enforcement Network (FinCEN) and OFAC's use of blocked transaction reports for suspicious activity reporting, we identified 387 SARs that describe transactions processed by the filing institution that potentially violated an OFAC sanctions program. The SARs were filed by [REDACTED] (383 SARs), [REDACTED] (2 SARs), and [REDACTED] (2 SARs). The 387 SARs described either (1) transactions that were initially blocked or rejected but then were resent with the suspicious terms omitted or altered and processed by the bank (318 SARs) or (2) instances where the bank blocked or rejected transactions but processed other similar, or almost identical, related transactions (69 SARs). We referred the SARs to OFAC for a possible determination of enforcement action in connection with its administration of foreign sanctions programs. We referred the SARs to OCC for consideration in conducting its OFAC compliance examinations of the three banks.

The 387 SARs at issue are listed in Attachments 1 and 2. Attachment 1 lists the SARs where a blocked or rejected transaction was resent and processed, and Attachment 2 lists the SARs where the bank had blocked or rejected a transaction but reported that other similar transactions were processed.

We provided OFAC and OCC with these SARs under the authority of the Bank Secrecy Act and applicable regulations.¹ These provisions provide for sharing of information, in this case with OFAC and OCC, where the information may prove useful in OFAC's administration of foreign sanctions programs, and with OCC for

¹ 31 U.S.C. § 5311 and 31 C.F.R. 1010.950 (d)

Sensitive But Unclassified

Sensitive But Unclassified

Page 2

consideration in its OFAC compliance examinations of the three banks. Further, we advised OFAC and OCC of the need to protect the information and ensure that data will remain exempted with disclosure.²

If you have any questions, please contact me at 202-927-5400 or Sharon Torosian, Audit Director, at (617) 223-8638.

Attachments

cc: Krista Marting, Program Analyst, Management Programs Division, Office of Financial Management,
Becky Martin, Assistant Director, Office of Financial Management
Cynthia Clark, Deputy Chief Counsel, FinCEN
Rich Delmar, Counsel to the Inspector General

² 31 U.S.C. § 5319 and 5 U.S.C. § 552

Sensitive But Unclassified



OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Sensitive But Unclassified

October 17, 2013

OIG-CA-14-001

MEMORANDUM FOR ADAM J. SZUBIN
DIRECTOR
OFFICE OF FOREIGN ASSETS CONTROL

FROM: Marla A. Freedman
Assistant Inspector General for Audit

SUBJECT: Referral of Potential OFAC Violations by Three Banks

During our ongoing audit of the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control's (OFAC) use of blocked transaction reports for suspicious activity reporting, we identified 387 Suspicious Activity Reports (SARs) that describe transactions processed by the filing institutions that potentially violated an OFAC sanctions program. The SARs were filed by [REDACTED] (383 SARs), [REDACTED] (2 SARs), and [REDACTED] (2 SARs). The 387 SARs described either (1) transactions that were initially blocked or rejected but then were resent with the suspicious terms omitted or altered and processed by the bank (318 SARs) or (2) instances where the bank blocked or rejected transactions but processed other similar, or almost identical, related transactions (69 SARs). As discussed with Tyler Hand, Assistant Chief Counsel, Enforcement, we are referring these potential violations to your office for appropriate enforcement action.

The 387 SARs at issue are listed in Attachments 1 and 2. Attachment 1 lists the SARs where a blocked or rejected transaction was resent and processed, and Attachment 2 lists the SARs where the bank had blocked or rejected a transaction but reported that other similar transactions were processed. We are providing copies of the SARs to Luke Ballman, Senior Advisor for Legislative Affairs separately.

As an example of a SAR where a blocked or rejected transaction was resent and processed, the narrative from a SAR that [REDACTED] filed on November 8, 2012, stated:

Sensitive But Unclassified

Page 2

"[REDACTED] is filing this SAR because a client of a [REDACTED] foreign correspondent bank customer sent a payment that was blocked/rejected by [REDACTED]'s internal OFAC monitoring systems but later sent a similar payment that did not contain the information that triggered the [REDACTED] OFAC rejection/block in the original payment.

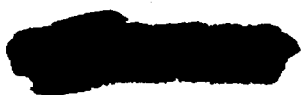
On September 22, 2010 [REDACTED] attempted to wire \$ [REDACTED] to an entity named [REDACTED]. The payment details read [REDACTED]. [REDACTED] is an island that is considered part of [REDACTED] rejected the payment on September 24, 2010 because it appeared to be prohibited by OFAC regulations.

On September 24, 2010 [REDACTED] this time using their account at [REDACTED] account, originated a second \$ [REDACTED] wire transfer to benefit [REDACTED]. However, this time the payment details read [REDACTED]. The wire was processed straight through and was not stopped in [REDACTED]'s OFAC filters because it made no reference to Iran or any other sanctioned country or entity/person." (Attachment 1, OIG No. 60, BSA ID [REDACTED])

As an example of a SAR where the bank had blocked or rejected a transaction but reported that other similar transactions were processed, the narrative from a SAR that [REDACTED] filed on January 22, 2010, stated:

"[REDACTED] is reviewing OFAC blocked or rejected transactions in the six months preceding this filing to identify additional payments, if any, involving the account number of the entity that caused the original payment to be rejected or blocked where the account number is now affiliated with a different named entity.

On June 15, 2009 [REDACTED] a client of [REDACTED] Commercial bank account number [REDACTED] tried to wire a \$920.00 payment to a [REDACTED] a client of [REDACTED] Bank account number [REDACTED]. [REDACTED] rejected the payment because of [REDACTED] Rep w/shop's apparent affiliation with [REDACTED] and [REDACTED] are both [REDACTED] foreign correspondent banking clients. [REDACTED] has located 2 [REDACTED] on June 5, 2009 and July 16, 2009 for \$48,000 and \$26,850, respectively. The payments were made by [REDACTED] and [REDACTED] both clients of [REDACTED]. The payments benefited an entity named [REDACTED] Rep w/shop account number [REDACTED], a client of [REDACTED]. The wire payments were processed straight through



Sensitive But Unclassified

Page 3

and were not stopped in [REDACTED]'s OFAC filters because they made no reference to [REDACTED] [REDACTED] or any other sanctioned country or entity/person."
(Attachment 2, OIG No. 1, BSA ID [REDACTED])

As background, we identified the 387 transactions through a review of SARs filed in calendar years 2010, 2011, and 2012 using the following word search criteria: OFAC, SDN, SDGT, Block, Blocked, and Blocking. Through this word search criteria, we identified a total of 1,474 SARs, of which 387 SARs are the subject of this memorandum.

Please be advised that we are providing the SARs to you under the authority of the Bank Secrecy Act and applicable regulations.¹ These provisions allow sharing of this information with OFAC, as it will prove useful in the Director of OFAC's investigation of potential regulatory violations of sanctions. In this regard, we request that your office protect the information and ensure that the reports and the data contained therein are exempt from disclosure.² We are sending a similar memorandum to the Office of the Comptroller of the Currency for its consideration in conducting OFAC compliance examinations of the three banks. We are also notifying FinCEN that we have provided these SARs to OFAC.

If you have any questions, please contact me at 202-927-5400 or Sharon Torosian, Audit Director, at (617) 223-8638.

Attachments (Copies of Listed SARs Provided Separately)

cc: Luke Ballman, Senior Advisor for Legislative Affairs
Richard Delmar, Counsel to the Inspector General

¹ 31 U.S.C. § 5311 and 31 C.F.R. 1010.950 (d)

² 31 U.S.C. § 5319 and 5 U.S.C. § 552

Sensitive But Unclassified

100

100



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Sensitive But Unclassified

OFFICE OF
INSPECTOR GENERAL

October 17, 2013

OIG-CA-14-002

MEMORANDUM FOR THOMAS J. CURRY
COMPTROLLER OF THE CURRENCY

FROM: Marla A. Freedman
Assistant Inspector General for Audit

SUBJECT: Referral of Potential OFAC Violations by Three Banks

As discussed with Laura McAuliffe, Senior Advisor, OIG/GAO Liaison, we are referring the following information about potential Office of Foreign Assets Control (OFAC) sanction program violations to the Office of the Comptroller of the Currency (OCC). We are providing this information for use by OCC in conducting OFAC compliance examinations of [REDACTED], and [REDACTED]. We also referred these potential violations to OFAC.

Specifically, during an ongoing Office of Inspector General audit of the Financial Crimes Enforcement Network (FinCEN) and OFAC's use of blocked transaction reports for suspicious activity reporting, we identified 387 Suspicious Activity Reports (SARs) that describe transactions processed by the filing institution that potentially violated an OFAC sanctions program. The SARs were filed by [REDACTED] (383 SARs), [REDACTED] (2 SARs), and [REDACTED] (2 SARs). The 387 SARs described either were (1) transactions that were initially blocked or rejected but then were resent with the suspicious terms omitted or altered and processed by the bank (318 SARs) or (2) instances where the bank blocked or rejected transactions but processed other similar, or almost identical, related transactions (69 SARs).

The 387 SARs at issue are listed in Attachments 1 and 2. Attachment 1 lists the SARs where a blocked or rejected transaction was resent and processed, and Attachment 2 lists the SARs where the bank had blocked or rejected a transaction but reported that other similar transactions were processed.

As background, we identified the 387 transactions through a review of SARs filed in calendar years 2010, 2011, and 2012 using the following word search criteria: OFAC, SDN, SDGT, Block, Blocked, and Blocking. Through this word search

Sensitive But Unclassified

Sensitive But Unclassified

Page 2

criteria, we identified a total of 1,474 SARs, of which 387 SARs are the subject of this memorandum.

Please be advised that we are providing the SARs to you under the authority of the Bank Secrecy Act and applicable regulations.¹ These provisions allow sharing of this information with OCC for appropriate regulatory purposes, including oversight of the banks' compliance with OFAC rules and requirements. In this regard, we request that your office protect the information and ensure that the reports and the data contained therein are exempt from disclosure.² We are also notifying FinCEN that we have provided these SARs to OCC.

If you have any questions, please contact me at 202-927-5400 or Sharon Torosian, Audit Director, at (617) 223-8638.

Attachments (Copies of Listed SARs Provided Separately)

cc: Laura McAuliffe, Senior Advisor, OIG/GAO Liaison
Rich Delmar, Counsel to the Inspector General

¹ 31 U.S.C. § 5311 and 31 C.F.R. 1010.950 (d)

² 31 U.S.C. § 5319 and 5 U.S.C. § 552

Sensitive But Unclassified

SENSITIVE BUT UNCLASSIFIED (SBU)



SBU Cover Sheet

**For further information, refer to the
Treasury Security Manual (TD P 15-71) at
<http://intranet.treas.gov/security/>**

TD F 15-05.11 (3/07)



SENSITIVE BUT UNCLASSIFIED

Audit Report



OIG-13-016

Management Report for the Audit of the Financial Management Service's Fiscal Years 2012 and 2011 Schedules of Non-Entity Government-wide Cash

November 26, 2012

Office of Inspector General

Department of the Treasury

This document belongs to the Department of the Treasury Office of Inspector General. It may not be released without the express permission of the Office of Audit. Refer requests and inquiries for the document to: Michael Fitzgerald, as noted in the transmittal letter.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 26, 2012

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

FROM: Michael Fitzgerald
Director, Financial Audits

SUBJECT: Management Report for the Audit of the Financial
Management Service's Fiscal Years 2012 and 2011
Schedules of Non-Entity Government-wide Cash— —
SENSITIVE BUT UNCLASSIFIED

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 Government-wide Cash (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 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 duties are effectively segregated; and 5. Contingency planning protects information resources, minimizes the risk of unplanned interruptions, and provides for recovery

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-13-014, dated November 16, 2012).

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Page 2

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 GWC and the reliability of key systems." KPMG LLP issued the accompanying sensitive but unclassified management report to provide the specific findings and recommendations pertaining to this significant deficiency.

Due to the sensitive nature of the information contained in the accompanying management report, it has been designated as Sensitive But Unclassified in accordance with the Department of the Treasury Security Manual (Treasury Department Publication 15-71) Chapter III, Section 24. Recipients of this report must not, under any circumstances, show or release its contents for purposes other than official review. It must be safeguarded to prevent publication or other improper disclosure of the information it contains.

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

SENSITIVE BUT UNCLASSIFIED



SENSITIVE BUT UNCLASSIFIED

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 Government-wide Cash (GWC) of the U.S. Department of the Treasury's (Treasury) Financial Management Service (FMS) as of September 30, 2012 and 2011 (hereinafter referred to as the Schedules), 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 GWC. In planning and performing our fiscal year (FY) 2012 audit, we considered FMS' internal control over financial reporting related to GWC by obtaining an understanding of the design effectiveness of FMS' internal control related to GWC, determining whether internal controls related to GWC 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 GWC. Accordingly, we do not express an opinion on the effectiveness of FMS' internal control over financial reporting related to GWC. 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 GWC 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 GWC that might be deficiencies, significant deficiencies, or material weaknesses. In our FY 2012 audit, we did not identify any deficiencies in

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

SENSITIVE BUT UNCLASSIFIED



internal control over financial reporting related to GWC 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 GWC 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 fiscal year (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 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:

- CASHLINK II,
- Secure Payment System (SPS),
- Central Accounting and Reporting System (CARS), and
- Treasury Check Information System (TCIS).

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;
- Treasury Receivable and Accounting Collection System (TRACS); and
- Payments, Claims and Enhanced Reconciliations (PACER) On-Line.

We identified 11 control deficiencies, of which 7 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 data 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 control 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. We also found management had delayed the status of the completion of TCIS POA&M milestones in FY 2012. Management proactively reported this weakness and has begun developing corrective actions.

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 and SPS 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, PACER Online, 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 environment. 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 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

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.



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 contingency planning weaknesses related to PAM and RO Payments. However, we found that the backup controls detailed in the SPS System Security Plan (SSP) do not reflect the primary 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.

This report is intended solely for the information and use of 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

SENSITIVE BUT UNCLASSIFIED

U.S. Department of the Treasury Financial Management Service Non-Entity Government-wide Cash

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

Table of Contents

BACKGROUND	7
CONCLUSION	8
DETAILED FINDINGS AND RECOMMENDATIONS	9

Appendices

APPENDIX I – AUDIT METHODOLOGY & CRITERIA.....	27
APPENDIX II – RISK RATING OF DETAILED FINDINGS.....	30
APPENDIX III – STATUS OF PRIOR YEAR FINDINGS	32
APPENDIX IV – LIST OF ACRONYMS	34

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

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 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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

CONCLUSION

Although we found that FMS made progress in several areas to address the prior year significant deficiency, FMS did not consistently implement NIST and Treasury recommended guidance across all general IT control environments or comply with FMS' policies. Specifically, we identified 7 new control weaknesses and made 10 recommendations spanning four general IT environments, which are the Treasury Web Application Infrastructure (TWAI), residing at the Federal Reserve Bank; the FMS mainframe environments; the Mid-Tier UNIX platform, which is managed by the BPD; and the CASHLINK 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 five 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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

DETAILED FINDINGS AND RECOMMENDATIONS

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).*

In FY 2011, we evaluated mainframe access controls and found several instances of excessive access to the mainframe environment.

In FY 2012, we found that FMS has not implemented corrective actions to remediate Findings 1-3 of this report. KPMG inquired of the Mainframe Engineering Division (MED) team and noted that FMS has developed an overall approach to identify the current mainframe access levels to programs, datasets, resources, and batch job submissions and to remove invalid access. KPMG noted that a separation of duties policy that details approved access levels and privileges by job function was missing from FMS' approach. As a result, management may not adjust access in a manner consistent with the concept of least privileges.

In addition, KPMG and MED discussed the status of the nine prior recommendations, and KPMG determined that these recommendations were not addressed. Management plans to implement corrective actions in FY 2013. As a result, this finding remains open.

Criteria

FMS Entity-Wide IT Standards Manual, Section 3, Roles and Responsibilities, Section 2, Separation of Roles and Responsibilities, states:

The principle of separation of duties requires the assignment of portions of security-related tasks to several individuals. This ensures no single individual has total control of the system's security mechanisms; therefore, no one individual can completely compromise the system. Separation of duties should be implemented using the security principle of least privilege. The concept of least privilege requires that users and processes in a system should have the least number of privileges for the least amount of time to perform assigned tasks.

FMS Entity-Wide IT Standards Manual, S 201, Access Control, Section 2, Account Management, states:

IT system owners and IT resource owners are required to perform periodic reviews, at least annually, of FMS user roles/accounts/profiles. This review may include compliance with least privilege and separation of duties principles. All requests for access and account modification should be documented electronically, appropriately approved, and retained.

FMS Entity-Wide IT Standards Manual, S 205, Configuration Management, Section 5, Access Restrictions for Change, states:

The automated change-tracking tool uses automated mechanisms (password requirements) to enforce access restrictions and support auditing of the enforced actions. Access audit files are maintained. The

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

System Owner approves the individual requests for system access. The E-ICAM process these requests and provide the appropriate logical access approved by the System Owner.

Recommendations

Develop and implement corrective actions to address the nine recommendations related to this finding that we made in the FY 2011 SBU Report on Non-Entity Government-wide Cash: Information Technology Controls over Systems Managed by FMS and Third Parties, issued as OIG-12-025. Refer to recommendations #1-9.

2. *Separation of duties principles were violated by granting conflicting access to critical resources on the FMS IBM mainframe environment (Repeat Condition).*

In FY 2011, we evaluated separation of duties for the TRACS, STAR, PACER Online, RO Payments, and PAM applications. We found that these mainframe applications had individuals with write access to both development and production datasets in violation of FMS' IT security policy to separate incompatible functions.

As noted in Finding 1, FMS has not implemented corrective actions to remediate this finding. Management plans to implement corrective actions in FY 2013. In addition, KPMG and MED discussed the status of the three prior-year recommendations, and KPMG determined that these recommendations were not addressed. As a result, this finding remains open.

Criteria

The FMS Entity-Wide IT Security Standards Manual, Section 3, *Roles and Responsibilities*, Section 3.2, *Separation of Roles and Responsibilities*, states:

The principle of separation of duties requires the assignment of portions of security related tasks to several individuals. This ensures no single individual has total control of the system's security mechanisms; therefore, no one individual can completely compromise the system. Separation of duties should be implemented using the security principle of least privilege. The concept of least privilege requires that users and processes in a system should have the least number of privileges for the least amount of time to perform assigned tasks.

Recommendations

Develop and implement corrective actions to address the three recommendations related to this finding that we made in the FY 2011 SBU Report on Non-Entity Government-wide Cash: Information Technology Controls over Systems Managed by FMS and Third Parties, issued as OIG-12-025. Refer to recommendations #10-12.

3. *FMS did not adequately restrict access over mainframe batch job submission (Repeat Condition).*

In FY 2011, we reported that batch jobs could be submitted without first providing passwords for many ACIDs, which could allow an individual to elevate his/her access privileges, update datasets, and potentially avoid detection.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

As noted in Finding 1, FMS has not implemented corrective actions to remediate this finding. Management plans to implement corrective actions in FY 2013. In addition, KPMG and MED discussed the status of the two prior-year recommendations, and KPMG determined that these recommendations were not addressed. As a result, this finding remains open.

Criteria

FMS Entity-Wide IT Standards Manual, S 201, Access Control, Section 2, *Account Management*, states:

IT system owners and IT resource owners are required to perform periodic reviews, at least annually, of FMS user roles/accounts/profiles. This review may include compliance with least privilege and separation of duties principles. All requests for access and account modification should be documented electronically, appropriately approved, and retained.

FMS Entity-Wide IT Standards Manual, Section 3, *Roles and Responsibilities*, Section 2, *Separation of Roles and Responsibilities*, states:

The principle of separation of duties requires the assignment of portions of security-related tasks to several individuals. This ensures no single individual has total control of the system's security mechanisms; therefore, no one individual can completely compromise the system. Separation of duties should be implemented using the security principle of least privilege. The concept of least privilege requires that users and processes in a system should have the least number of privileges for the least amount of time to perform assigned tasks.

Recommendations

Develop and implement corrective actions to address the two recommendations related to this finding that we made in the FY 2011 SBU Report on Non-Entity Government-wide Cash: Information Technology Controls over Systems Managed by FMS and Third Parties, issued as OIG-12-025. Refer to recommendations #13-14.

4. *Separation of duties for the UNIX Mid-Tier environments is not documented for sensitive users.*

For the UNIX Mid-Tier environments that host SPS, FMS and BPD management have not identified incompatible duties for sensitive users as required by the FMS Entity-Wide IT Security Standards Manual; therefore, we could not determine if policies were implemented to segregate these duties. Sensitive users include system administrators, DBAs, developers, change management support, and computer operations personnel.

During our testing associated with the FY 2012 audit, we found that there were many group accounts established on UNIX Mid-Tier environments. We obtained and inspected system security plans (SSPs) for SPS and its supporting general support system (GSS) and found no documentation detailing the following:

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

- Description, purpose, and approval of these groups residing on the UNIX Mid-Tier development, test, and production environments;
- Privileges and actions that each group can perform;
- Job functions and sensitive roles assigned to each group; and
- Process to approve, log, and monitor these groups.

Additionally, we inquired of several FMS and BPD employees regarding the implementation of separation of duties controls for sensitive users and obtained differing views of the controls in place. Specifically, we found the following:

- FMS management was unable to define the various development and test groups across the SPS environment. Since management has not defined the SPS Mid-Tier groups, we were unable to test for the appropriateness of access across the development, production, and test environments.
- The process to approve, manage, and monitor DBA access across the UNIX Mid-Tier environments has not been documented. Moreover, FMS could not demonstrate that the privileges in the development, test, and production environments given to individuals with existing DBA roles and were commensurate with their job duties..

FMS' SPS UNIX Mid-Tier support is provided by BPD, and this environment is maintained in Parkersburg, West Virginia. This finding is similar to the separation of duties weaknesses for the mainframe environment (refer to Finding 2 above). BPD is aware of and is in the process of remediating known separation of duties weaknesses for this environment. Furthermore, management has not documented in detail within their system security plans for SPS and GSS how incompatible duties will be separated amongst sensitive users.

A lack of segregation of duties is a factor related to information systems that may increase the risk of fraud. Without documenting how separation of duties is implemented, there is no clear central understanding amongst management how incompatible duties are prevented from occurring. This may lead to granting individuals incompatible roles with the ability to circumvent internal controls designed to detect and prevent unauthorized access and changes to production data.

Criteria

The **FMS Entity-Wide IT Security Standards Manual**, Section 3, *Roles and Responsibilities*, Section 3.2, *Separation of Roles and Responsibilities*, states:

The principle of separation of duties requires the assignment of portions of security related tasks to several individuals. This ensures no single individual has total control of the system's security mechanisms; therefore, no one individual can completely compromise the system. Separation of duties should be implemented using the security principle of least privilege. The concept of least privilege requires that users and processes in a system should have the least number of privileges for the least amount of time to perform assigned tasks.

NIST SP 800-53 Revision 3, states:

Access Control Policy and Procedures (AC-1)

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]:

- a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Separation of Duties (AC-5)

The organization:

- a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
- b. Documents separation of duties; and
- c. Implements separation of duties through assigned information system access authorizations.

Least Privilege (AC-6)

The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish.

Recommendations

We recommend that FMS management:

1. Develop a segregation of duties (SOD) matrix that complies with the IT security standards from FMS and NIST for sensitive users across the UNIX Mid-Tier environments and use this matrix when assigning access to groups or creating new groups through the change control process.
 2. Analyze existing groups on the UNIX Mid-Tier environments and document the following:
 - a. Description, purpose, and approval of each existing UNIX Mid-Tier group;
 - b. Privileges and actions that each group can perform;
 - c. Job functions and sensitive roles assigned to each group; and
 - d. Process to approve, log, and monitor of groups.
 3. Remove any inappropriate access that does not comply with the SOD matrix.
5. *FMS does not monitor privileged programs that bypass mainframe security (Repeat Condition).*

In FY 2011, we reported that FMS and the Mainframe Engineering Division (now referred to as the Data Services Branch) management did not have a list of privileged programs that management had approved as described in the NIST SP 800-53 Revision 3, CM-8, Information System Component Inventory. Additionally, FMS did not implement an automatic tool to alert Mainframe Engineering Division management when new privileged programs were added to the mainframe to determine if the addition was approved, appropriate, and safe as described for “High Impact” systems in NIST SP 800-53, Revision 3, CM-8 (3), Information System Component Inventory, Control Enhancement 3.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

In FY 2012, we found that FMS completed corrective actions to manage privileged programs as of June 29, 2012; however, FMS' corrective actions did not completely resolve the prior year issue over privileged programs. Specifically, we found the following:

1. In FY 2011, we recommended that FMS develop an authoritative inventory of management-approved privileged programs and confirm that existing privileged programs are safe and required for successful operations of the Mainframe.

In FY 2012, FMS provided us with a list of seven privileged programs that management deemed necessary to monitor and review. However, there are hundreds of privileged programs within the FMS Mainframe environment; therefore, the list of seven privileged programs is not a complete, authoritative list. In addition, FMS could not demonstrate that management performed a comprehensive analysis over all of the programs to determine if they are safe, approved by management, and not modified without management approval.

Although FMS stated that they gain comfort over their privileged programs by vendor integrity statements and audit logging, FMS only provided one integrity statement from a vendor, which did not cover all the privileged programs from other vendors on the FMS mainframe. FMS also stated that they have integrity statements for all privileged programs; however, these statements could not be provided. Additionally, FMS could not demonstrate that audit logging occurs.

2. In FY 2011, we recommended that FMS develop change management procedures to monitor privileged programs.

In FY 2012, FMS stated that change management procedures existed for privileged programs; however, FMS could not provide us with the change management procedures to confirm that changes to privileged programs are safe, approved by management, and not altered without management's approval.

3. In FY 2011, we recommended that FMS implement an automated mechanism to track privileged programs and notify appropriate management when privileged programs are added or existing privileged programs are modified.

In FY 2012, FMS stated that they use CA-Scheduler to run jobs nightly to report any access by system programmers on the seven selected privileged programs only and mainframe management reviews this report daily. However, FMS could not demonstrate that audit logging was taking place and CA-Scheduler is a job scheduler tool (that directs when batch jobs should run) not an automatic tool that notifies management of unauthorized changes. FMS stated they are planning to implement a tool by December 2012 called CA-Auditor to report changes to privileged programs by using the freeze frame feature.³

³ Provides the capability to recover the mainframe server from backup by restoring the network server storage spaces.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

Due to the competing priorities with the consolidation of FMS and the BPD organizations, FMS management has not allocated the resources necessary to ensure that privileged programs are authorized and secure.

Without a complete, authoritative inventory of approved privileged programs, FMS management cannot confirm that the deployed privileged programs on FMS' mainframe are safe, approved by management, and have not been modified without management's approval. A systems programmer could bypass the mainframe security software by inserting a "backdoor" to mainframe security software and executing his/her malicious program in supervisor (full control) state. As the program executes outside of the mainframe security software with supervisor state privileges, the individual's actions would largely be undetectable and not audited by CA-Top Secret. With these powerful privileges, the individual could potentially alter check or other payment files and leave minimal audit trails.

Criteria

The **FMS Entity-Wide IT Security Standards Manual, Standard 205: Configuration Management**, states:

Information System Component Inventory (CM-8)

Control: The organization develops, documents, and maintains an inventory of information system components/configuration items.

Information System Component Inventory Control Enhancement (CM-8(3))

For High systems, the organization employs automated mechanisms at all times to detect the addition of unauthorized components/devices into the information system.

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

Information System Component Inventory (CM-8)

Control: The organization develops, documents, and maintains an inventory of information system components that:

- a. Accurately reflects the current information system;
- b. Is consistent with the authorization boundary of the information system;
- c. Is at the level of granularity deemed necessary for tracking and reporting; and
- d. Is available for review and audit by designated organizational officials.

Information System Component Inventory Control Enhancement (CM-8(1))

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Information System Component Inventory Control Enhancement (CM-8(3))

Employs automated mechanisms to detect the addition of unauthorized components/devices into the information system.

Recommendations

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

Since FMS closed this finding in Treasury's Joint Audit Management Enterprise System, we repeat the following recommendations made in our FY 2011 report:

4. Develop a complete authoritative information system inventory of all management-approved privileged programs, and confirm that existing privileged programs are safe and required for successful operation of the mainframe.
5. Develop and implement change control procedures to monitor privileged programs to confirm that they were safe, approved by management, and had not been altered without management's approval.
6. Implement an automated mechanism to track the inventory of existing programs and notify appropriate officials when new privileged programs are added or existing privileged programs are modified.

6. *SPS audit and monitoring process need improvement.*

The current SPS audit capabilities and functions do not adhere to the Fiscal Service Baseline Security Requirements (BLSRs) and NIST SP 800-53, Revision 3, guidance as required for HIGH categorized systems. While SPS has controls to review business level transactions, it does not have any automated capabilities or any supporting processes to log and monitor security-relevant events.

During the design of SPS, FMS management did not adequately identify requirements and provide the capabilities to log and monitor security-related events to support the review and follow up of these type of events. In addition, management has not documented within their system security plan the specific security-related events that SPS should monitor on an on-going basis.

By not adhering to NIST guidance over audit log review policies, IT security personnel would be unable to identify and mitigate significant threats to the information system. Additionally, this could cause the Department of Treasury personnel to remain unaware of security incidents that have already taken place, leaving the system in a compromised state for an extended period.

Criteria

Fiscal Service BLSRs, dated June 5, 2012, prescribed the following:

Auditable Events: The organization:

- a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [identity of each user and device accessing or attempting to access an IT system; time and date of the access and the logoff; activities that might modify, bypass, or negate IT security safeguards; and security relevant actions associated with processing (TRE)];
- b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

c. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [identity of each user and device accessing or attempting to access an IT system; time and date of the access and the logoff; activities that might modify, bypass, or negate IT security safeguards; and Security-relevant actions associated with processing, immediately following an event. (FS)]

[Appropriate IT security auditing shall be enabled to support:

- Detection of intrusion attempts on the system
- Detection of denial of service attacks on the system
- Detection of unauthorized access and/or modification to data stored on the system
- Tracing users to actions

The system will, at a minimum, record the following types of events:

- Log on (success/failure)
- Account management (success/failure)
- Audit policy changes (success/failure)
- Audit system events (success/failure)
- Deletion of files and folders (directories) (success/failure)
- All actions by privileged users (system operators, system administrators, and security officers) such as password, file, and account changes (FS)]

[In addition to the events listed above, the security-relevant events captured in audit logs will be defined after analyzing business models, personnel requirements, assessing the impact of the architecture and the design alternatives. (FS)]

NIST SP 800-53, Revision 3, control AU-2 requires the following for systems with a high categorization:

The organization:

- a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*];
- b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
- c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].

Control Enhancements:

- (3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

(4) The organization includes execution of privileged functions in the list of events to be audited by the information system.

Recommendations

We recommended in the FY 2012 FISMA report, issued as OIG-13-008⁴, that FMS undertake three corrective actions to address the weaknesses in the SPS audit and monitoring process. See FISMA Recommendations #14, 15, and 16.

7. *FMS' oversight of its systems and mission data being managed by service providers needs improvement.*

FMS utilizes many service providers to manage its IT systems, processes, and security controls. During our FY 2012 audit, we identified the following entities:

- PNC Financial Services manages the CA\$HLINK II application at its site in Riverdale, Maryland.
- BPD manages the UNIX Mid-Tier environment that maintains and processes the SPS application in Parkersburg, West Virginia.

Although the Fiscal Service Baseline Security Requirements (BLSR) direct system owners, Information System Security Officers (ISSO), and other applicable field-personnel to assess the security controls of service providers and to update the system security plans accordingly, FMS does not monitor IT security control compliance of its service providers and has not addressed the risks or implemented compensating controls. FMS does not have procedures on how FMS should monitor the operating effectiveness of its service providers' controls, or a process in place to ensure that its service providers (BPD and PNC Financial Services) are implementing its IT security controls as prescribed by NIST SP 800-53, Revision 3.

Specifically we found that system security plans or additional FMS procedures do not establish the security roles and responsibilities between:

- FMS and PNC Financial Services for CA\$HLINK II; and
- FMS and BPD for employed controls for Mid-Tier UNIX and SPS.

In addition, a similar finding was reported in the during FY 2009 audit.

Criteria

The **Fiscal Service BLSRs** state the following in the "Monitoring" section CA-2_01 and PL-2_02: "The organization assesses the security controls in the information system (at least annually) to determine the extent to which the controls are implemented correctly, operating as intended, and

⁴ OIG-13-007, The Department of the Treasury Federal Information Security Management Act Fiscal Year 2012, November 9, 2012

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

producing the desired outcome with respect to meeting the security requirements for the system (CA-2_01).”

Additionally, Section PL-02_02 also states that “Updates the security plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.”

NIST SP 800-53 Revision 3, section 2.4, page 12, states that “Organizations are responsible and accountable for the *risk* incurred by use of services provided by service providers and address this risk by implementing compensating controls when the risk is greater than the authorizing official or the organization is willing to accept.”

In addition, NIST SP 800-53, Revision 3, prescribes the following:

SA-9 External Information System Services

Control: The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. Monitors security control compliance by external service providers.

Recommendations

We recommend that FMS management:

7. Document the following in the CA\$HLINK II, Mid-Tier UNIX, and SPS SSPs: (a) the security controls that are being performed by the service providers and (b) the FMS’ monitoring controls employed to determine that these employed controls are operating effectively.
 8. Develop an enforcement process to obtain assurance that the IT security controls employed by the service providers are operating effectively.
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.***

The UNIX Mid-Tier Platform, residing at the BPD in Parkersburg, West Virginia, hosts FMS’ SPS application. FMS is responsible for managing the SPS application-layer, while BPD controls and maintains the UNIX Mid-Tier platform. The applications and the platform have their own separate SSPs, authorizations to operate (ATOs), and POA&Ms.

FMS and BPD need to improve their coordination for the orderly transfer of POA&M items relating to UNIX Mid-Tier platform-specific weaknesses affecting FMS applications, per the FMS Transferring POA&M Items Standard. We found several platform-specific weaknesses initially tracked in the POA&Ms for the SPS application that were not transferred in a timely manner to BPD

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

for inclusion in the UNIX Mid-Tier POA&M, thereby not enabling the monitoring controls necessary to ensure prompt remediation. KPMG noted this issue is similar to the FY 2009 finding related to “insufficient information is received from service providers.”

Specifically, we found that seven platform-specific weaknesses in the SPS POA&M were identified in the August 11, 2011 Security Assessment Report, that were not transferred to the UNIX Mid-Tier POA&M as of June 19, 2012.

Delays in the transfer of POA&M items from FMS to BPD occurred due to competing initiatives involved with the Bureau of the Fiscal Service consolidation. In addition, the current FMS Transferring POA&M Items Standard does not include specified time frames for the orderly transfer of POA&M items across organizations.

By not maintaining updated POA&Ms, including all identified security weakness, management's ability to monitor aggregated risks to its systems as well as prioritize limited IT resources to address known security weaknesses may be hindered. Additionally, without a current centralized list of all known security weaknesses, management may not be able to identify reoccurring security issues across multiple systems that could be remediated by a department-wide strategic corrective action plan.

Criteria

The **FMS Transferring POA&M Items Standard (Pr-204.1)**, dated October 10, 2008, states:

1. The Information System Security Officer (ISSO) of the source IT system, working through their Mission Assurance Facilitator, contacts the ISSO and MA [Mission Assurance] facilitator of the destination IT system, providing background source documentation as well as their internal review results, requesting the destination IT system complete a separate review to determine if the mitigation of the vulnerability is within the destination IT system's boundary.
2. ISSO and technical and support staff of the destination IT system assisted by the Mission Assurance facilitator complete a thorough review and analysis of the vulnerability and its supporting documentation within ten (10) working days of the transfer request to establish their view and document their results.

The **FMS Entity-Wide IT Security Standards Manual, Standard 204: Certification, Accreditation, and Security Assessments**, states:

CA-5 Plan of Action and Milestones

The organization updates existing plan of action and milestones at least quarterly, based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

P-POA&M.11 - Bureaus shall ensure that all new weaknesses are entered into appropriate POA&Ms within: 1) one month of identification for program-level weaknesses and those for FIPS 199 HIGH systems, and 2) two months for weaknesses for other systems.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

Recommendations

We recommend that FMS management:

9. FMS and BPD improve their coordination for the orderly transfer of POA&M items across the organizations to ensure timely remediation of weaknesses.
 10. Enhance the FMS Transferring POA&M Items Standard to require the orderly transfer of POA&Ms items across the organizations within specified time frames.
- 9. *SPS configuration management process lacks adequate information and robust control to address Treasury requirements.***

The SPS Configuration Management Plan does not establish operational requirements as well as document the following elements: mandatory configuration settings for the information system components to reflect the most restrictive mode; list of authorized and unauthorized programs; and mechanisms to verify configuration settings and respond to unauthorized changes. The selected system Configuration Management Plan did not provide a clear distinction between program change control and system configuration management processes identified in the FMS Entity-Wide IT Standards. The lack of clarity and baseline features within the selected system Configuration Management Plan was overlooked by FMS management when establishing the plan.

Both the FMS Entity-Wide IT Standards and the SPS Configuration Management Plan outline roles and responsibilities at a high level, but do not provide sufficient detail regarding workflow, task ownership, and management oversight. Additionally, the content of the SPS Configuration Management Plan does not provide a clear distinction between program change control and system configuration management processes; rather, it outlines at a high level the method to request, approve, test, and implement planned programmatic changes. The lack of clarity in these governing standards has caused confusion in understanding what the SPS configuration baseline contains.

Managing the configuration settings of the system is an essential control element within Treasury's risk management and IT security controls framework for the stability, integrity, confidentiality, and availability of the system to perform mission tasks. Without an effective configuration management process at the entity and system level, a clearly defined standard settings documentation or baseline for SPS, and controls to prevent the baseline from unauthorized changes, management cannot provide sufficient control to enforce and maintain settings in the system. This will hinder FMS' attempts to validate and enforce SPS configuration settings to prevent unauthorized access, changes, and disclosure to the system and data, which may ultimately introduce risk into the security posture of the SPS environment.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

Criteria

FMS Entity-Wide IT Standards, dated April 10, 2012, prescribe the following configuration management controls:

Baseline Configuration (CM-2)

Control Enhancement 1: The organization reviews and updates the baseline configuration of the information system annually; when required due to changes to the information system.

Control Enhancement 5: For High systems, the organization develops and maintains a list of Bureau approved software.

Additional FMS requirements applicable to CM-2

FMS ensures:

Changes to Configuration Items (CIs) are tracked.

Security baseline requirements are established for each FMS infrastructure component.

Baseline verifications with approved changes are implemented. Audits are conducted to verify that system performance and configuration are accurately identified in the baseline documentation. The configuration audit verifies that changes are fundamentally correct as specified in the configuration and technical documentation, and that trusted systems are consistent with the security policy of the system.

Configuration Settings (CM-6)

Control: For High systems, the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using an automated means to check that the security configuration settings of Bureau-installed/operated equipment are continually maintained in accordance with the applicable NIST-promulgated or other NIST 800-70 compliant checklists that reflect the most restrictive mode consistent with operational requirements.

Control Enhancement 2: For High systems, the organization employs automated mechanisms to respond to unauthorized changes to all configurable devices.

NIST SP 800-53, Revision 3, states the following:

Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings.

Recommendations

We recommended in the FY 2012 FISMA report, issued as OIG-13-008, that FMS management undertake three corrective actions to address the weaknesses in the SPS configuration management process. See FISMA Recommendations #29, 30, and 31.

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

Treasury Directive Publication (TD P) 85-01 Volume I and NIST SP 800-53, Rev. 3, require that bureaus conduct vulnerability scanning of their IT assets at least monthly, so that high-risk weaknesses identified are remediated in a timely manner.

During our FY 2012 testing, FMS and BPD management were unable to provide us with supporting documentation confirming that the SPS Internet Protocol (IP) addresses scanned from October 1, 2011 to June 30, 2012 were the actual IP addresses in production at the time of the vulnerability scans. Therefore, we were unable to test the effectiveness of the controls over vulnerability scanning and flaw remediation process for SPS, and we could not determine if vulnerability scans had been performed for the in-scope SPS server, if any vulnerabilities were identified, and if any corresponding corrective actions had been implemented.

With the combination of FMS and the BPD into the Bureau of the Fiscal Service, the threat management process has not been 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 SPS.

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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

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.

Control Enhancement 2 (CE 2): For High systems, the list of information system vulnerabilities scanned is updated at least semi-annually.

Control Enhancement 5 (CE 5): For High systems, the organization includes privileged access authorization to all information system components as applicable (e.g., OS, DB, WEB APP, etc.) for selected vulnerability scanning activities to facilitate more thorough scanning.

Control Enhancement 7 (CE 7): For High systems, the organization employs automated mechanisms at least annually to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

NIST SP 800-53 Revision 3, states:

RA-5 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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

SI-2 Flaw Remediation

The organization:

- a. Identifies, reports, and corrects information system flaws;
- b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
- c. Incorporates flaw remediation into the organizational configuration management process.

Control Enhancements:

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

Recommendations

We recommended in the FY 2012 FISMA report, issued as OIG-13-008, that the FMS Assistant Commissioner undertake two corrective actions to address the weaknesses in SPS threat management process. See FISMA Recommendations #20 and 21.

11. SPS system security plan does not reflect the primary backup process.

The SSP for SPS did not reflect the current and primary source of backups for the application. FMS management stated that the error was due to a management oversight when updating the SSP.

Failing to document an up-to-date baseline of security controls may have a negative effect on subsequent security activities. Specifically, FMS may not be able to implement, assess, authorize, and monitor the security controls properly for the selected systems; therefore, the system security controls may not be sufficient to protect the confidentiality, integrity, and availability of sensitive bureau information.

Criteria

NIST SP 800-53 Revision 3, states:

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

SENSITIVE BUT UNCLASSIFIED

Non-Entity Government-wide Cash:

Information Technology Controls Over Systems Managed by FMS and Third Parties

- 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 recommended in the FY 2012 FISMA report, issued as OIG-13-008, that FMS management undertake a corrective action to improve the SPS system security plan to include the primary backup testing controls. See FISMA Recommendation #13.

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.

SENSITIVE BUT UNCLASSIFIED

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*

SENSITIVE BUT UNCLASSIFIED

APPENDIX II – RISK RATING OF DETAILED FINDINGS

<u>Corresponding Finding in the “Detailed Findings and Recommendations” Section</u>	<u>Title of Finding</u>	<u>Risk Rating</u>
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

SENSITIVE BUT UNCLASSIFIED

Audit Methodology & Criteria

Appendix II

<u>Corresponding Finding in the “Detailed Findings and Recommendations” Section</u>	<u>Title of Finding</u>	<u>Risk Rating</u>
Finding 11	SPS system security plan does not reflect the primary backup process.	Low

SENSITIVE BUT UNCLASSIFIED

Status of Prior Year Findings

Appendix III

APPENDIX III – STATUS OF PRIOR YEAR FINDINGS

<u>FY 2011 Finding</u>	<u>Title of Finding</u>	<u>Action Complete</u>	<u>Action In Process</u>
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 in FY 2012 as 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.		X ⁵
Finding 7	Incomplete auditing and accountability controls have been implemented on TCIS.		X ⁶

⁵ 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.

⁶ FMS notified KPMG that it closed the TCIS auditing and accountability 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.

SENSITIVE BUT UNCLASSIFIED

Status of Prior Year Findings

Appendix III

<u>FY 2011 Finding</u>	<u>Title of Finding</u>	<u>Action Complete</u>	<u>Action In Process</u>
Finding 8	TCIS user accounts were not disabled within the timeframes set by FMS policy.	X	
Finding 9	FMS did not appropriately restrict physical access to the KROC Data Center and IT Command Center.	X	

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

List of Acronyms

Appendix IV

APPENDIX IV – LIST OF ACRONYMS

Acronym	Definition
AC	Access Control
ACID	Accessor ID
BFS	Bureau of the Fiscal Service
BPD	Bureau of Public Debt
BLSR	Baseline Security Requirements
DBA	Database Administrator
CARS	Central Accounting and Reporting System
CM	Configuration Management
CP	Contingency Planning
E-ICAM	Enterprise Identity, Credentialing, and Access Management
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
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GWC	Government-wide Cash
GSS	General Support System
ISSO	Information System Security Officer
IP	Internet Protocol
IT	Information Technology
JCL	Job Control Language
KROC	Kansas City Regional Operations Center
MED	Mainframe Engineering Division
NIST SP	National Institute of Standards and Technology Special Publication
OMB	Office of Management and Budget
PACER On-line	Payments, Claims and Enhanced Reconciliation
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
TCIS	Treasury Check Information System
TD P	Treasury Directive Publication
TMA	Treasury Managed Accounts

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

List of Acronyms

Appendix IV

Acronym	Definition
TRACS	Treasury Receivable and Accounting Collection System
TWAI	Treasury Web Application Infrastructure

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED (SBU)



SBU Cover Sheet

**For further information, refer to the
Treasury Security Manual (TD P 15-71) at
<http://intranet.treas.gov/security/>**

TD F 15-05.11 (3/07)



SENSITIVE BUT UNCLASSIFIED

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 document belongs to the Department of the Treasury Office of Inspector General. It may not be released without the express permission of the Office of Audit. Refer requests and inquiries for the document to: Michael Fitzgerald, as noted in the transmittal letter.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 29, 2012

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

FROM: Michael Fitzgerald
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— — SENSITIVE BUT UNCLASSIFIED

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 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).

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Page 2

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.

Due to the sensitive nature of the information contained in the accompanying management report, it has been designated as Sensitive But Unclassified in accordance with the Department of the Treasury Security Manual (Treasury Department Publication 15-71) Chapter III, Section 24. Recipients of this report must not, under any circumstances, show or release its contents for purposes other than official review. It must be safeguarded to prevent publication or other improper disclosure of the information it contains.

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

SENSITIVE BUT UNCLASSIFIED



SENSITIVE BUT UNCLASSIFIED

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.

SENSITIVE BUT UNCLASSIFIED



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:

- CASHLINK 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 CASHLINK 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

SENSITIVE BUT UNCLASSIFIED

**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

BACKGROUND	7
CONCLUSION	8
DETAILED FINDINGS AND RECOMMENDATIONS	9

Appendices

APPENDIX I – AUDIT METHODOLOGY & CRITERIA.....	15
APPENDIX II – RISK RATING OF DETAILED FINDINGS.....	18
APPENDIX III – STATUS OF PRIOR YEAR FINDINGS	20
APPENDIX IV – LIST OF ACRONYMS	21

SENSITIVE BUT UNCLASSIFIED

*Non-Entity Assets, Non-Entity Costs, and Custodial Revenue:
Information Technology Controls Over Systems Managed by FMS and Third Parties*

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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue: Information Technology Controls Over Systems Managed by FMS and Third Parties

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 CASHLINK 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.

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue: Information Technology Controls Over Systems Managed by FMS and Third Parties

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 (CASHLINK 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).

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue:

Information Technology Controls Over Systems Managed by FMS and Third Parties

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

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue:

Information Technology Controls Over Systems Managed by FMS and Third Parties

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 its 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:

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue: Information Technology Controls Over Systems Managed by FMS and Third Parties

- (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 JFICS 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

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue: Information Technology Controls Over Systems Managed by FMS and Third Parties

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

SENSITIVE BUT UNCLASSIFIED

Non-Entity Assets, Non-Entity Costs, and Custodial Revenue: Information Technology Controls Over Systems Managed by FMS and Third Parties

- 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.

SENSITIVE BUT UNCLASSIFIED REPORT

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.

SENSITIVE BUT UNCLASSIFIED REPORT

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*

SENSITIVE BUT UNCLASSIFIED REPORT

Audit Methodology & Criteria

Appendix I

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

SENSITIVE BUT UNCLASSIFIED REPORT

APPENDIX II – RISK RATING OF DETAILED FINDINGS

<u>Corresponding Finding in the “Detailed Findings and Recommendations” Section</u>	<u>Title of Finding</u>	<u>Risk Rating</u>
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

SENSITIVE BUT UNCLASSIFIED REPORT

Audit Methodology & Criteria

Appendix II

<u>Corresponding Finding in the “Detailed Findings and Recommendations” Section</u>	<u>Title of Finding</u>	<u>Risk Rating</u>
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

SENSITIVE BUT UNCLASSIFIED REPORT

Status of Prior Year Findings

Appendix III

APPENDIX III – STATUS OF PRIOR YEAR FINDINGS

<u>FY 2011 Finding</u>	<u>Title of Finding</u>	<u>Action Complete</u>	<u>Action in Process</u>
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.

SENSITIVE BUT UNCLASSIFIED REPORT

List of Acronyms

Appendix IV

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



DEPARTMENT OF THE TREASURY
WASHINGTON

October 30, 2008

INSPECTOR GENERAL

INFORMATION MEMORANDUM FOR SECRETARY PAULSON

FROM:

Eric M. Thorson
Inspector General

SUBJECT:

Management and Performance Challenges Facing the
Department of the Treasury (OIG-CA-09-001)

The Reports Consolidation Act of 2000 requires that we provide you with our perspective on the most serious management and performance challenges facing the Department of the Treasury, for inclusion in the Department's annual performance and accountability report.

This year, we are reporting two new challenges:

- Management of Treasury's New Authorities Related to Distressed Financial Markets
- Regulation of National Banks and Thrifts

Both of these challenges relate to the crises that began in the subprime mortgage market and spread more broadly into the U.S. and global financial markets.

We also continue to report four challenges from last year:

- Corporate Management
- Management of Capital Investments
- Information Security
- Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

We removed one previously reported challenge, Linking Resources to Results, based on the progress the Department has made in implementing managerial cost accounting in its operations.

Furthermore, as we have pointed out in the past, management and performance challenges do not always represent a deficiency in management or performance. Instead, they can represent inherent risks associated with Treasury's mission, organizational structure, or the environment in which it operates. In this regard, the Department can and should take steps to mitigate these challenges but may not be able to entirely eliminate them. As such, they require ongoing management attention.

Challenge 1 – Management of Treasury’s New Authorities Related to Distressed Financial Markets

Last year we reported as a matter of increasing concern the deterioration of the real estate market and its impact on the credit markets. With worsening conditions over the past year and the impact the subprime mortgage situation has had on the broader financial markets, we have elevated this concern to the most serious management and performance challenge facing the Department.

Treasury, along with the Federal Reserve and the Federal Housing Finance Agency (FHFA), has been dealing with multiple financial crises requiring unprecedented actions through the latter half of Fiscal Year 2008. In July 2008, Congress passed the Housing and Economic Recovery Act which gave Treasury broad new authorities to address the distressed financial condition of Fannie Mae and Freddie Mac. While the hope at the time was that Treasury would not need to exercise those authorities, less than 6 weeks later, FHFA put the two mortgage giants into conservatorship and Treasury agreed to purchase senior preferred stock in the companies, established a new secured line of credit available to the companies, and initiated a temporary program to purchase new mortgage-backed securities issued by the companies.

As the turmoil in the financial markets increased, Treasury and the Federal Reserve took a number of additional unprecedented actions including the rescue of Bear Stearns and American International Group (AIG). It became evident that a more systemic, comprehensive plan was needed to stabilize the financial markets. Treasury sought and obtained additional authorities through passage of the Emergency Economic Stabilization Act (EESA), which gave the Treasury Secretary \$700 billion in authority to, among other things: (1) purchase capital in qualifying U.S. controlled financial institutions; and (2) buy, maintain, and sell toxic mortgage-related assets from financial institutions. These authorities are intended to bolster credit availability and address other serious problems in the U.S. and world financial markets.

As of this writing, the Department has aggressively moved forward to make capital infusions through the purchase of senior preferred stock in nine large banks in an effort to loosen up the credit market. A number of others have subsequently sought to participate in the Capital Purchase Program. The Department is also implementing the mechanisms to carry out its other authorities and responsibilities for the Troubled Assets Relief Program (TARP). It plans to rely extensively on the private sector, initially with a small cadre of Treasury staff to exercise managerial control over TARP. With the hundreds of billions of dollars involved, the need to move quickly, and with so much of the program to be managed by financial agents and contractors, the risk is high that Treasury objectives will not be achieved or taxpayer dollars will be wasted. Accordingly, Treasury needs to ensure strong controls are in place and that its managerial oversight is effective.

Additionally, the Act provides for the appointment of a Special Inspector General to provide oversight of this program. It also directs the U.S. Government Accountability Office (GAO) to conduct ongoing monitoring and report on the program every 60 days. Having said that, it is important to keep in mind that the presence of a Special Inspector General and the work by GAO are not a substitute for sound internal controls and appropriate management stewardship of this critical program.

Also, while the structure and execution of the EESA is still unfolding, it appears that Treasury will be relying to some extent on the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS) to both evaluate their supervised institutions for participation in TARP and to monitor their compliance with the requirements for participation and the use of the capital that Treasury provides, including requirements related to limits on executive compensation. If this is to be effective, there will need to be close coordination between the Treasury team managing implementation of EESA, OCC, and OTS (as well as the other Federal Banking Agencies).

Going forward sound administration of the significant taxpayer dollars committed to this rescue effort will clearly be Treasury's most significant management challenge. Furthermore, given the rapidly changing conditions in the financial markets and the coming change in administrations, the importance of establishing a sustainable leadership team as quickly as possible to manage this program cannot be overstated.

Challenge 2 – Regulation of National Banks and Thrifts

Since September 2007, nine Treasury-regulated financial institutions failed with estimated losses to the deposit insurance fund exceeding \$10 billion. Predictions are that many more will fail before the economy improves. This is in sharp contrast to the relatively few and much smaller Treasury-regulated financial institutions that failed during the previous 5 years.

While there are many factors that have contributed to the current turmoil in the financial markets, Treasury's regulators, OCC and OTS, did not identify early or force timely correction of the unsafe and unsound practices by institutions under their supervision. The irresponsible lending practices by many institutions that contributed to the current crisis are now well recognized—including, degradation of underwriting standards, loan decisions based on factors other than the borrowers' ability to repay, and with the ready availability of investor financing, a mentality of "originate to sell" instead of the more prudent "originate to hold" permeated the industry. At the same time, financial institutions engaged in other high risk activities including high asset concentrations in areas such as commercial real estate, and over-reliance on unpredictable brokered deposits to fund rapid growth.

The banking industry will continue to be under pressure over the next several years. For example, OCC, OTS, and the other federal banking regulators recently reported that 2007 data for Shared National Credits (loan commitments of \$20 million or more that are shared by three or more federally supervised institutions) showed a large increase in volume during

the year, with shared credits now totaling \$2.8 trillion (a 22.6 percent increase over 2006). The regulators also reported a significant deterioration in quality of these credits. It has also been reported that the next substantial stress to financial markets will come from troubled credit card debt and auto loans, and this may significantly impact those financial institutions that previously had limited exposure to the subprime mortgage crises

Our office is mandated to look into Treasury-regulated bank failures that result in material losses to the deposit insurance fund. In this regard, during the last 6 months, we completed one review of the NetBank failure and are currently engaged in five. These reviews are useful in identifying the causes for failures and assessing the supervision exercised over a particular failed institution. It should be noted that OCC and OTS have been responsive to our recommendations for improving supervision. However, these reviews do not address supervisory effectiveness overall. It is therefore essential that OCC and OTS take a critical look at their respective (and collective) supervisory processes to identify why those processes did not prevent or better mitigate the unsafe and unsound practices that led to the current crisis and what can be done to better protect the financial health of the banking industry going forward.

Recognizing that the focus of EESA is on the current crisis, another consideration is the need for Treasury to identify, monitor, and manage *emerging* domestic and global systemic economic risks. It should be noted that these emerging risks may go beyond the current U.S. regulatory structure. Treasury, in concert with its regulatory partners, needs to diligently monitor regulated as well as unregulated products and markets for new systemic risks that may require action.

Challenge 3 – Corporate Management

Starting in 2004, we identified corporate management as an overarching management challenge. In short, Treasury needs to provide effective corporate leadership in order to improve performance as a whole. Inherent in this is the need for clear lines of accountability between corporate, bureau, and program office management; enterprise solutions for core business activities; and effective oversight of capital investments and information security. With nine bureaus and a number of program offices, Treasury is a highly decentralized organization. As we reported last year, the Department has made progress in building up a sustainable corporate control structure. The challenge continues to be maintaining emphasis on corporate governance, particularly as the Department develops the infrastructure to carry out its vastly expanded role in addressing the current economic crisis and as key management officials turnover with the change of administration.

Challenge 4 – Management of Capital Investments

Managing large capital investments, particularly information technology (IT) investments, is a difficult challenge facing any organization whether in the public or private sector. In prior years we have reported on a number of capital investment projects that either failed or had

serious problems. In light of this, with hundreds of millions of procurement dollars at risk, Treasury needs to exercise continuous vigilance in this area as it proceeds with its:

- (1) transition to a new telecommunications contract (TNet) under the General Services Administration's Networx program, a transition that has already experienced delays;
- (2) implementation of enhanced information security requirements; (3) the anticipated renovation of the Treasury Annex; and (4) other large capital investments.

During the last year, the Department reinstituted a governance board consisting of senior management officials to provide executive decision-making on, and oversight of, IT investment planning and management and to ensure compliance with the related statutory and regulatory requirements.

Challenge 5 – Information Security

While improvements have been made, by its very nature information security will continue to be a management challenge to the Department. Our Fiscal Year 2008 audit addressing the objectives of the Federal Information Security Management Act of 2002 (FISMA) and Office of Management and Budget (OMB) requirements found that Treasury's non-IRS bureaus made progress in improving information security controls and practices.

Notably, during the past year Treasury strengthened its inventory reporting and Plan of Action and Milestones (POA&M) processes for tracking and correcting security weaknesses. However, our audit found that (1) minimum security control baselines were not sufficiently documented, tested, and/or implemented as required; (2) computer security incidents were not consistently reported timely or correctly categorized; (3) common security configuration baselines were not fully compliant; and (4) federal desktop core configurations were not fully implemented. Treasury management has indicated its commitment to address these issues. It should be noted, however, that the annual FISMA review is not designed to detect all information security vulnerabilities.

Challenge 6 – Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

As reported in previous years, Treasury faces unique challenges in carrying out its responsibilities under the Bank Secrecy Act (BSA) and USA Patriot Act to prevent and detect money laundering and terrorist financing. While the Financial Crimes Enforcement Network (FinCEN) is the Treasury bureau responsible for administering BSA, a large number of federal and State entities participate in efforts to ensure compliance with BSA. These entities include the five federal banking regulators, the Internal Revenue Service (IRS), the Securities and Exchange Commission, the Department of Justice, and State regulators. Many of these entities also participate in efforts to ensure compliance with U.S. foreign sanction programs administered by Treasury's Office of Foreign Assets Control (OFAC).

The dynamics and challenges for Treasury of coordinating the efforts of multiple entities, many external to Treasury, are difficult. In this regard, FinCEN and OFAC entered into memoranda of understanding (MOU) with many federal and State regulators in an attempt to build a consistent and effective process. However, these MOUs are non-binding (and without penalty) and their overall effectiveness have not been independently assessed.

Furthermore, the Patriot Act has increased the types of financial institutions required to file BSA reports. In Fiscal Year 2007, nearly 18 million BSA reports were filed. Although these reports are critical to law enforcement, past audits have shown that many contain incomplete or erroneous data. Additionally, past audits have also shown that examination coverage by regulators of financial institution compliance with BSA has been limited.

Given the criticality of this management challenge to the Department's mission, we continue to consider BSA and OFAC programs as inherently high-risk. Further adding to this risk in the current environment is the risk that financial regulators and examiners may lessen their attention on BSA compliance as they address safety and soundness concerns. It should also be understood that due to resource constraints and mandatory requirements, particularly with respect to failed banks, we do not anticipate providing significant audit coverage to this challenge area during Fiscal Year 2009.

As mentioned above, we removed the previously reported management and performance challenge "Linking Resources to Results" because of the progress the Department has made in this area. For example, among other things, it updated its Managerial Cost Accounting Policy to provide additional guidance to its bureaus and offices for accumulating, measuring, analyzing, interpreting and reporting cost information.

We would be pleased to discuss our views on these management and performance challenges in more detail.

cc: Peter B. McCarthy, Assistant Secretary for Management and Chief Financial Officer




INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON

December 18, 2008

INFORMATION MEMORANDUM FOR SECRETARY PAULSON

FROM:

Eric M. Thorson 
Inspector General

SUBJECT:

Information Requested Relating to a Capital Infusion to IndyMac Bank, F.S.B. (OIG-CA-09-004)

On July 11, 2008, the Office of Thrift Supervision (OTS) closed IndyMac Bank and appointed the Federal Deposit Insurance Corporation (FDIC) receiver. FDIC estimated the loss to the Deposit Insurance Fund for the failed bank at \$8.9 billion. As required by law, my office began performing a material loss review of IndyMac to determine the cause(s) of the thrift's failure and assess OTS's supervision over the institution. That review is ongoing. As is common with the failure of a publicly-held insured financial institution, other Federal agencies including the Securities and Exchange Commission (SEC) and FDIC also conduct reviews. In the case of IndyMac, SEC reviewed workpapers prepared by IndyMac's auditor, Ernst & Young (E&Y). One such workpaper reported a telephone discussion involving IndyMac's Chief Executive Officer (CEO), E&Y auditors, and OTS's West Region Director, Darrell Dochow, regarding an infusion of capital to IndyMac from its holding company, backdated to the first quarter of 2008. Because of its potential relevance to our material loss review, FDIC's Inspector General in turn provided the E&Y workpaper to our office.

At your request, I initiated an inquiry into the matter and am providing you with a status of what we have learned. Specifically, I am addressing whether:

- the Director of Office of Thrift Supervision's (OTS) West Region approved a capital infusion received by IndyMac Bank, F.S.B. (IndyMac), from its holding company after March 31, 2008, to be recorded as capital of the thrift as of March 31, 2008, and
- if so, the effect of recording the transaction in this manner.

The E&Y workpaper referred to review differences (proposed adjustments)¹ identified by the auditor during its review of IndyMac's interim financial statements for the quarter ending March 31, 2008. It also referred to proposed adjustments identified by E&Y during its audit of

¹ It is not unusual for an auditor to propose adjustments. It is also not unusual for management to waive the recordation of those adjustments. In practice, the auditor keeps track of the total effect of any unrecorded adjustments and if that total effect becomes material to users, the auditor will insist that the adjustments be recorded. Failure to do so by management will result in a modification of the auditor's opinion.

IndyMac's calendar year 2007 financial statements. Had the proposed adjustments identified by the auditor during its 2007 audit and 2008 review been recorded, IndyMac's capital ratio as of March 31, 2008, would have fallen below the 10 percent "well-capitalized" minimum threshold.²

According to the workpaper, on May 9, 2008, E&Y participated in a conference call with OTS West Region Director Dochow and IndyMac's CEO, Michael Perry. During the call, CEO Perry asked if OTS would allow IndyMac to record an April 2008 capital contribution from IndyMac's holding company to IndyMac Bank as of March 31, 2008. If so, that would enable IndyMac to meet the "well capitalized" threshold as of March 31, 2008. The workpaper indicated that West Region Director Dochow acknowledged the issue of the review differences and agreed to IndyMac's proposal. As a result, IndyMac's total risk-based capital ratio was restored back over the 10 percent "well-capitalized" minimum threshold for the March 31 report.

We confirmed through inquiry and review of additional supporting documentation that the circumstances occurred essentially as represented in the E&Y workpaper. The one exception is that the capital contribution in question occurred on May 9, 2008, not in April 2008 (nearly 6 weeks after the end of the quarter and the day of the conference call between E&Y, West Region Director Dochow, and IndyMac CEO Perry). The circumstances and accounting of this transaction as described by OTS are unclear and the documentation provided by OTS was ambiguous and incomplete. For example, OTS provided information indicating that the IndyMac holding company made a \$50 million capital contribution on May 9, 2008, of which \$18 million (the amount necessary for IndyMac to be "well capitalized") was recorded by the thrift as capital as of March 31, 2008. OTS also stated that IndyMac had recorded this amount as a receivable at March 31, 2008. OTS, however, did not provide documentation showing the recordation of the receivable. Furthermore, based on other documentation we obtained, the capital contribution of \$50 million was intended by the holding company's board of directors to be for the second quarter (quarter ending June 30, 2008).

The impact of West Region Director Dochow's approval to record the capital infusion in the quarter ending March 31, 2008, was that IndyMac was able to maintain its "well-capitalized" status, and avoid the requirement in law to obtain a waiver from FDIC to accept brokered deposits.³ It also solved another problem in that E&Y indicated that without IndyMac's acceptance of several proposed adjustments relating to the bank's capitalization, it would not have signed the interim review. IndyMac needed the signed interim review in order to file a complete quarterly report (10Q), as required, with the SEC on May 15, 2008.

During our inquiry, we also discovered that OTS had allowed other thrifts to record capital contributions in an earlier period than received. While there is some support in authoritative accounting literature for recording capital contributions in one period that were received in a

² When an institution falls below "well-capitalized," certain restrictions automatically take affect.

³ There are five established capital classifications for insured financial institutions: well-capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized. The use of brokered deposits is limited to well-capitalized insured depository institutions. Adequately capitalized institutions are required to obtain a waiver from FDIC in order to accept brokered deposits.

later period,⁴ that support is limited.⁵ Basically, IndyMac could record the capital infusion as of the quarter ending March 31, 2008, provided there was an actual note, a board resolution, or some form of communication showing the intent of the holding company at the time to infuse the capital (we also would expect that the holding company would have the capital available at March 31). However, in our work thus far, we have neither found nor been shown any indication that this intent existed. It is unclear what information OTS had at the time and what its basis was for allowing the capital infusion to be recorded for the quarter ending March 31, 2008. A separate inquiry as to a motive for approving and recording this transaction in the manner it was recorded is still ongoing. We are also continuing to obtain additional documentation to assess the accounting treatment of the capital contribution as of March 31, 2008. Our findings in that regard will also be discussed in the separate audit report.

Should you or your staff have any questions, you may contact me at (202) 622-1090 or Marla A. Freedman, Assistant Inspector General for Audit, at (202) 927-5400.

⁴ Financial Accounting Standards Board (FASB) Evolving Issues Task Force Abstract 85-1, *Classifying Notes Received for Capital Stock* (Abstract 85-1).

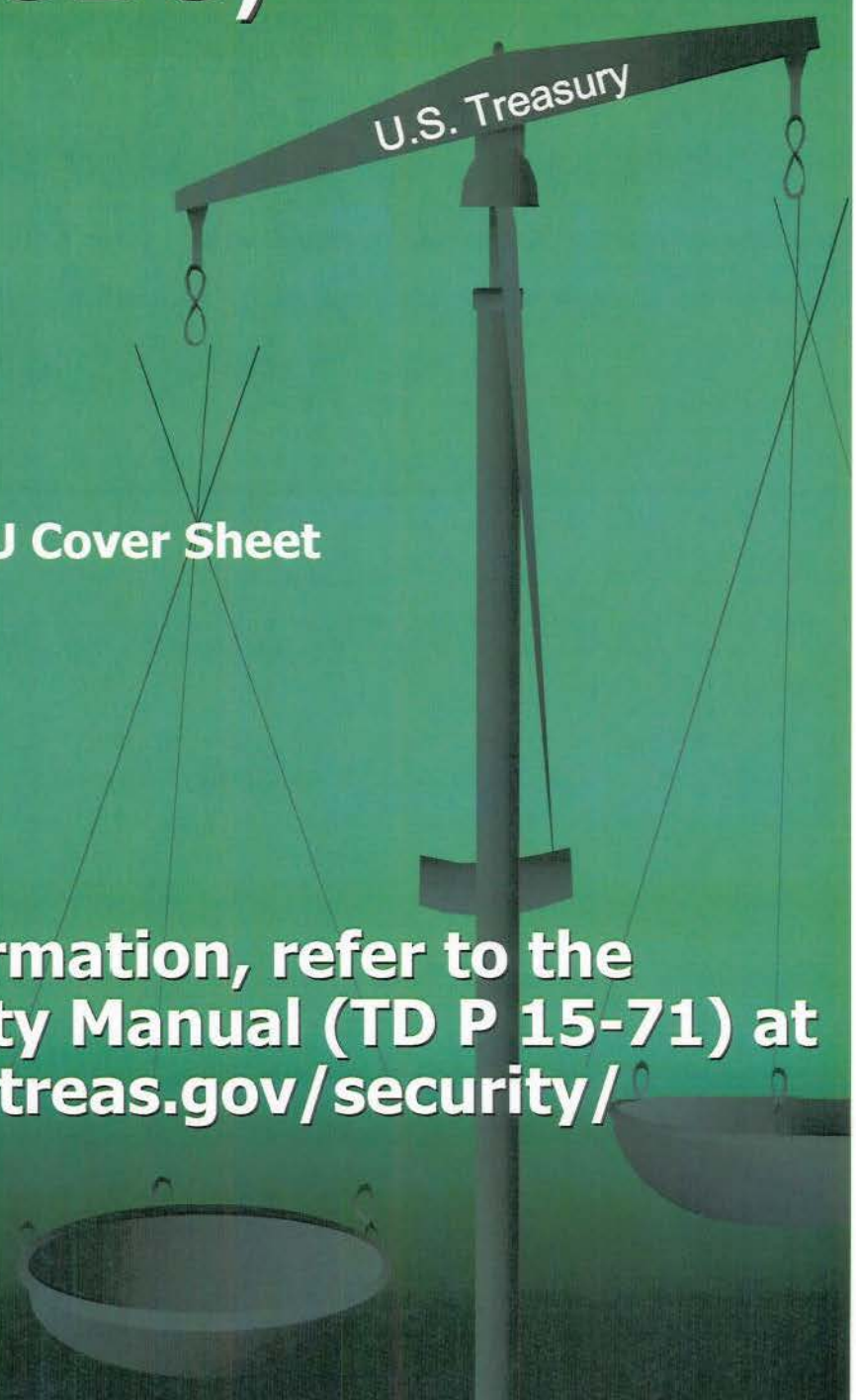
⁵ In recent discussions with a FASB staff representative regarding Abstract 85-1 and the applicability of it to these circumstances, the reporting of a note as an asset is generally not appropriate, except in very limited circumstances and when there is substantial evidence of the ability and intent to pay within a reasonably short period of time.

SENSITIVE BUT UNCLASSIFIED (SBU)

SBU Cover Sheet

**For further information, refer to the
Treasury Security Manual (TD P 15-71) at
<http://intranet.treas.gov/security/>**

TD F 15-05.11 (3/07)






DEPARTMENT OF THE TREASURY
WASHINGTON

MAR 17 2009

SENSITIVE BUT UNCLASSIFIED

INFORMATION MEMORANDUM FOR SECRETARY GEITHNER

FROM:

Eric M. Thorson 
Inspector General

SUBJECT:

Information Requested Regarding the Office of Thrift Supervision
(OIG-09-CA-008)¹

In response to your request, my office reviewed the actions of Office of Thrift Supervision (OTS) officials, in particular current OTS Acting Director Scott M. Polakoff, with regard to the reporting of a certain infusion of capital into BankUnited, F.S.B. (BankUnited). I am providing you with the following information.

Based on our review, we determined that Mr. Polakoff was aware of, and even directed, the backdating of an \$80 million infusion of capital into BankUnited.

Specifically, Mr. Polakoff² participated in a conference call on August 4, 2008, with other OTS headquarters supervisory staff³ and OTS Southeast Region officials to discuss BankUnited. The purpose of the call was to talk about the CAMELS⁴ ratings for the recently concluded examination of the thrift and the appropriate supervisory and enforcement response. It should be noted that the thrift had recognized a significant second quarter charge-off of about \$74 million to its loan portfolio. Among the items discussed during the call was BankUnited management's willingness to infuse capital from the holding company into the thrift to offset that loss. With that in mind, the amount of funds available at the holding company for infusion was discussed and Mr. Polakoff told the regional staff to request BankUnited management to infuse as close to \$80 million of available funds as possible. The timing of the recognition of the infusion was also discussed. Mr. Polakoff advised that for regulatory purposes the infusion should be recognized as of June 30, 2008, and the Thrift Financial Report (TFR)⁵ amended accordingly.

¹ This memorandum contains privileged bank examination information which must be safeguarded.

² Due to the sensitivity of this matter, we did not interview Mr. Polakoff. Instead, we obtained corroborating evidence, including internal OTS emails and inquiry with other OTS officials to establish and confirm our understanding of what took place.

³ The other OTS headquarters officials participating in the conference call were the OTS Deputy Director, Examinations, Supervision and Consumer Protection; and the OTS Managing Director, Examinations, Supervision and Consumer Protection.

⁴ CAMELS is an acronym for the performance rating components in a Report of Examination. Capital adequacy, Asset quality, Management administration, Earnings, Liquidity, and Sensitivity to market risk. Numerical values range from 1 to 5, with 1 being the highest rating and 5 representing the worst rating.

⁵ The TFR is a financial report that thrifts are required to file quarterly with OTS. The report includes detailed

SENSITIVE BUT UNCLASSIFIED

Page 2

The Southeast Region Director commented to Mr. Polakoff that BankUnited did not have a note or other required documentation to support recognition of the infusion in the June quarter under generally accepted accounting principles (GAAP). Mr. Polakoff indicated that he was willing to accept that in this case.⁴ After the briefing, OTS Southeast Region officials called BankUnited's chief executive officer and directed that the capital infusion be made immediately and an amended TFR be filed. The infusion was made on August 5, 2008.

For your information, our review revealed that BankUnited was included on OTS's Problem Bank Report in August 2008, and received a composite CAMELS rating of 4 as a result of a July 2008 examination. In addition, based on June 30, 2008, financial information, BankUnited was categorized as being well-capitalized with a total risk-based capital ratio of 13.87 percent. Although BankUnited met the regulatory threshold requirement of 10 percent risk-based capital to maintain a well-capitalized status, in accordance with prompt corrective action, OTS imposed a 15 percent risk-based capital level by a Memorandum of Understanding (MOU) issued in July 2008. The increased threshold of 15 percent risk-based capital was not met as of June 30, 2008. According to the latest OTS Problem Bank Report, BankUnited's composite CAMELS rating is now 5. Losses totaled over \$1 billion for 2008.

There is some support in authoritative accounting literature for recording capital contributions in one period that were received in a later period, but that support is limited.⁶ In addition, OTS recently issued guidance regarding the accounting treatment of capital contributions.⁷ Under this newly issued guidance, and consistent with accounting literature, BankUnited could have recorded the capital infusion as of the quarter ending June 30, 2008, provided there was an actual note showing the intent of the holding company to infuse the capital at that time. However, in this case, there was no note and we believe it was wrong for OTS to direct the thrift to backdate the \$80 million capital infusion.

We are continuing our audit of OTS's actions to allow, or in the case of BankUnited direct, the backdating of capital infusions for certain thrifts. We anticipate completing that audit and issuing a report in May 2009.

cc: Bernard Knight, Acting General Counsel

information about the institution's operations and financial condition. OTS requires the TFR to be prepared in accordance with GAAP.

⁶ Financial Accounting Standards Board Evolving Issues Task Force Abstract 85-1, *Classifying Notes Received for Capital Stock* (Abstract 85-1) states a company must show the intent, have the capital to give, and then actually infuse the capital prior to the issuance of its published financial statements. In recent discussions with a FASB staff representative regarding Abstract 85-1 and the applicability of it to these circumstances, the reporting of a note as an asset is generally not appropriate, except in very limited circumstances and when there is substantial evidence of the ability and intent to pay within a reasonably short period of time.

⁷ OTS, New Directions 09-04, *Recognition of Capital Contributions in the Form of Cash or Notes*, dated January 23, 2009.