KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls

July 30, 2012

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 of the Thrift Savings Plan (TSP) computer access and technical security controls. Initially, we were contracted to conduct a performance audit over these controls during the spring of 2011. However, at the request of the Federal Retirement Thrift Investment Board's (Board) Staff (Agency), EBSA agreed to postpone this audit until January 2012 in order to provide the Agency additional time to implement proper security controls. During the planning phase of the audit, we determined that a number of related prior year recommendations continued to remain open. Given their impact on the TSP security program, EBSA revised the scope of the audit to focus on determining the status of the open prior EBSA TSP recommendations. Our fieldwork audit procedures were performed from January 9, 2012 through March 16, 2012, primarily at the Agency headquarters in Washington D.C. and Serco Inc. in Virginia.

We conducted this performance audit in accordance with the standards applicable to such audits 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our revised audit objectives. Criteria used for this engagement are defined in EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes the Federal Employees' Retirement system Act of 1986 (FERSA), as amended, and applicable Board regulations and bulletins. The detailed objectives of this engagement are enumerated within Section I.A.

The Agency is responsible for managing an entity-wide information security program that helps

support the mission of the TSP. Because of the change of audit scope discussed above, the audit focused on assessing the status of the prior open EBSA TSP recommendations, not on full testing of the key controls within the TSP security program.

Overall, based on the interviews conducted (Appendix A), documentation inspected (Appendix B), and test procedures performed, we conclude that the Agency has not fully implemented corrective action for any of the seven open EBSA TSP recommendations in this area. To strengthen the Agency's security and information technology (IT) program, focused efforts are needed to more timely implement all prior recommendations, as described in Section III of this report. We strongly recommend timely implementation to address these previously reported recommendations and to strengthen the overall security program and IT control environment related to access administration, security configuration, incident response, appropriate segregation of duties, information privacy, contractor oversight, and risk evaluation.

Specifically, we assessed the status of seven prior year recommendations, as follows:

- One reported in the "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, October 24, 2007";
- Four reported in the "Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, March 30, 2007"; and
- Two reported in the "Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008."

Section III.B documents the status of these prior recommendations. In summary, all seven recommendations remain open.

We present four new recommendations related to TSP computer access and technical security, all of which address fundamental controls. 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. These new recommendations address general policy and procedure weaknesses, the lack of certification and accreditation review, the lack of a vulnerability management program, and the lack of a configuration management program. All recommendations are intended to strengthen TSP computer access and technical security controls. The Agency should review and consider these recommendations for timely implementation. The Agency's responses to these recommendations are included as an appendix within this report (Appendix D).

On April 10, 2012, subsequent to the completion of fieldwork for this performance audit, the Agency was notified by Serco, Inc., a third-party service provider, that a breach of TSP data had occurred. The Agency indicated that the incident resulted in unauthorized access to certain personal information of approximately 123,000 TSP participants. Further, the Agency indicated that the Federal Bureau of Investigation (FBI) had informed Serco, Inc. about the breach of TSP data. The Agency issued a press release to the public on May 25, 2012, regarding the incident and provided letters to the TSP participants impacted by the breach shortly thereafter. We did not conduct any testing over the facts and circumstances of this breach.

Section I of this report discusses the EBSA's objectives, scope and methodology, and report organization for this performance audit. Section II is an overview of the TSP program, including security and technical controls. Section III presents the details that support the current year findings and recommendations and the status of prior year recommendations. In Appendices A and B, we identify the key personnel with whom we met and the documentation provided by the Agency and contractor personnel that we reviewed during our performance audit. We discussed recommendations with the appropriate Agency representatives (Appendix C). Final Agency comments, including the Executive Director's formal reply, are included as an appendix within this final report (Appendix D). The Agency concurred with all the findings and recommendations.

This performance audit did not constitute an audit of 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 (for purposes of the Office of Management and Budget's Circular No. A-127, *Financial Management Systems*, July 23, 1993 as revised). 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.

KPMG LLP

July 30, 2012

I. INTRODUCTION

A. Objectives

The U.S. Department of Labor (DOL), Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit of the Thrift Savings Plan (TSP) computer access and technical security controls to include testing over significant controls in this area. However, because of the Federal Retirement Thrift Investment Board's Staff's (Agency) lack of progress in addressing prior year findings and its impact on the TSP security program, EBSA revised the scope of this audit to focus on determining the status of applicable open recommendations. The resulting objective of this engagement was to determine the status of and report on the Agency's progress in implementing the following prior year recommendations:

- "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, October 24, 2007," No. 2007-1: Information Security over Laptops and Portable Devices;
- "Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, March 30, 2007" (2007 Computer Access), No. 2007-1: Security and Logical Access-related Policies Need to Be Strengthened;
- 2007 Computer Access, No. 2007-2: Security and Logical Access-related Practices Need to Be Strengthened;
- 2007 Computer Access, No. 2007-3: Logical Access Administration over TSP Systems Needs to Be Strengthened;
- 2007 Computer Access, No. 2007-4: Logical Access Configuration over TSP Systems Needs to Be Strengthened;
- "Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008" (2008 Computer Access), No. 2008-1: Security and Privacy Risk Assessments and Formal Corrective Action Plans Should Be Improved; and
- 2008 Computer Access, No. 2008-2: Authentication of TSP Participants to the Web Site Should Be Strengthened.

B. Scope and Methodology

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and EBSA's *Thrift Savings Plan Fiduciary Oversight Program.* In particular, we conducted our engagement as a performance audit defined by the *Government Auditing Standards* as an "objective analysis so that management and those charged with governance and oversight can use the information to improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability." We performed our engagement 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 activities and controls associated with the applications, processes and personnel involved with TSP operations. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we conducted interviews, collected and inspected auditee-provided documentation and evidence, participated in process walk-throughs, and designed and performed certain tests of controls. We conducted these test procedures primarily at Serco Inc.'s location in Virginia, and at Agency headquarters in Washington, DC.

Testing procedures were based on the objectives and control areas for information security and access controls in the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM). In addition, various Federal standards and guidelines[1] were used to evaluate the status of the prior year recommendations.

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

1 Office of Management and Budget (OMB) Circular No. A-130, Appendix III; Federal Information Processing Standards (FIPS) 191 and 140-2; and National Institute of Standards and Technology (NIST) Special Publications 800-18, 800-27, 800-37, 800-53, and 800-63.

C. Organization of Report

Section II presents an overview of the TSP and the information technology providers that are involved in implementing the TSP security program and an overview of the TSP security and privacy programs. Section III presents a detailed discussion of all recommendations.

II. OVERVIEW OF TSP ACCESS CONTROLS AND SECURITY

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). The TSP 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 the uniformed services, and members of Congress and Congressional employees. For FERS participants, the TSP also provides agency automatic (1 percent) and matching contributions. The TSP began accepting contributions on April 1, 1987, and as of March 31, 2012, TSP assets totaled approximately $313 billion and retirement savings accounts were being maintained for approximately 4.5 million participants[2].

The FERSA also established the Federal Retirement Thrift Investment Board (Board) and the position of Executive Director. The Executive Director and the Board members are TSP fiduciaries. The Executive Director manages the TSP for its participants and beneficiaries.

The Board's Staff (Agency) is responsible for administering TSP operations. To assist in the administration of TSP operations, the Agency has outsourcing relationships with several vendors to provide hosting, development, maintenance, and business continuity services for the TSP system. An integral component of the administration of TSP operations and these services is to to help maintain the confidentiality, integrity, and availability of participant and TSP management data.

B. TSP Systems and the Information Technology Providers

The Agency is responsible for implementing and maintaining a security program that protects the TSP information resources that are operated by contractors in addition to those that are maintained by the Agency. The TSP systems use a dedicated mainframe running access control software and several servers for processing. The core mainframe application is SunGard's OmniPlus, a commercial off-the-shelf (COTS) 401(k) recordkeeping software application. The Agency has outsourced many of the primary functions of the TSP information technology (IT) environment, including production and backup operations, hosting and application development,

[2] Source: Federal Retirement Thrift Investment Board meeting minutes, April 30, 2012.

and maintenance. For non-IT related services, the Agency also has responsibility for implementing and enforcing the security program requirements over those contractors, as they apply to the contracted service (e.g., call center operations). The following provides a brief description of the contracted functions for IT-related services:

- *Production and Backup Operations* - The Agency has contracted for production and backup operations services with Serco Inc. (Serco). Serco provides the day-to-day operational services over the TSP systems, which includes the administration, configuration, and management of logical access to the TSP systems.
- *Production and Backup Hosting* **–** The Agency has contracted the production and backup hosting of the TSP systems to a data center provider. Hosting services include the physical and environmental safeguarding of the TSP systems.
- *Application Development and System Maintenance* **–** The Agency's application development and maintenance services are also performed by Serco. Serco has subcontracted some application development and support services for OmniPlus and for system engineering and maintenance duties.

C. TSP Security Program

1. TSP Security Policies and Procedures

In September 2011, the Agency approved its Enterprise Information Security Risk Management (EISRM) Directive, which was designed to address security requirements, roles, and responsibilities and develop a security framework; this policy has not yet been fully enforced or distributed to employees and contractors, and related subsequent policies remain in draft status. The Agency is currently developing individual policies meant to support the EISRM and align to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control categories. The purpose of the individual policies noted above is to define the minimum set of security requirements for protecting the Agency's information systems, complying with applicable regulations, and implementing accepted leading practices and guidance.

2. TSP Security Controls Monitoring

The Agency monitors the TSP security program by evaluating security controls in operation and performs periodic scans of the network to identify known vulnerabilities..

3. TSP Logical Security

Logical security controls include the activities over administration and configuration of the TSP system components, in addition to consideration for authenticating and managing participant access to their accounts.

a. Logical Access Administration

Logical access administration pertains to the management and operational aspects of granting and managing access to TSP resources. The Security Application Group, managed by Serco, centralizes all system administration functions for the TSP systems. System administrators are designated for the TSP mainframe, networks, and TSP subsystems, and a backup administrator is typically in place to perform primary duties as needed. Access is granted by the system's Security Administrator based on a user's job role, and assigned on a least privilege basis commensurate with the responsibilities of that job.

In the event of separation, termination, or transfer of service, a manager or supervisor must submit a request via e-mail to the Security Application Team to have the ACID or user ID for the respective system(s) removed or suspended. In addition, accounts are to be periodically reviewed by the Security Application Group in order to verify that account privileges are still appropriate and consistent with the original access request, and the account is still active (i.e., being used and not inactive for a period of time). Changes to access follow the same protocol for granting access in that the change must be approved by the Agency and submitted to the Security Application Group.

b. Configuring Access to TSP Systems

Technical security configurations and safeguards over the TSP system components include how user access is authenticated and added to the network, TSP systems and mainframe. In addition, this includes defining and monitoring sensitive transaction types and actions that are considered auditable events.

(1) Networks and TSP System Components

Sensitive functions at the local area network (LAN)/ wide area network (WAN) operating environment (e.g., local and domain administrator rights) and at the database management system

(DBMS) level are to be restricted to administrator personnel. For the LAN/WAN, restricting local and domain administrator access precludes individuals from having administrator rights over their workstations or the domain. Because most TSP subsystem databases have data that is sensitive in nature (e.g., financial or Personally Identifiable Information (PII)), application controls are designed to protect the TSP subsystems by restricting direct access to DBMS. Restricting access of the security administrator functions to designated personnel is intended to protect the confidentiality, integrity, and availability of the resident data.

(2) Mainframe

Many sensitive datasets containing TSP information reside in the TSP mainframe. The mainframe has numerous configurable settings that, if altered or incorrectly configured, could expose the mainframe and resident files and data to potential risk of corruption or deletion. The mainframe also contains configurable settings for general system-wide mainframe security. These settings are intended to protect access to and interaction with the various sensitive datasets that reside on the TSP mainframe.

c. Participant Identity Management

Participant identity management consists of the processes and controls put into place to authenticate and validate participant interactions and transactions on the TSP Web and ThriftLine systems. The TSP has a large participant community that relies on system controls to protect their personal information and accounts.

Participant account numbers include TSP-assigned 13-digit account numbers, and each account number is linked to a participant's social security number to create the proper credential. Access to the web site and Thriftline uses the same account credentials. The web site uses an 8-character password and the Thrifline uses a personal identification number (PIN) for further authentication of the participant.

D. TSP Privacy Program

The Agency's Office of General Counsel (OGC) has overall responsibility for policy implementation considerations with regard to the Privacy Act. This includes the responsibility to carry out and conduct training to staff and contractors regarding their responsibilities for handling participant information. In addition, OGC is responsible for monitoring the compliance

requirements in accordance with the Privacy Act with respect to employee and contractor behavior, specifically any release of PII information.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We conducted a performance audit to determine the status of prior year recommendations related to the Thrift Savings Plan (TSP) computer access and technical security controls at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency). This performance audit consisted of reviewing applicable policies and procedures and testing select manual and automated process controls, which included interviewing key personnel (Appendix A), reviewing key reports and documentation (Appendix B), and observing selected procedures.

Initially, we were contracted to conduct a performance audit over computer access and technical security controls to include testing over significant controls in this area during the spring of 2011. However, at the request of the Agency, the U.S. Department of Labor Employee Benefits Security Administration (EBSA) agreed to postpone this audit until January 2012 in order to provide the Agency additional time to implement proper security controls. During the planning phase of the audit, we determined that a number of related prior year recommendations continued to remain open. Given their impact on the TSP security program, EBSA revised the scope of the audit to focus on determining the status of the open prior EBSA TSP recommendations. The objective of this revised engagement was to determine and report on the status of corrective actions to address the following prior computer access and technical security recommendations:

- "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, October 24, 2007," No. 2007-1: Information Security over Laptops and Portable Devices;
- "Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, March 30, 2007" (2007 Computer Access), No. 2007-1: Security and Logical Access-related Policies Need to Be Strengthened;
- 2007 Computer Access, No. 2007-2: Security and Logical Access-related Practices Need to Be Strengthened;
- 2007 Computer Access, No. 2007-3: Logical Access Administration over TSP Systems Needs to Be Strengthened;
- 2007 Computer Access, No. 2007-4: Logical Access Configuration over TSP Systems Needs to Be Strengthened;
- "Performance Audit of the Computer Access and Technical Security Controls over the

Thrift Savings Plan System, April 16, 2008" (2008 Computer Access), No. 2008-1: Security and Privacy Risk Assessments and Formal Corrective Action Plans Should Be Improved; and

- 2008 Computer Access, No. 2008-2: Authentication of TSP Participants to the Web Site Should Be Strengthened.

We present four new recommendations related to TSP computer access and technical security controls, all addressing fundamental controls. 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. All recommendations are intended to strengthen the TSP's security controls. The Agency should review and consider these recommendations for timely implementation. The Agency's responses to these recommendations are included as an appendix within this report (Appendix D).

Section III.B documents the status of the seven prior recommendations noted above. In summary, while the Agency has made progress to implement certain of these recommendations, we report that all seven recommendations have been partially implemented and remain open.

Section III.C presents the findings and recommendations from this performance audit. Section III.D summarizes each 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 as of March 16, 2012.

2007 Federal Retirement Thrift Investment Board Administrative Staff Recommendation No. 1:

Original Recommendation: To strengthen information security over laptops and portable devices, the Agency should:

a) Encrypt all hard drives on laptops issued by the Agency;
b) Enforce the use of virus screening on all external laptops and portable devices prior to being allowed connection to the Agency's network;

c) Evaluate the use of cable locks and other anti-theft techniques for Agency-issued laptops;
d) Consider strengthening the password composition rules for portable devices; and
e) Finalize and disseminate the Personally Identifiable Information (PII) Incident Response and Notification Plan.

Reason for Recommendation: The Agency controls the manner by which laptops and portable devices are distributed and accessed through various operational and technical controls. However, based on our 2007 review of the Agency's procedures and our comparison of them to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems; certain Office of Management and Budget (OMB) Memorandums; and U.S. Department of Labor Employee Benefits Security Administration (EBSA) Notice 06-11, Personally Identifiable Information on Portable Computer Equipment, we noted that improvements could be made over these practices.

March 2012 Status: **Partially Implemented.**

Parts a, b, c, and d of the original recommendation were closed in the report entitled "Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, as of October 7, 2009;" therefore, they were not included in the scope of our 2011 performance audit.

Regarding part e, the Agency had not developed a PII Incident Response and Notification Plan. A draft version of the Incident Response Policy, which requires that incidents involving PII be reported immediately to the Incident Response Team exists, however, the policy had not been finalized, approved or implemented by management. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

2007 Computer Access and Technical Security Controls Recommendation No. 1:

Original Recommendation: To strengthen the TSP security program, the Agency should document, finalize and fully implement the necessary security policies and procedures to enforce the TSP security program. Specifically, we recommend that the Agency:

a) Complete and implement the Thrift Savings Plan Data Security Policy as part of the TSP security program.
b) Update the TSP Electronic Media Management Policy to clarify the Agency's approved method for sanitizing media and TSP supporting equipment.
c) Update the TSP System Security Plan to include provisions for training incident response personnel and testing the Agency's incident response capability. Additionally, the Agency should periodically test the incident response capability.
d) Monitor and enforce the TSP policy for using the Internet, personal software, and peer-to-peer software for contractor locations.

Reason for Recommendation: The TSP security program controls, in order to be effective, must be communicated and enforced. These draft policies are integral parts of the information security requirements for the TSP system and its operation.

March 2012 Status: **Partially Implemented.**

a, b, d) While the Agency recently approved its Enterprise Information Security Risk Management (EISRM) Directive, which was designed to address security requirements, roles, and responsibilities and develop a security framework, the policy has not yet been fully enforced or distributed to employees and contractors, and related subsequent policies remain in draft status. The Agency is currently developing individual policies meant to support the EISRM and once completed will align to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control categories. However, at this time, these policies are in varying states of completion and have not been been approved or implemented, including policies related to access controls, electronic media management, and incident response, which respectively address the open recommendations. As such, these portions of the

recommendation remain open.

c) The agency no longer had a TSP System Security Plan, and therefore was unable to update the incident response provisions as noted in the original recommendation. Additionally, the Agency's incident response capability had not recently been tested. As such, this portion of the recommendation remains open.

The lack of a system security plan undermines the security requirements, boundaries, and controls needed to support an IT system's infrastructure. A system security plan is intended to provide an overview of the system, describe the security controls in place or planned for meeting system requirements, and provide security categorization and rationale for the information system. See 2011 Recommendation No. 2 for further information.

Disposition: **Recommendation Open**.

2007 Computer Access and Technical Security Controls Recommendation No. 2:

Original Recommendation: To strengthen the controls over the TSP's most privileged users and access to sensitive areas of the system, the Agency should document, finalize and fully implement the necessary procedures to enforce logical access requirements over the privileged users and access to sensitive areas of the TSP systems. Specifically, we recommend that the Agency:

a) Document and implement procedures to log and monitor system administrator activities such as changes to security parameters and configurations.

b) Complete and implement access administration procedures for granting access to sensitive and critical datasets, periodically recertifying mainframe accounts, and monitoring and reviewing mainframe access privileges.

c) Monitor and enforce the requirements for performing background investigations and acknowledging non-disclosure requirements for handling Privacy Act and TSP-related sensitive data.

Reason for Recommendation: Several weaknesses were identified related to the logical access administration and configuration over the TSP systems. Policy and procedures will help to reduce the risk of inconsistent logical access administration and configuration alterations.

March 2012 Status: **Partially Implemented.**

Part c of the original recommendation was closed in the report entitled "Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System as of October 7, 2009;" therefore, it was not included in the scope of our 2011 performance audit.

a) and b) As noted above, the Agency recently approved its EISRM Directive, which was designed to address security requirements, roles, responsibilities and establish a security framework. However, the policy had not yet been fully enforced or distributed to employees and contractors for implementation. While one contractor maintained procedural documentation on access administration and mainframe audit logging, it was not complete and had not been formally approved by the Agency. The Agency plans to develop audit and accountability and access control policies, which will include policies for administering access to TSP systems and logging and monitoring requirements to respectively address the open recommendations. As such, these portions of the recommendation remain open.

Disposition: **Recommendation Open.**

2007 Computer Access and Technical Security Controls Recommendation No. 3:

Original Recommendation: To strengthen the administration of logical and physical access over TSP systems, the Agency should evaluate, implement and monitor the logical and physical access administration over TSP accounts in the TSP systems. Specifically, we recommend that the Agency:

a) Monitor and enforce the consistent use of logical and physical access controls, including remote and temporary access, over all TSP systems and system resources to include the monitoring of access authorizations,

removal of separated personnel and the removal or disabling of inactive user IDs, and periodic recertification of user access.

b) Evaluate and appropriately restrict access to powerful system privileges and sensitive system datasets on the mainframe. Monitor the access periodically to ensure consistency with the authorized access.

c) Evaluate and implement consistent log monitoring practices over users with privileged access to TSP systems. On a system by system basis, the evaluation should consider the types of events that should be captured, the frequency with which the events should be monitored, the requirements to support the evaluation of the logs (e.g., management sign-off), the retention period for audit logs, and the incorporation of these requirements into the Agency's procedures. Once approved, the Agency should update, distribute, and enforce the policy.

d) Assign unique user IDs and passwords to database administrator accounts for CODIS, DeDIS, AMI, and CFIS and for domain administrators. In addition, evaluate the appropriateness of multiple domain administrator accounts.

Reason for Recommendation: The TSP systems utilize various hardware and software technologies at multiple locations where consistent administration over these systems is a necessity. The consistent use of logical access administration practices will provide further assurance to the Agency that the TSP systems are being properly managed and maintained.

March 2012 Status: **Partially Implemented.**

a) and c) The Agency recently approved its EISRM Directive, which was designed to address security requirements, roles, and responsibilities and develop a security framework. However, the policy has not yet been fully enforced or distributed to employees and contractors. Access controls and audit and accountability are two of the 20 individual policies referenced in the EISRM Directive. Further, all of these policies remain in draft. Once completed, individual policies and procedures will align to the NIST SP 800-53 control categories.

During fieldwork, we noted that the Agency did have a process in place for administering TSP system accounts; however, we reviewed the

active user access listings for the OmniPay, AG[3], and Omni Security systems as of January 30, 2012, February 21, 2012, and February 23, 2012, respectively, and noted exceptions during our testing. Specifically, we identified 10 separated users, with access to one or more applications, related to these three TSP systems as follows:

- One of the 122 OmniPay users retained access after termination,
- Three of the 715 AG users retained access after termination, and
- Eight of the 836 Omni Security users retained access after termination.

We also noted that while procedures for logging and monitoring mainframe use and administering access had been developed by a contractor, the design of the procedure was weak and lacked approval by Agency management. Specifically, we noted the following weaknesses:

- The mainframe logging procedures lacked detail on the types of events that should be captured, the frequency with which the specific reports and events should be monitored, the requirements to support the evaluation of the logs (e.g., management sign-off), the retention period for audit logs, and the incorporation of these requirements into the Agency's procedures.
- A daily mainframe security violation report was generated, but review of the report was not evidenced or retained.
- Current access administration procedures relied on email approvals for access requests, which resulted in inconsistent documentation for requesting system access.
- Team leads were allowed to approve their own access during the annual recertification review.
- New hires and terminated employees were not reviewed as part of the recertification process.

Additionally, we noted that the annual access recertification for 2011 was not completed in a timely manner. Although the annual recertification began in July 2011, as of March 2012, evidence of completion could not be

[3] AG is the Agency's document imaging system that replaced PowerImage in 2011.

provided as several teams had not yet replied to initial requests by the Security team or were just beginning the recertification process. As such, this portion of the recommendation remains open.

b) During our testing over mainframe privileged accounts, bypass privileges, and sensitive datasets, we noted that Agency has made progress in restricting bypass privileges and limiting access to mainframe system privileged accounts. However, we determined that individuals under the JASI profile had excessive access to several 1) key system libraries and datasets, and 2) key application datasets during our review of these critical datasets. As such, this portion of the recommendation remains open.

d) The Agency had not made progress in assigning unique user IDs and passwords to database administrator accounts and domain administrator accounts. Additionally, an evaluation of the appropriateness of multiple domain administrator accounts had not been performed. As such, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

2007 Computer Access and Technical Security Controls Recommendation No. 4:

Original Recommendation: To strengthen the configuration of logical access over the TSP systems, the Agency should evaluate and apply a level of technical controls over the TSP application and general support systems as required by the TSP System Security Plan. Specifically, we recommend the Agency:

a) Evaluate the configuration of the technical controls of current TSP systems and correct the technical security configuration gaps (i.e., password settings, account policy and group policy settings, time-out settings and auditable events) that can be immediately addressed. In instances where the gaps cannot be addressed due to a limitation of the current technology, or where the business disruption to the change has a negative impact, the Agency should develop and implement compensating operational controls to address the weaknesses identified with the technical controls.

b) Establish, document and enforce configuration standards for the mainframe system security settings and sensitive dataset configurations.

Reason for Recommendation: The TSP systems utilize various hardware and software technologies at multiple locations where consistent configuration over these systems is a necessity. The consistent use of logical access configuration practices will provide further assurance to the Agency that the TSP systems are being properly managed and maintained.

March 2012 Status: **Partially Implemented.**

a) An evaluation of the configuration of the technical controls of current TSP systems and the correction of the technical security configuration gaps had not been completed. To compensate for this situation, the Agency implemented a Cisco Security Monitoring, Analysis and Response System (Cisco system), an Intrusion Detection System (IDS), and Intrusion Prevention System (IPS); however, alerts were not enabled to alert information technology (IT) personnel of security issues. While the Cisco system was not actively monitored, it was available for retrospective analysis. As such, this portion of the recommendation remains open.

b) A mainframe configuration baseline was established and documented. However, the document did not specifically define the applicable system, the date of documentation, or whether it had been approved by Agency management. We further determined that it did not contain evidence that it was reviewed and updated on a periodic or as needed basis. Through inspection of the mainframe configurations, we noted that 3 of the 31 configuration settings did not meet either the documented baseline or recommended best practices. As such, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

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:

a) Conduct a comprehensive risk assessment over the controls in place over the TSP systems and related system components using NIST and

Federal Information Processing Standards (FIPS) guidance. This assessment should include establishing a set of minimum security control requirements in line with the Agency's assessed information criticality and sensitivity ratings. After the minimum controls have been identified, an assessment of the controls in place should be performed in order to identify control design and operational effectiveness gaps and weaknesses.

b) Conduct a Privacy Impact Assessment (PIA) over the TSP system following Privacy Act and OMB guidance. For any weaknesses identified, corrective action plans should be created to actively track progress of remediation of any weaknesses.
c) Formalize the designation of a Chief Privacy Officer with the responsibility for monitoring and enforcing privacy related policies and procedures, and clearly identify privacy related roles and responsibilities for 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: A current comprehensive risk assessment over the TSP systems and related system components had not been completed by the Agency. We also noted that a PIA had not been performed over the TSP system and a Chief Privacy Officer with the responsibility for monitoring and enforcing privacy related policies and procedures had not been designated. In addition, policies and procedures for protecting and using sensitive and personally identifiable information had not been fully identified nor created. Lastly, information security and privacy weaknesses identified through internal or external assessments were not being centrally tracked and managed nor were corrective action plans with milestones and target end dates for remediation being included.

March 2012 **Partially Implemented.**

Status: Part c of the original recommendation was closed in the report entitled "Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings as of July 30, 2010;" therefore, it was not included in the scope of our 2011 performance audit.

a) The Agency had not performed a comprehensive risk assessment over the controls in place over the TSP systems and related system components using NIST and FIPS guidance. Additionally, policies related to certification and accreditation and risk assessment requirements had not been finalized and approved. While the Agency recently approved its EISRM Directive, which was designed to address security requirements, roles, and responsibilities and develop a security framework, the policy was not yet fully enforced or distributed to employees and contractors, and related subsequent policies remained in draft status. As such, this portion of the recommendation remains open.
b) The Agency communicated that it understands the importance of a PIA as an integral part of the Agency's overall risk assessment process. However, a formal PIA had not been performed. As such, this portion of the recommendation remains open.
d) The Agency had not formalized policies related to incident response or the process for handling incidents related to the breach of information such as PII. Therefore, no formalized policies existed that addressed the protection of sensitive and PII information or related to a PII incident response and notification plan. While the Agency recently approved its EISRM Directive, which was designed to address security requirements, roles, and responsibilities and develop a security framework, the policy was not yet fully enforced or distributed to employees and contractors, and related subsequent policies remained in draft status. As such, this portion of the recommendation remains open.
e) System specific POA&Ms had not been implemented by the Agency to track identified security weaknesses, corrective action plans, milestones, and target completion dates. Certification and accreditation policies and procedures, including POA&M requirements, remained in draft status and had not been formalized and approved by the Agency. As such, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

2008 Computer Access and Technical Security Controls Recommendation No. 2:

Original Recommendation: To strengthen the controls over participant identity management, we recommend that the Agency conduct a formal E-Authentication risk assessment using relevant NIST and OMB guidance to evaluate the authentication level for the TSP Web. The results from this assessment should be considered for incorporation into the requirements for the Agency's solicitation of a technical software product for authenticating participant's identity to the TSP Web. Lastly, participant account credentials should be encrypted at rest in OmniPlus recordkeeping system.

Reason for Recommendation: The Agency has not performed an E-Authentication risk assessment to further evaluate authentication requirements and identify current weaknesses such as participant credentials being stored as open text in the OmniPlus recordkeeping system. As the tools and techniques for perpetrating attacks on information systems and data continue to evolve, the management, technical, and operational controls needed to verify participant and transaction authenticity and protect identities, particularly over open networks like the Internet, must keep pace.

March 2012 Status: **Partially Implemented.**
An E-Authentication risk assessment analysis had not been conducted to evaluate the authentication level for the TSP Web. While Agency management agrees that participant account credentials should be encrypted at rest in the OmniPlus recordkeeping system, these controls have not been implemented. The Agency is currently researching maturing technologies for encryption solutions and in the interim, plans to protect the credentials in question through access rules and authentication procedures. However, these access rules and procedures have not yet been implemented.

Disposition: **Recommendation Open**.

C. 2011 Findings and Recommendations

While conducting our performance audit over TSP computer access and technical security controls, we identified four new findings and developed related recommendations. EBSA requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

General Policy and Procedure Weaknesses

During our audit work, we determined that general policy and procedure weaknesses existed over TSP computer access and technical security. On September 22, 2011, Agency management approved the EISRM Program Directive, a framework for addressing security requirements, roles, and responsibilities. However, the directive is awaiting distribution to Agency employees and contractors. Furthermore, the EISRM Program Directive will be supplemented by individual policies and procedures that will align to the NIST SP 800-53 control categories; however, these policies, listed below, are currently in draft status, and no timeline has been established for their completion.

- Access Control
- Audit and Accountability
- Certification and Authorization
- Identification and Authentication
- Incident Response
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Risk Assessment
- Security Planning
- Awareness and Training
- System and Information Integrity

According to Agency personnel, the Agency did not dedicate the resources needed to finalize and distribute the key IT related policies. For policies and procedures to be effective, they should be formalized and communicated appropriately. Without complete policies, responsibilities and controls are not appropriately documented, disseminated, implemented, or monitored. Therefore, information systems may be more susceptible to improper access, use, or loss of sensitive information.

Per the Agency's *Enterprise Information Security and Risk Management Program and Policy Authorization Directive Number 61,* dated September 22, 2011, page 23, "Enterprise Information Security and Risk Management (EISRM) Program Charter: […] (c) EISRM Program Component Three: Policy documents based on the Management, Operational, and Technical controls as mandated by FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* and catalogued in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations (current revision, as amended), and/or any other policy documents deemed necessary and sufficient by the Enterprise Risk Management Committee (i.e., the Risk Executive Function) and approved by the Executive Director. Policies authorized under this Directive SHALL include those addressing the following control families and/or security categories: Access Control (AC); Audit and Accountability (AU); Certification and Authorization (CA); Identification and Authentication (IA); Incident Response (IR); Media Protection (MP); Personnel Security (PS); Physical and Environmental Protection (PE); Risk Assessment (RA); Security Planning (PL); Awareness and Training (AT); and System and Information Integrity (SI)."

1. **To strengthen general policy and procedure weaknesses over TSP computer access and technical security, the Agency should:**
   a) **Distribute the EISRM Directive to Agency employees and contractors.**
   b) **Complete the development and documentation of and then communicate policies and procedures for each key component of the TSP system related to:**
      - **Access Control**
      - **Audit and Accountability**
      - **Certification and Authorization**
      - **Identification and Authentication**
      - **Incident Response**
      - **Media Protection**
      - **Personnel Security**
      - **Physical and Environmental Protection**
      - **Risk Assessment**
      - **Security Planning**
      - **Awareness and Training**
      - **System and Information Integrity**

The documentation, dissemination, implementation, and monitoring of TSP policies and

procedures will assist TSP personnel and support the prevention of improper access, use, or loss of sensitive information from TSP systems.

Lack of Certification and Accreditation Review

During our audit work, we determined that the Agency had not certified or accredited any of the TSP system components. We did note that the certification and accreditation had been started for the ThriftLine, TSP's integrated voice response system; however, the related documentation was still in draft form.

According to Agency personnel, the Agency did not dedicate the resources needed to certify and accredit the aforementioned systems. If information systems do not go through a certification and accreditation process, an increased risk exists that information systems may not provide the appropriate level of controls that are necessary for the protection of the information system. Additionally, Agency management may not be aware of the security risks posed by the use of the systems. As a result, the potential exists that systems are operating in a production environment without appropriate controls or management oversight.

The Agency's, *Enterprise Information Security and Risk Management Program and Policy Authorization Directive* Number 61, dated September 22, 2011, page 11, states: "Continuous Authorization (as per the NIST SP 800-37) of all new and existing Information Systems, including:

a) Creation of a Security Assessment Report (SAR) for each Information System prior to Authorization of each Information System and updating of the SAR thereafter throughout the SDLC;
b) Certification by the Certification Agent (i.e., the ISSM) of the accuracy of each Information System Authorization package (including the Security Plan and the Security Assessment Report) and the effectiveness of the security controls whenever making a formal recommendation for or against issuing a new, or continuing a pre-existing, Authorization to Operate (ATO) by the Authorizing Official;
c) Creation and continuous maintenance of a Plan of Actions and Milestones (POA&M) document to schedule mitigation of any residual risks deemed unacceptable by the System Owner or Authorizing Official."

On page 18, it establishes a risk response process and mitigation strategy that includes, "A Comprehensive Certification and Authorization (C&A) process, designed to mitigate potential security impacts identified in the Security Categorization and Initial Risk Assessment for an

Information System, as described in 7(b)(2)(A) above. The C&A process shall result in the creation of several additional documents required for the issuance of an Authorization to Operate:

a) System Security Plan (SSP), including:
    a. All security controls as indicated by the Security Categorization baseline,
    b. Information System Boundaries, and
    c. Security Concept of Operations (SecConOps);
b) Privacy Impact Assessment (PIA) (subject to final approval by the Privacy Officer);
c) Interconnection Security Agreements (ISAs) and related Memorandums of Understanding (MOUs);
d) System Test and Evaluation (ST&E) plans and test results;
e) Security Assessment Report detailing residual risk;
f) Plan of Actions and Milestones (POA&M) Document detailing planned mitigations to residual risk; and
g) System-specific Disaster Recovery Plans (DRPs) and related test plans (for Mission Critical Systems)"

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* dated February 2004, (FIPS 199) page 1, states: "These standards shall apply to: (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 199 whenever there is a federal requirement to provide such a categorization of information or information systems."

FIPS 199, page 1, further states, "This publication establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."

2. The Agency should perform a certification and accreditation review for each key component of the TSP system, and complete its certification and accreditation review of the ThriftLine, including finalizing the related documentation.

Performing a certification and accreditation on the key components of the TSP system will allow the Agency to identify and provide the appropriate level of controls that are necessary for the protection of the information system. Additionally, certifying and accrediting TSP system components will allow the Agency to identify and manage the risks associated with the TSP system and implement the appropriate controls needed to mitigate those risks.

Lack of a Vulnerability Management Program

During our internal and external vulnerability assessment, we determined that multiple application security patches designed to remediate vulnerabilities in the TSP system environment were not implemented. Many of these patches were security vulnerability fixes that were released to the public years ago.

The Agency communicated that scanning of security vulnerabilities was performed over the TSP system environment. However, the Agency did not actively monitor and remediate the vulnerabilities because of deficiencies in its oversight policies and procedures.

This lack of a vulnerability management program to continuously monitor and assess the security posture of the Agency leads to organizational lack of awareness of potential direct threats and risks associated with the Agency's systems. This lack of awareness directly impacts the organization's risk management framework as risks arise when security vulnerabilities become untraceable and unknown to the organization. Additionally, a lack of a continuous vulnerability management program increases the potential for direct exploitation, as new vulnerabilities are discovered daily.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, states:

"RA-5 Vulnerability Scanning
Control: 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)."

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

a) Policies governing a vulnerability management program.

b) Procedures for the usage of the security tools to continuously monitor the deployment of security patches and assist in remediation efforts.

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

d) Mechanism for tracking senior management approval for risk management decisions to transfer, mitigate, or accept risks related to identified vulnerabilities.

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.

Lack of a Configuration Management Program

During our audit, we determined that the Agency had not developed and implemented a configuration management program, which resulted in a lack of formal system security baselines. According to Agency personnel, the Agency did not dedicate the resources needed to develop and implement a configuration management program.

This lack of a formalized configuration management program leads to unknown configuration settings, inconsistencies across the organization's technical environment, challenges in managing these systems, and violations with the Agency's risk strategy. Without security baselines and enforcement of those baselines, an organization is unable to develop the perquisites required for developing a change management program and framework.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, states:

"CM-2 Baseline Configuration
Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9."

4. **The Agency should develop and implement a configuration management program that contains the following elements for security baselines:**
   a) **Policies directing the selection and application of management approved security baselines.**
   b) **Procedures for selection and application of management approved security baselines.**
   c) **Mechanism for review of security baselines in accordance with an organizationally defined frequency.**
   d) **Mechanism for updating security baselines upon changes.**

Implementation and review of security baselines will help the Agency monitor system changes in

order to remediate, transfer, or accept the risks associated with those changes.

D. Summary of Open Recommendations

2007 FEDERAL RETIREMENT THRIFT INVESTMENT BOARD ADMINISTRATIVE STAFF RECOMMENDATION

FUNDAMENTAL CONTROL RECOMMENDATION

1. To strengthen information security over laptops and portable devices, the Agency should:
   e) Finalize and disseminate the Personally Identifiable Information (PII) Incident Response and Notification Plan.

2007 RECOMMENDATIONS

FUNDAMENTAL CONTROL RECOMMENDATIONS

1. To strengthen the TSP security program, the Agency should document, finalize and fully implement the necessary security policies and procedures to enforce the TSP security program. Specifically, we recommend that the Agency:
   a) Complete and implement the Thrift Savings Plan Data Security Policy as part of the TSP security program.
   b) Update the TSP Electronic Media Management Policy to clarify the Agency's approved method for sanitizing media and TSP supporting equipment.
   c) Update the TSP System Security Plan to include provisions for training incident response personnel and testing the Agency's incident response capability. Additionally, the Agency should periodically test the incident response capability.
   d) Monitor and enforce the TSP policy for using the Internet, personal software, and peer-to-peer software for contractor locations.

2. To strengthen the controls over the TSP's most privileged users and access to sensitive areas of the system, the Agency should document, finalize and fully implement the necessary procedures to enforce logical access requirements over the privileged users and access to sensitive areas of the TSP systems. Specifically, we recommend that the Agency:
   a) Document and implement procedures to log and monitor system administrator activities such as changes to security parameters and configurations.

b) Complete and implement access administration procedures for granting access to sensitive and critical datasets, periodically recertifying mainframe accounts, and monitoring and reviewing mainframe access privileges.

3. To strengthen the administration of logical and physical access over TSP systems, the Agency should evaluate, implement and monitor the logical and physical access administration over TSP accounts in the TSP systems. Specifically, we recommend that the Agency:
   a) Monitor and enforce the consistent use of logical and physical access controls, including remote and temporary access, over all TSP systems and system resources to include the monitoring of access authorizations, removal of separated personnel and the removal or disabling of inactive user IDs, and periodic recertification of user access.
   b) Evaluate and appropriately restrict access to powerful system privileges and sensitive system datasets on the mainframe. Monitor the access periodically to ensure consistency with the authorized access.
   c) Evaluate and implement consistent log monitoring practices over users with privileged access to TSP systems. On a system by system basis, the evaluation should consider the types of events that should be captured, the frequency with which the events should be monitored, the requirements to support the evaluation of the logs (e.g., management sign-off), the retention period for audit logs, and the incorporation of these requirements into the Agency's procedures. Once approved, the Agency should update, distribute, and enforce the policy.
   d) Assign unique user IDs and passwords to database administrator accounts for CODIS, DeDIS, AMI, and CFIS and for domain administrators. In addition, evaluate the appropriateness of multiple domain administrator accounts.

4. To strengthen the configuration of logical access over the TSP systems, the Agency should evaluate and apply a level of technical controls over the TSP application and general support systems as required by the TSP System Security Plan. Specifically, we recommend the Agency:
   a) Evaluate the configuration of the technical controls of current TSP systems and correct the technical security configuration gaps (i.e., password settings, account policy and group policy settings, time-out settings and auditable events) that can be immediately addressed. In instances where the gaps cannot be addressed due to a limitation of the current technology, or where the business disruption to the change has a negative

impact, the Agency should develop and implement compensating operational controls to address the weaknesses identified with the technical controls.

b) Establish, document and enforce configuration standards for the mainframe system security settings and sensitive dataset configurations.

2008 RECOMMENDATIONS

FUNDAMENTAL CONTROL RECOMMENDATIONS

1. To strengthen the controls over the security and privacy program we recommend that the Agency:
   a) Conduct a comprehensive risk assessment over the controls in place over the TSP systems and related system components using NIST and FIPS guidance. This assessment should include establishing a set of minimum security control requirements in line with the Agency's assessed information criticality and sensitivity ratings. After the minimum controls have been identified, an assessment of the controls in place should be performed in order to identify control design and operational effectiveness gaps and weaknesses.
   b) Conduct a Privacy Impact Assessment (PIA) over the TSP system following Privacy Act and OMB guidance. For any weaknesses identified, corrective action plans should be created to actively track progress of remediation of any weaknesses.
   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.

2. To strengthen the controls over participant identity management, we recommend that the Agency conduct a formal E-Authentication risk assessment using relevant NIST and OMB guidance to evaluate the authentication level for the TSP Web. The results from this assessment should be considered for incorporation into the requirements for the Agency's solicitation of a technical software product for authenticating participant's identity to the TSP Web. Lastly, participant account credentials should be encrypted at rest in OmniPlus recordkeeping system.

2011 RECOMMENDATIONS

FUNDAMENTAL CONTROL RECOMMENDATIONS

1. To strengthen general policy and procedure weaknesses existed over TSP computer access and technical security, the Agency should:
   i. Distribute the EISRM Directive to Agency employees and contractors.
   ii. Complete the development and documentation of and then communicate policies and procedures for each key component of the TSP system related to:
      - Access Control
      - Audit and Accountability
      - Certification and Authorization
      - Identification and Authentication
      - Incident Response
      - Media Protection
      - Personnel Security
      - Physical and Environmental Protection
      - Risk Assessment
      - Security Planning
      - Awareness and Training
      - System and Information Integrity

2. The Agency should perform a certification and accreditation review for each key component of the TSP system, and complete its certification and accreditation review of the ThriftLine, including finalizing the related documentation.

3. The Agency should develop and implement a vulnerability management program that contains the following elements:
   a) Policies governing a vulnerability management program.
   b) Procedures for the usage of the security tools to continuously monitor the deployment of security patches and assist in remediation efforts.
   c) Mechanism for tracking and reporting security patch deployments such as POA&Ms.
   d) Mechanism for tracking senior management approval for risk management decisios to transfer, mitigate, or accept risks related to identified vulnerabilities.

4. The Agency should develop and implement a configuration management program that

contains the following elements for security baselines:

a) Policies directing the selection and application of management approved security baselines.
b) Procedures for selection and application of management approved security baselines.
c) Mechanism for review of security baselines in accordance with an organizationally defined frequency.
d) Mechanism for updating security baselines upon changes**.**

APPENDIX A

KEY PERSONNEL INTERVIEWED

While performing fieldwork, we inquired of the following personnel:

A. Federal Retirement Thrift Investment Board's Staff

Harley Becker	Information Technology (IT) Specialist
Anne Beemer	Controller, Office of Finance
Brack Boone	Auditor, Control Group
Susan Crowder	Deputy Chief Financial Officer
Roy Friend	Senior IT Advisor
Sheila Fry	Supervisory IT Specialist
Walter Halfmann	Senior Systems Analyst
Khatrina Higgs	TSP Accounting Team Lead
Bruce Jones	IT Specialist, Information Security
Troy Poppe	Deputy Chief Information Officer (CIO), Operations
Kelly Powell	Human Resources Program Manager
Tee Ramos	Supervisory IT Specialist
Mark Walther	CIO

B. Serco, Inc.

Lori Hogan-Waterman	Mainframe Security, Team Lead
Ted Keys	Database Administrator (DBA) Team Lead
Crystal Lewis	Accounting Project Lead
Ken Trinh	Network Tech Support

C. ICF Jacob & Sundstrom

Patricia Budzynski	System Programmer-Project Manager

D. Keane Federal

Bruce Milner	Database Administrator

E. Savantage Solutions

Joseph Smith	Team Lead

KEY DOCUMENTATION REVIEWED

While performing fieldwork, the following key documentation was reviewed:

- Enterprise Information Security And Risk Management (EISRM) Program Directive, as of September 22, 2011
- EISRM Program Directive Approval, as of September 22, 2011
- Draft Access Control Policy, as of January 26, 2012
- Draft Audit Trails Policy, as of January 26, 2012
- Draft Certification and Authorization Policy, as of January 26, 2012
- Draft Identification and Authentication Policy, as of January 26, 2012
- Draft Incident Response Policy, as of January 26, 2012
- Draft Media Protection Policy, as of January 26, 2012
- Draft Personnel Security Policy, as of January 26, 2012
- Draft Physical and Environmental Protection Policy, as of January 26, 2012
- Draft Risk Assessment Policy, as of January 26, 2012
- Draft Security Planning Policy, as of January 26, 2012
- Draft Security Training and Awareness Policy, as of January 26, 2012
- Draft System and Information Integrity Policy, as of January 26, 2012
- April 7, 2009 Agency Memorandum, Information Security Documents, Priority 1
- March 17, 2008 Agency Memorandum, Applicability of OMB Circular No. A-130
- March 21, 2005 Agency Memorandum, Federal Information Security Management Act of 2002 (FISMA)
- June 3, 2008 Agency Memorandum, Agency Compliance with Several Technology Related Statutes/Guidance
- Serco Inc. Security Applications Administrators Procedures, as of November 2011
- Minimum Baseline Standards, Top Secret Release 14, by Serco Inc.
- Mainframe TSS Reports, as of February 3, 2012
- TSP Critical Dataset Descriptions
- Codis Dedis User Listing, as of February 21, 2012
- AG User listing, as of February 21, 2012
- Omni Pay User Listing, as of January 3, 2012
- Omni Security (including OmniPlus and PSR) User Listing, as of February 23, 2012
- Savantage User Listing, as of December 28, 2011
- Listing of Contractors and Sub-Contractors, as of February 7, 2012

APPENDIX C

ENTRANCE AND EXIT CONFERENCE ATTENDEES

An overall entrance conference, covering the entire FY 2011 Thrift Savings Plan (TSP) audit plan and proposed schedule, was held at the Agency on October 18, 2010. Attendees were as follows:

A. Federal Retirement Thrift Investment Board's Staff (Agency)

Anne Beemer	Controller, Office of Finance
Mark Hagerty	Chief Information Officer (CIO)
Penny Moran	Director, Office of Benefit Services
Jim Petrick	Chief Financial Officer
Karrenthya Simmons	Internal Auditor

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance

C. KPMG LLP

Heather Flanagan	Partner
Derek Thomas	Manager
Greg Schuster	Manager
Michele Ho	Computer Systems Analyst

An entrance conference, specifically covering the TSP computer access and technical security controls audit, was held at the Agency on December 15, 2011. Attendees were as follows:

A. Federal Retirement Thrift Investment Board's Staff (Agency)

Anne Beemer	Controller, Office of Finance
Brack Boone	Auditor
Roy Friend	Senior Information Technology (IT) Advisor
Sheila Fry	Technical Planning Manager
Mark Hagerty	Senior IT Advisor, Former CIO
Bruce Jones	Information Security Program Manager

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

Troy Poppe	Deputy CIO, Operations
Tee Ramos	Software Applications Manager
Susan Smith	Deputy CIO, Applications

B. KPMG LLP

James DeVaul	Partner
Tyler Harding	Computer Systems Analyst
Rachel Briskman	Computer Systems Analyst
Patricia Farley	Jr. Computer Systems Analyst

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

An exit conference was held on June 19, 2012 with the Agency. Attendees were as follows:

A. Federal Retirement Thrift Investment Board's Staff (Agency)

Brack Boone	Auditor
Sheila Fry	Technical Planning Manager
Bruce Jones	Information Security Program Manager
Troy Poppe	Deputy Chief Information Officer (CIO) Operations
Karrenthya Simmons	Auditor
Mark Walther	CIO

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance
Ian Dingwall	Chief Accountant

C. KPMG LLP

Heather Flanagan	Partner
James DeVaul	Partner
Derek Thomas	Senior Manager
Alvamerry Schaefer	Computer Systems Analyst