Employee Benefits Security Administration

Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations No. 2

November 18, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Members of the Federal Retirement Thrift Investment Board
Washington, D.C.

Ian Dingwall
Chief Accountant
U.S. Department of Labor, Employee Benefit Security Administration
Washington, D.C.

As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit to determine the status of certain prior year EBSA recommendations and sub-recommendations[1] related to the Thrift Savings Plan (TSP) and directed to the Federal Retirement Thrift Investment Board's Staff (Agency). Our fieldwork was performed from July 28 through September 16, 2014 at Agency headquarters in Washington, D.C. Our scope period for testing was January 1, 2014 through July 18, 2014.

We conducted this audit in accordance with the performance audit standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate audit evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. Criteria used for this audit is defined in the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes United States Code (USC) Title 5, Chapter 84, and Code of Federal Regulations (CFR) Title 5, Chapter VI.

The objective of our audit was to determine the status of certain TSP recommendations and sub-recommendations that had not been closed by EBSA as of September 30, 2013. The following prior year recommendations and sub-recommendations were in scope for this performance audit:

- *Review of the Thrift Savings Plan Withdrawals Process, as of August 24, 2005*, No. 2005-1: Daily Disbursement Reconciliation Process;

[1] Certain EBSA prior year recommendations have multiple components; for purposes of this report, we refer to these components as "sub-recommendations." Recommendations are identified by a number (e.g., No. 2013-1), while sub-recommendations are identified by a number and a letter (e.g., No. 2013-2a).

- *Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008*, Nos. 2008-1d and e: Security and Privacy Risk Assessments and Formal Corrective Action Plans Should Be Improved;
- *Performance Audit of the Thrift Savings Plan Loan Process, as of October 18, 2010*, No. 2009-2: Interest Accrual Calculations for Participants in Nonpay Status;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of August 14, 2009:*
  - No. 2009-1a: Logical Access Controls at the Call Centers Should Be Strengthened (Maryland Call Center);
  - No. 2009-2a: Logical Access Controls at the Call Centers Should Be Strengthened (Virginia Call Center);
  - No. 2009-5: Call Center Physical Access Controls Need to Be Strengthened;
- *Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings, as of July 30, 2010*, Nos. 2010-2a and b: Project Integration and Knowledge Transfer Activities Need To Be Improved;
- *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls, as of July 30, 2012*, No. 2011-3c: Lack of a Vulnerability Management Program;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of November 19, 2012*, No. 2012-2b: Additional Logical Access Control Weaknesses at the Call Centers;
- *Performance Audit of Certain Thrift Savings Plan Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, as of September 27, 2012*, No. 2012-1: Insufficient Performance of Budget Review and Estimates Analysis;
- *Performance Audit of the Thrift Savings Plan Systems Enhancements and Software Change Controls, as of November 27, 2013*, No. 2013-4a: IT Contracts Should Support Implementation of the EISRM Policy;
- *Performance Audit of the Thrift Savings Plan Service Continuity Controls, as of March 26, 2014:*
  - No. 2013-3b: Separation of Duties Weaknesses;
  - No. 2013-5a, b, and c: Weaknesses in Primary and Alternate Data Center Physical Access Controls; and
  - No. 2013-8c: Replication and Tape Backup Data Tests and Restoration Process Weaknesses.

These prior year recommendations and sub-recommendations addressed fundamental or other controls over various aspects of the TSP. Fundamental control recommendations address significant procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Other control recommendations address procedures or processes that are less significant than fundamental controls. Our audit resulted in no new recommendations.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objective. As of July 18, 2014, we determined the status of the 18 prior EBSA TSP recommendations and sub-recommendations previously listed. In summary, we report that 17 recommendations and sub-recommendations have been implemented and closed and 1 sub-recommendation has not been implemented and remains open.

EBSA tracks the status of recommendations at the recommendation level. However, the Agency tracks status at the sub-recommendation level. The 18 prior EBSA TSP recommendations and sub-recommendations included in the scope of this audit address 14 recommendations. Of those 14 recommendations, we consider 7 of them closed based on our audit results.

The Agency's response to the recommendation, including the Executive Director's formal reply, is included as an appendix within this report (Appendix A). The Agency concurred with the recommendation.

This performance audit did not constitute an audit of the TSP's financial statements in accordance with *Government Auditing Standards.* KPMG was not engaged to, and did not render an opinion on the Agency's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of this audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

While we understand that this report may be used to make the results of our performance audit available to the public in accordance with *Government Auditing Standards*, this report is intended for the information and use of the U.S. Department of Labor Employee Benefit Security Administration, Members of the Federal Retirement Thrift Investment Board, and Agency management. The report is not intended to be, and should not be, used by anyone other than these specified parties.

KPMG LLP

November 18, 2014

I. BACKGROUND OF THE THRIFT SAVINGS PLAN

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act of 1986 (FERSA), as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS) and provides a Federal (and, in certain cases, state) income tax deferral on employee contributions and related earnings. The TSP is available to Federal and Postal employees, members of Congress and certain Congressional employees, and members of the uniformed services. For FERS participants, the TSP also provides agency automatic one percent and matching contributions. The TSP began accepting contributions on April 1, 1987, and as of June 30, 2014, had approximately $418 billion in assets and approximately 4.6 million participants[2].

The FERSA established the Federal Retirement Thrift Investment Board (the Board) and the position of Executive Director. The Executive Director and the members of the Board are TSP fiduciaries. The Executive Director manages the TSP for its participants and beneficiaries. The Board's Staff (the Agency) is responsible for administering TSP operations.

[2] Source: Minutes of the July 28, 2014 Federal Retirement Thrift Investment Board meeting, posted at www.frtib.gov.

II. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objective

The U.S. Department of Labor (DOL) Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit to determine the status of certain prior year EBSA recommendations and sub-recommendations related to the Thrift Savings Plan (TSP) and directed to the Federal Retirement Thrift Investment Board's (Board) Staff (Agency).

The prior EBSA TSP recommendations and sub-recommendations in scope for this performance audit were:

- *Review of the Thrift Savings Plan Withdrawals Process, as of August 24, 2005*, No. 2005-1: Daily Disbursement Reconciliation Process;
- *Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008*, Nos. 2008-1d and e: Security and Privacy Risk Assessments and Formal Corrective Action Plans Should Be Improved;
- *Performance Audit of the Thrift Savings Plan Loan Process, as of October 18, 2010*, No. 2009-2: Interest Accrual Calculations for Participants in Nonpay Status;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of August 14, 2009:*
  - Nos. 2009-1a: Logical Access Controls at the Call Centers Should Be Strengthened (Maryland Call Center);
  - Nos. 2009-2a: Logical Access Controls at the Call Centers Should Be Strengthened (Virginia Call Center);
  - No. 2009-5: Call Center Physical Access Controls Need to Be Strengthened;
- *Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings, as of July 30, 2010*, Nos. 2010-2a and b: Project Integration and Knowledge Transfer Activities Need To Be Improved;
- *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls, as of July 30, 2012* No. 2011-3c: Lack of a Vulnerability Management Program;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of November 19, 2012*, No. 2012-2b: Additional Logical Access Control Weaknesses at the Call Centers;

- *Performance Audit of Certain Thrift Savings Plan Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, as of September 27, 2012*, No. 2012-1: Insufficient Performance of Budget Review and Estimates Analysis;
- *Performance Audit of the Thrift Savings Plan Systems Enhancements and Software Change Controls, as of November 27, 2013*, No. 2013-4a: IT Contracts Should Support Implementation of the EISRM Policy;
- *Performance Audit of the Thrift Savings Plan Service Continuity Controls, as of March 26, 2014:*
  - No. 2013-3b: Separation of Duties Weaknesses;
  - No. 2013-5a, b, and c: Weaknesses in Primary and Alternate Data Center Physical Access Controls; and
  - No. 2013-8c: Replication and Tape Backup Data Tests and Restoration Process Weaknesses.

EBSA tracks the status of recommendations at the recommendation level. However, the Agency tracks status at the sub-recommendation level. The 18 prior EBSA TSP recommendations and sub-recommendations listed above address 14 recommendations.

B. Scope and Methodology

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States using EBSA's *Thrift Savings Plan Fiduciary Oversight Program*. Our scope period for testing was January 1, 2014 through July 18, 2014. We performed the audit in four phases: (1) planning, (2) arranging for the engagement with the Agency, (3) testing and interviewing, and (4) report writing.

The planning phase was designed to assist team members to develop a collective understanding of the prior TSP recommendations in scope and the corrective actions implemented by the Agency. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we performed the following procedures to achieve our audit objective:

- Inspected auditee-provided documentation and evidence;

- Tested a non-statistical sample of employees with outstanding loans who were in nonpay status during the scope period to determine whether accrued interest was properly calculated;
- Tested a non-statistical sample of business days to determine whether daily disbursement reconciliation reconciling items were resolved timely and that no reconciling items related to August 2004 and prior;
- Tested a non-statistical sample of quarterly budget reviews to determine whether the Agency conducted budget reviews on a more frequent basis than semi-annually.
- Tested a non-statistical sample of Agency plans of action and milestones to determine if documented security weaknesses, corrective action plans, milestones, and target completion dates for weaknesses were identified through conducted reviews;
- Tested a non-statistical sample of vulnerabilities identified in the Maryland and Virginia call centers to determine if documentation existed detailing the tracking, review, and closure of vulnerabilities;
- Tested a non-statistical sample of new hires at the Maryland call center to determine if access to the network was properly approved prior to access being granted;
- Tested a non-statistical sample of employees and contractors to determine if management authorization was completed and documented before gaining access to the primary and/or alternate data centers;
- Tested a non-statistical sample of employees and contractors to determine if documentation existed detailing the recertification of access for individuals with physical access to the primary and/or alternate data center;
- Tested a non-statistical sample of terminated employees and contractors with access to primary and/or alternate data center to determine if data center access was immediately removed upon termination;
- Tested a non-statistical sample of backup project managers to determine whether they had sufficient knowledge about the related projects to adequately perform key project lead duties in case the key project leads were unable to perform such responsibilities;
- Tested a non-statistical sample of Maryland call center new hires to determine if security awareness training was provided to employees before they were granted access to TSP information and information systems;
- Inspected the one information system design and development task that occurred during our scope period to determine if security-related documentation and evaluation and assurance of security controls were included in the system change documentation; and
- Tested a non-statistical sample of patch implementations to determine if a mechanism was being used to capture the deployment, testing, and approval of security patches.

We conducted these test procedures at the Agency headquarters in Washington, D.C. In Appendix B, we identify the key documentation provided by the Agency personnel that we reviewed during our performance audit.

Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the sample items tested and were not extrapolated to the population.

The report writing phase entailed drafting a preliminary report, conducting an exit conference, providing a formal draft report to the Agency for comment, and preparing and issuing the final report.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We conducted a performance audit to determine the status of certain prior U.S. Department of Labor Employee Benefits Security Administration (EBSA) recommendations and sub-recommendations related to the Thrift Savings Plan (TSP) and directed to the Federal Retirement Thrift Investment Board's (the Board) Staff (Agency). Our scope period for testing was January 1, 2014 through July 18, 2014. This performance audit consisted of reviewing applicable policies and procedures and testing manual and automated processes and controls, which included interviewing key personnel, reviewing key reports and documentation (Appendix B), and observing selected procedures.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objective. As of July 18, 2014, we determined that status of the following prior EBSA TSP recommendations and sub-recommendations:

- *Review of the Thrift Savings Plan Withdrawals Process, as of August 24, 2005*, No. 2005-1: Daily Disbursement Reconciliation Process;
- *Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008*, Nos. 2008-1d and e: Security and Privacy Risk Assessments and Formal Corrective Action Plans Should Be Improved;
- *Performance Audit of the Thrift Savings Plan Loan Process, as of October 18, 2010*, No. 2009-2: Interest Accrual Calculations for Participants in Nonpay Status;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of August 14, 2009:*
  - No. 2009-1a: Logical Access Controls at the Call Centers Should Be Strengthened (Maryland Call Center);
  - Nos. 2009-2a: Logical Access Controls at the Call Centers Should Be Strengthened (Virginia Call Center);
  - No. 2009-5: Call Center Physical Access Controls Need to Be Strengthened;
- *Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings, as of July 30, 2010*, Nos. 2010-2a and b: Project Integration and Knowledge Transfer Activities Need To Be Improved;

- *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls, as of July 30, 2012*, No. 2011-3c: Lack of a Vulnerability Management Program;
- *Performance Audit of the Thrift Savings Plan Participant Support Process, as of November 19, 2012*, No. 2012-2b: Additional Logical Access Control Weaknesses at the Call Centers;
- *Performance Audit of Certain Thrift Savings Plan Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, as of September 27, 2012*, No. 2012-1: Insufficient Performance of Budget Review and Estimates Analysis;
- *Performance Audit of the Thrift Savings Plan Systems Enhancements and Software Change Controls, as of November 27, 2013*, No. 2013-4a: IT Contracts Should Support Implementation of the EISRM Policy;
- *Performance Audit of the Thrift Savings Plan Service Continuity Controls, as of March 26, 2014:*
  - No. 2013-3b: Separation of Duties Weaknesses;
  - Nos. 2013-5a, b, and c: Weaknesses in Primary and Alternate Data Center Physical Access Controls; and
  - No. 2013-8c: Replication and Tape Backup Data Tests and Restoration Process Weaknesses.

Section III.B documents the status of the 18 prior EBSA TSP recommendations and sub-recommendations noted above. In summary, we report that 17 recommendations and sub-recommendations have been implemented and closed and 1 sub-recommendation has not been implemented and remains open.

These prior year recommendations and sub-recommendations addressed fundamental or other controls over various aspects of the TSP. Fundamental control recommendations address significant procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen the TSP's controls. The Agency should review and consider the open recommendation for timely implementation. The Agency's response to this recommendation is included as an appendix within this report (Appendix A).

EBSA tracks the status of recommendations at the recommendation level. However, the Agency tracks status at the sub-recommendation level. The 18 prior EBSA TSP recommendations and sub-

recommendations included in the scope of this audit address 14 recommendations. Of those 14 recommendations, we consider 7 of them closed based on our audit results.

Exhibit III-1 shows the number of open EBSA TSP recommendations by audit area as of June 30, 2014 and the number of those recommendations closed during this audit. This exhibit does not consider other EBSA TSP performance audit reports issued in final form since June 30, 2014.

Exhibit III-1

Audit Area	Recommendations Open as of June 30, 2014	Recommendations Closed During This Audit	Remaining Open Recommendations
Computer Access and Security Controls	12	0	12
Participant Support/ Call Center Operations	14	3	11
Service Continuity	8	0	8
System Enhancements and Software Change Controls	5	0	5
Project Management Practices	2	1	1
Withdrawals	6	1	5
Loan Operations	2	1	1
Board Administrative Staff	2	1	1
All Other	14	0	14
Total	**65**	**7**	**58***

* Fifty of these are fundamental control recommendations.

Section III.C summarizes the open recommendation.

B. Findings and Recommendations from Prior Reports

The findings and recommendations from prior reports that required follow-up are presented in this section. The discussion below includes the current status of each recommendation and sub-recommendation within the scope of this audit. When sub-recommendations were addressed in this audit, we also included the current status of the related recommendations.

2005 Withdrawal Process Recommendation No. 1:

Original Recommendation: The Agency should enhance supervisory review procedures over daily disbursement reconciliations to ensure reconciling items are resolved timely. The Agency should also ensure that the reconciling items related to August 2004 and prior are promptly corrected in the TSP general ledger. In addition, the supervisors should document evidence of their review on each reconciliation.

Reason for Recommendation: Of the 25 daily reconciliations judgmentally selected for testing, we noted that reconciling items on 24 reconciliations were not timely resolved. Specifically, we identified certain reconciling items that were identified during the period of August 2003 through August 2004 that as of February 2005 had not been properly adjusted in the TSP general ledger (i.e., Savantage). In addition, we noted one reconciliation completed in February 2005 that had no evidence of supervisory review.

Status: **Implemented.**

The Agency indicated that reconciling items on the Standard Form 1166 reconciliations were related to a programming error with the Savantage disbursement module and its respective reports. A new disbursement application, OMNIPay, was deployed in July 2011 which eliminated this outstanding issue. We inspected a screenshot of the System Change Request (SCR) and the related results of testing completed while the change was in development to support proper functioning of the change.

Additionally, we selected a non-statistical sample of 5 daily reconciliations and noted that all reconciling items were resolved timely and no reconciling items related to August 2004 and prior. We also inspected the journal entry

recorded by the Agency to adjust reconciling items that were identified during the period August 2003 through August 2004 and determined that such reconciling items were properly adjusted. We noted in the report titled *Performance Audit of the Thrift Savings Plan Withdrawals Process, as of November 9, 2011*, that all reconciliations selected for testing during that performance audit had evidence of supervisory review. Therefore, we consider this recommendation closed.

Disposition: **Recommendation Closed**.

2008 Computer Access and Technical Security Controls Recommendation No. 1:

Original Recommendation: To strengthen the controls over the security and privacy program, we recommend that the Agency:

d. Complete, implement and monitor policies related to protecting sensitive and PII information and the PII incident response and notification plan leveraging OMB guidance.
e. Implement formal plans of action and milestones (POA&Ms) to capture security weaknesses, corrective action plans, milestones, and target completion dates for weakness remediation identified through any and all reviews conducted.

Reason for Recommendation: Policies and procedures for protecting and using sensitive and personally identifiable information (PII) had not been fully identified nor created. In addition, information security and privacy weaknesses identified through internal or external assessment were not being centrally tracked and managed nor were corrective actions plans with milestones and target end dates for remediation being included.

Status: **Implemented.**

d. The Agency implemented an Incident Response policy on June 29, 2012 that requires the protection of sensitive information and PII. We determined that the Agency uses a vulnerability scanning tool to track database administrative weaknesses, vulnerable ports into databases, and other avenues that may lead to a breach of PII. Upon inspection of the

Virginia call center POA&Ms as of February 2014 and June 2014, we noted that they included results from the Agency's scanning tool. Additionally, we noted that the Agency has formed an IT Incident Response Team (IRT), and procedures are in place to notify appropriate parties after declaring a data breach. After the resolution of a breach incident, the IRT develops an "After-Action Report," which documents the details of the incident, identifies "lessons learned" from the incident, and recommends short and long term activities to be taken by the Agency and contractors to reduce further damage and mitigate potential future incidents. As such, this portion of the recommendation is closed.

e. The Agency has implemented the use of POA&Ms to track and capture security weaknesses, corrective action plans, milestones, and target completion dates for weakness remediation identified through any and all reviews conducted. During our fieldwork, we noted that the Agency tracked a total of 35 different POA&Ms, which included different systems, major applications, general support systems, infrastructure areas, and remote locations, as of July 28, 2014. To test the process, we inspected a selection of four POA&Ms and noted they captured security weaknesses, corrective action plans, milestones, and target completion dates for identified weakness remediation. As such, this portion of the recommendation is closed.

Disposition: **Sub-recommendations d and e Closed.**
Recommendation Open (sub-recommendations a and b).

2009 Loan Operations Recommendation No. 2:

Original Recommendation: The Agency should evaluate the specific cause of the deficiency identified and develop the appropriate corrective action to ensure that interest is properly accrued and posted to the accounts of the participants in nonpay status.

Reason for Recommendation: During our testing of 58 statistically selected loans in nonpay status, we noted that the full amount of interest was not properly accrued in one participant's account during the period of nonpay status.

Status: **Implemented.**

The Agency's review of the reamortization interest calculation identified that when a reamortization is processed because of a nonpay status and a second reamortization is processed before a loan payment is posted, the second reamortization calculation fails to include interest in arrears. The Agency indicated that its analysis and testing confirmed that this error was limited to nonpay reamortizations (i.e., the military, regular, and administrative) and that an SCR was submitted to correct the issue. Although the Agency provided a screenshot of the SCR, personnel did not provide the related results of testing completed while the change was in development to support proper functioning of the change.

As an alternative procedure, the Agency created a scenario in a test environment to demonstrate that the new system configuration corrected the cause of the error. We inspected the scenario and determined that the SCR was properly implemented.

Additionally, we selected a non-statistical sample of 5 loans in nonpay status in the scope period and determined that accrued interest was properly calculated.

Disposition: **Recommendation Closed.**

2009 Participant Support Recommendation No. 1:

Original Recommendation: To strengthen logical access controls at the Maryland call center, we recommend that the Agency:

a. Implement a vulnerability management program that identifies and implements corrective action plan requirements for the call center.

Reason for Recommendation: During our 2009 testing at the Maryland call center, we noted that a comprehensive vulnerability management program that monitors and patches technical security weaknesses was not in place over the technical infrastructure that supported the call center.

Status: **Implemented.**

a. We noted that the Agency has implemented an Information Assurance Vulnerability Management (IAVM) Program that applies to all information systems. Agency personnel identify vulnerabilities in the Maryland call center via vulnerability scans and notify the contractor accordingly. We inspected email correspondence between the Agency and the Maryland call center contractor and noted that the Agency provided detailed scan results to the contractor and included instructions to create or update the contractor-maintained POA&M documentation.

Disposition: **Sub-recommendation a Closed.**
Recommendation Closed.

2009 Participant Support Recommendation No. 2:

Original Recommendation: To strengthen logical access controls at the Virginia call center, we recommend that the Agency:

a. Monitor the implementation of corrective actions to address the vulnerability identified at the call center.

Reason for Recommendation: During our 2009 testing at the Virginia call center, one vulnerability was identified during our external vulnerability scanning procedures at the call center.

Status: **Implemented.**

a. We noted that the Agency has implemented an IAVM Program that applies to all information systems. In addition, the Agency has implemented procedures to report identified vulnerabilities to local call center support staff for tracking of corrective actions in the call center's POA&M document.

Disposition: **Sub-recommendation a Closed.**
Recommendation Closed.

2009 Participant Support Recommendation No. 5:

Original Recommendation: To strengthen physical access controls at the Maryland call center, we recommend that the Agency monitor implementation of any corrective actions at the call center that result from the evaluation of the physical access controls to prevent individuals from having more access than they need to perform their job functions.

Reason for Recommendation: Access to the TSP dedicated areas within the call center was not always granted based on least privilege. We identified a total of 15 Field Site Support staff members who did not have a valid need to access the TSP dedicated areas and subsequently had their physical access permissions revoked.

Status: **Implemented.**

We noted that the Maryland call center implemented an employee badge policy which requires the completion of a badge access tracking log. We inspected the call center badge access log review for months April 2014 and May 2014 and noted that individuals identified for removal of call center access were removed as requested.

Disposition: **Recommendation Closed.**

2010 Project Management Practices Recommendation No. 2:

Original Recommendation: We recommend that the Agency:

a. Ensure that project integration processes are established to evaluate dependent relationships with project activities and resources. Consider the implementation of project tools that can aid in enabling the programmatic view of project activities and resources.
b. Adopt minimum standards for conducting lessons learned and knowledge transfer in projects in order to adequately safeguard against information loss and related issues with project execution. In addition, identify backup individuals for key personnel positions in the event of changes to key project personnel or contractors.

Reason for Recommendation: During our 2010 audit work, we noted a lack of evidence demonstrating that adequate planning and consideration to project integration across the TSP Projects was contemplated to fully identify the dependencies and interrelationships across the projects. In addition, we noted that while quarterly presentations were provided to the Board summarizing the current status of each Agency project, knowledge of selected projects and their integration with other projects and TSP initiatives was centrally understood and managed by one key individual on a day-to-day basis without adequate documentation or procedures to fully transfer this knowledge to proper Agency personnel prior to the individual's retirement.

Status: **Implemented.**

a. The Agency's Project Management Office manually tracks project integrations via spreadsheet. The Project and Acquisition Committee (PAC) Charter, dated May 2014, outlines project integration processes in which PAC members are responsible for evaluating dependent relationships with project activities and resources. In addition, PAC members must understand each project's deliverables and how they meet the needs of business owners and key stakeholders, and bring office and Agency wide knowledge of existing and future workloads in order to provide input on the prioritization of projects. As such, this portion of the recommendation is closed.

b. In September 2013, the Agency implemented its Project Management Policy, which requires a project to be formally closed only after the project's success has been assessed and lessons learned that can be applied to the benefit of future projects have been documented. Further, we noted per the Project Management Policy that the transfer of project knowledge occurs during project execution between the Project Manager and the Integrated Project Team. We inspected one Post Project Review completed during our scope period and noted that the Agency maintained documentation of lessons learned and that additional knowledge transfers occurred during Executive Leadership Committee presentations.

   During our fieldwork, we noted that backup project managers have been identified for current Agency projects. These backup project managers

are aligned within the sponsoring office where the project is being implemented. As such, this portion of the recommendation is closed.

Disposition: **Sub-recommendations a and b Closed.**
Recommendation Closed.

2011 Computer Access and Technical Security Controls Recommendation No. 3:

Original Recommendation: The Agency should develop and implement a vulnerability management program that contains the following elements:

c. Mechanism for tracking and reporting security patch deployments such as POA&Ms.

Reason for Recommendation: Development and implementation of a vulnerability management program will allow the Agency to better manage risks associated with security vulnerabilities. By managing vulnerabilities within the environment, the Agency will develop controls that will support its risk management framework program.

Status: **Implemented.**

c. We noted the Agency has implemented the use of a commercially available tool to track and report security patch deployments. We inspected tracking and reporting information for a sample of two months of patches and noted that documentation over patch deployments, such as management approval, test results, and final approval and implementation, was maintained.

Disposition: **Sub-recommendation c closed.**
Recommendation Open (sub-recommendations b and d).

2012 Board Administrative Staff Recommendation No. 1:

Original Recommendation: The Agency should develop and implement formal policies and procedures to perform a budget to actual expenditure analysis on a more frequent basis than semi-annually.

Reason for Recommendation: Based on testwork performed, we noted that the Agency performs the Budget Review and Estimates analysis on a semi-annual basis.

Status: **Implemented.**

In October 2012, the Agency issued two Budget Directives which documented the general guidelines for the preparation, approval, and maintenance of the Annual Spend Plan for the Agency. Additionally, they addressed the creation of monthly status of funds reports and quarterly budget reviews.

We inspected one quarterly budget review which occurred between semi-annual dates and noted that it included individual offices, identified those with variances over a certain threshold, and documented the related analysis.

Disposition: **Recommendation Closed.**

2012 Participant Support Process Recommendation No. 2:

Original Recommendation: To strengthen logical access controls at the Maryland call center, the Agency should:

b. Develop and implement a monitoring process to ensure the call centers follow the Agency protocol that requires all individuals to complete security awareness training before they are granted access to any TSP information or information systems.

Reason for Recommendation: Based on our 2012 testwork, we noted at the Maryland call center that no evidence was provided that six of the ten new hires selected at the call center had completed the required security awareness training before obtaining access to TSP resources.

Status: **Implemented.**

b. The Agency required the call center contractor to update its training procedures to require security awareness training during new-hire training. We inspected a sample of five new hires at the Maryland Call Center during our scope period and noted that the selected individuals

obtained and passed security awareness training before being granted access to TSP-related information and information systems.

Disposition: **Sub-recommendation b Closed.**
Recommendation Open (sub-recommendation a).

2013 Systems Enhancements and Software Change Controls Recommendation No. 4:

Original Recommendation: To strengthen the administration of acquisitions and contracts, the Agency should:

a. Require contracts related to information systems design or development include security functional requirements, security related documentations, and evaluation and assurance of security controls throughout the SDLC.

Reason for Recommendation: Based on our 2013 testwork, we noted that the system enhancement and software change control contracts reviewed did not include information security requirements that addressed the scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Status: **Implemented.**

a. The Agency executed one contract related to information systems during our scope period. Per review of contract documentation, we noted that it requires the contractor to comply with the Agency's Enterprise Information Security and Risk Management (EISRM) security policies. Regarding security functional requirements, we noted that the contract identifies the security service responsibilities of the contractor.

Disposition: **Sub-recommendation a closed.**
Recommendation Open (sub-recommendation b).

2013 Service Continuity Controls Recommendation No. 3:

Original Recommendation: To strengthen appropriate separation of duties, the Agency should:

b. Document and enforce the separation of conflicting roles and tasks, or document an acceptance of risk with appropriate justification and compensating controls.

Reason for Recommendation: During our 2013 testwork, we noted that the Agency lacked segregation of duties controls in key functions. Lack of adequate separation of duties may result in errors going undetected and inappropriate or unauthorized processing of participant transactions and/or modification of participant data.

Status: **Implemented.**

b. The Agency's EISRM Access Policy includes separation of duties requirements for information systems, including both roles and tasks that are to be enforced by the Information System Owners and the Information System Security Manager/Chief Information Security Officer. In addition, in the current technology and enterprise support services contract, the Agency documented separation of duties requirements for this key contractor.

Disposition: **Sub-recommendation b Closed.**
Recommendation Open (sub-recommendations a and c).

2013 Service Continuity Controls Recommendation No. 5:

Original Recommendation: To strengthen controls over physical access to TSP systems resources, the Agency should:

a. Recertify access for individuals with physical access to the data centers in accordance with Agency policy;
b. Obtain and retain evidence of management authorization prior to granting individuals access to the data centers; and
c. Promptly remove data center access for separated individuals in accordance with Agency policy.

Reason for Recommendation: During our 2013 testwork, we noted certain weaknesses in primary and alternate data center physical access controls. By not reviewing, approving, and disabling physical access, an increased risk exists that individuals may have unnecessary or inappropriate access to TSP systems and data, putting the Agency at risk of inadvertent or deliberate disclosure, modification, or destruction of data.

Status: **Partially Implemented.**

a. The Agency conducts recertification of access at least annually in accordance with its EISRM Access Policy. We inspected a sample of two months of access recertifications for the primary and alternate data centers and noted that individuals no longer requiring access were identified and removed by management. As such, this portion of the recommendation is closed.
b. We inspected a sample of three individuals granted access to the primary and/or alternate data centers during our scope period and noted access was granted only after management provided approval. We noted that documentation detailing management's authorization was maintained and provided as evidence for our testing. As such, this portion of the recommendation is closed.
c. The Agency indicated that nine employees and contractors who had physical access to the primary and/or alternate data centers were terminated during the scope period. Of the nine individuals, we noted that six maintained physical data center access for weeks after their terminations, which did not comply with the Agency's EISRM Access Control policy. As such, this portion of the recommendation remains open.

Disposition: **Sub-recommendations a and b Closed.**
Recommendation Open (sub-recommendation c).

2013 Service Continuity Controls Recommendation No. 8:

Original Recommendation: To strengthen the reliability of TSP systems backup technologies and the Agency's ability to restore the system from backup technologies in the event of a disaster, the Agency should:

a. Consider modifying related policies or achieve compliance with current policies.

Reason for Recommendation: During our 2013 audit, the Agency indicated that its primary backup strategy involved data replication technology for both mainframe and distributed systems. However, written policies provided during the audit period referenced a separate tape backup recovery strategy involving weekly recovery tests. The Agency indicated that the tape strategy was outdated and usage of backup tapes would occur only if an extreme situation existed which resulted in the replication technology being unavailable.

Status: **Implemented.**

a. In December 2013, the Agency updated its EISRM Contingency Planning policy to require system owners to oversee backup activities, primary backup technologies to be tested weekly, and secondary backup technologies to be tested annually. Per the updated policy, we also noted that the frequency with which backup tape media is transferred to secure offsite storage facilities (e.g., Iron Mountain or the alternate processing site) is either daily or as the media is generated by the backup system.

Disposition: **Sub-recommendation a Closed.**
Recommendation Open (sub-recommendations b and c).

C. Summary of Open Recommendation

FUNDAMENTAL CONTROL RECOMMENDATION

2013 Service Continuity Controls Recommendation:

5. To strengthen controls over physical access to TSP systems resources, the Agency should:
   c. Promptly remove data center access for separated individuals in accordance with Agency policy.

AGENCY'S RESPONSE

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77K Street, NE Washington, DC 20002

November 18, 2014

Mr. Ian Dingwall
Chief Accountant
Employee Benefits
Security Administration
United States Department of Labor
Suite 400
122 C Street, N.W.
Washington, D.C. 20001-2109

Dear Ian:

This is in response to KPMG's email of November 3, 2014, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations No. 2 October 2, 2014. My comments with respect to this report are enclosed.

Thank you once again for the constructive approach that the Department of Labor and its contractors are taking in conducting the various audits of the TSP. The information and recommendations that are developed as a result of your reviews are useful to the continued improvement of the Thrift Savings Plan.

Very truly yours,

Gregory T. Long

Enclosure

Executive Director's Staff Formal Comments on the
Employee Benefits Security Administration Performance Audit of the Status of certain Thrift Savings Plan Prior Year Recommendations No. 2

IV. **Recommendations to Address Fundamental**

Controls: 2013 Service Continuity Controls

Recommendation No. 5:

To strengthen controls over physical access to TSP systems resources, the Agency should: Promptly remove data center access for separated individuals in accordance with Agency policy.

V. **Response:**

The Agency concurs with this finding. We have taken action to fix the process. As of September 16, 2014, the data center team has been incorporated into the overall Agency team responsible for the account removal process. This enables us now to remove data center access as soon as someone separates from the Agency. As further defense, we also have a quarterly data center recertification process in place. We consider this finding to be closed.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

Federal Retirement Thrift Investment Board's (Board) Staff (Agency) Documents and Reports:

- Corrective Action Plan - Status of Audit Recommendations v2, dated June 4, 2014
- Enterprise Information Security and Risk Management (EISRM) Incident Response Policy, dated June 29, 2012
- Office of Enterprise Risk Management (OERM) Incident Response Policy, dated January 2014
- Enterprise Network System (ENS) Plan of Action and Milestone (POA&M) v62, dated August 12, 2014
- ENS POA&M v72, dated August 12, 2014
- Mainframe POA&M v04, dated August 12, 2014
- Mainframe POA&M v06, dated August 12, 2014
- Complete list of Agency POA&Ms, dated July 28, 2014
- EISRM System & Communications Protection (SC) Policy, dated June 26, 2012
- System Change Request (SCR) No. 03355, Loan Problem with Interest Calculation during Multiple Reamortizations
- SCR No. 03517, Install Omni Service Pack 3
- SCR No. 03114, Development Efforts for SF1166 Functionality in OmniPay
- Test Instance Results Document – Send SF166 file to Treasury, May 2011
- Journal entries supporting correction of the August 2004 reconciling items from daily disbursement reconciliations, February 3, 2004 and August 10, 2009
- Information Assurance Vulnerability Management Program, dated June 26, 2013

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- Maryland Call Center Contract, dated September 26, 2013
- Virginia Call Center POA&M, dated February 2014 and June 2014
- Active Physical Security Review Procedures, dated May 12, 2013
- Call Center Badge Access Log Review, dated July 1, 2014
- April 2014 Call Center Badge Access Listing, dated April 1, 2014
- May 2014 Call Center Badge Access Listing, dated May 1, 2014
- Confirmation for Removal of Call Center Access, dated May 2, 2014
- Project Acquisition Committee Charter, dated May 16, 2014
- Technology and Enterprise Support Services (TESS) Post Project Review, dated December 16, 2013
- TESS Lessons Learned, dated August 12, 2014
- Lessons Learned Identification Template, dated February 10, 2014
- Project Management Policy, dated September 30, 2013
- Agency Open and Closed Projects, January 1, 2014 – July 18, 2014
- Acquisition and Contracts Policy Lessons Learned, dated April 17, 2014
- TESS Executive Leadership Committee Presentation, dated February 24, 2014
- Agency Patch Deployments, dated February 2014 and June 2014
- Budget Directive 064, dated October 1, 2012
- Budget Directive 065, dated October 15, 2012
- Agency's 3rd quarter (June 30, 2014) budget review
- List of New Contractors at the Maryland Call Center, for the period February 3 – April 23, 2014
- Screenshots of Certificates of Completion for sampled new hires at Maryland Call Center

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- Screenshot of Maryland Call Center master employee list file location, dated August 2014
- TESS contract, reference number TIB-2013-RFP-0012, dated January 26, 2013
- TESS contract, reference number TIB-2013-C-0012, Modification P00003, Section H – Special Contract Requirements, dated March 7, 2014
- FRTIB Case Management System Version 1.0 Security Assessment Report, dated April 8, 2014
- EISRM Access Policy, dated June 29, 2012
- Memorandum dated April 1, 2014, Subject: Alternate Data Center Access List
- Memorandum dated July 1, 2014 Subject: Alternate Data Center Access List
- Memorandum dated April 1, 2014, Subject: Primary Data Center Access List
- Memorandum dated July 1, 2014 Subject: Primary Data Center Access List
- List Employees and Contractors Requiring Data Center Access from January 1 2014, dated September 2014
- Terminated Data Center Access Listing, dated August 19, 2014
- Various Data Center Access Approvals
- EISRM Continuity and Contingency Planning (CP) Policy, dated June 26, 2012
- Policy Change Order for EISRM CP Policy, dated December 18, 2013