Employee Benefits Security Administration

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

As of October 7, 2009

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Members of the Federal Retirement Thrift Investment Board
Washington, DC

Ian Dingwall
Chief Accountant
U.S. Department of Labor, Employee Benefits Security Administration
Washington, DC

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 prior year recommendations related to the Thrift Savings Plan (TSP) mainframe operations, computer access and technical security, and laptop security at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency). Our procedures were performed at the Agency's headquarters from March 19, 2009 through October 7, 2009. Our scope period for testing was April 17, 2008 to August 30, 2009.

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 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 audit objectives. Criteria used for this engagement is defined in EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes security related laws and regulations and industry best practices as defined by the National Institute of Standards and Technology (NIST). The detailed objectives for this engagement are enumerated within Section I.A.

The Agency manages an entity-wide information security program that helps support the mission of the TSP. Inherent to this security program are layers of physical and logical security related

policies, procedures and controls designed to help prevent and detect unauthorized access to TSP systems. As part of its system modernization investment, we noted that the Agency has made certain progress to address prior year recommendations related to improving the security programs policies and procedures, enforcing logical access controls, establishing privacy program requirements, and securing Agency laptops and portable devices. In addition, the Agency continues its efforts to upgrade hardware to increase processing capacity, strengthen its vulnerability and patch management process, and evaluate solutions to strengthen participant web-based authentication.

Overall, based on the interviews conducted (Appendix A), documentation inspected (Appendix B), and test procedures performed within the FY 2009 Computer Access Controls and Technical Security Controls audit program guides, we conclude that the Agency has not fully implemented corrective action for any of the eight open recommendations we assessed. To strengthen the Agency's security and information technology (IT) program, further efforts are needed to more timely implement all prior recommendations, as described in Section III of this report. For the open recommendations from 2005 through 2008, the Agency has plans to implement the necessary corrective actions through modernization and continuing efforts to complete, distribute, and enforce information security policies and procedures. The security program as a whole is designed and implemented to help TSP fiduciaries ensure that management, operational, and technical controls are in place to protect TSP data and system resources. Timely implementation is strongly recommended to address these previously reported recommendations and to strengthen certain management, operational, and technical controls over the TSP security and privacy programs.

Specifically, we assessed the status of the following prior year recommendations:

- One was reported in the "Post Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005";
- One was reported in the "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, June 30 2007";
- Four were reported in the "Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, March 30, 2007"; and

- Two were 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 year recommendations. In summary, while the Agency has made progress to implement these recommendations, we report that seven recommendations have been partially implemented and remain open, and one recommendation has not been implemented and remains open.

Section I of this report discusses the EBSA's objectives, scope and methodology, and report organization. Section II is an overview of the TSP program and a description of the control areas considered during this performance audit. Section III presents the details that support the status of the 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, respectively, during our performance audit. We discussed these 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 or partially concurred with all open recommendations (Appendix D).

This performance audit did not constitute an audit of 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 FIRM SIGNATURE

Current Date

I. INTRODUCTION

A. Objectives

KPMG LLP was contracted by the U.S. Department of Labor, Employee Benefits Security Administration (EBSA) to perform services under Section 8477(g) of the Federal Employees' Retirement System Act (FERSA) of 1986, as amended. These services included a performance audit to determine the status of prior year recommendations related to the Thrift Savings Plan (TSP) mainframe operations, computer access and technical security, and laptop security at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency).

The specific objectives of this performance audit were to determine the status and report on the Agency's progress in implementing the following prior year recommendations:

- "Post Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005," No. 2005-1, Service Level Reporting Requirements in Contractor Statements of Work;
- "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, June 30 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 EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which is designed to comply with the *Government Auditing Standards* issued by the Comptroller General of the United States. 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 help assist team members in developing a collective understanding of the activities and controls associated with the technical architecture and computer access controls over several local area networks and applications that comprise the 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 tests of controls. We conducted these test procedures primarily at the Agency's headquarters.

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.

When our test procedures required us to select a sample of items from a population for testing, we used a judgmental sample selection methodology. Accordingly, our conclusions are applicable to the sample we tested and were not extrapolated to the population.

[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 800-12, 800-14, 800-18, 800-40, 800-41, 800-44, 800-47, 800-48, 800-53, and 800-63.

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

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 that includes a description of the roles and responsibilities, policies and procedures, and the security controls monitoring function that is in place at the Agency and over the TSP program. Section III presents a detailed discussion of all recommendations.

II. OVERVIEW OF THE TSP ACCESS CONTROLS AND SECURITY

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act (FERSA) of 1986, 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 August 31, 2009, had approximately $229 billion in assets and 4.2 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 of the TSP systems. An integrated component of the administration of TSP operations and these services is to provide for the necessary controls to help maintain the confidentiality, integrity, and availability of the 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. At the perimeter of the TSP architecture, firewalls have been put in place to control the flow of network services; and intrusion detection systems (IDS) and intrusion prevention systems (IPS) have been put into place to detect and prevent unauthorized intrusion threats. On the inside of

---

[2] Source: frtib.gov, September 2009 Board Meeting Minutes.

the TSP perimeter (i.e., behind the firewalls), networks deploy anti-virus, anti-spyware and anti-malware software protection to reduce the risk of threats to the TSP systems.

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, 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. The contract's statement of work (SOW) requires Serco to provide the Agency with a monthly report containing system performance, capacity analysis, and service level operations and performance, and a quarterly report containing all service level achievement.
- *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 to SunGard for OmniPlus and to Jacob and Sundstrom (JASI) for system engineering and maintenance duties.

C. TSP Security Program

1. TSP Security Policies and Procedures

The Agency's foundational documents related to information security have historically been the TSP Security Plan and the draft TSP Data Security policy. However, the Information Security Program Manager has been charged with evaluating the Agency's information security program policy and procedures requirements and establishing the structure for the policies and procedures

for the TSP security program to follow. The Information Security Program Manager has drafted several documents for the TSP security program, which include the Agency's Information Security Program Directive and the Information Security Program Policies and Procedures documents. The purpose of the Agency's Information Security Program Directive is to set forth the policy of the Agency and establish the Agency's Information Security Program and, to the extent to which the Board determines is applicable, congruence with the *Federal Information Security Management Act* (FISMA). This document also outlines roles and responsibilities for the security program. The purpose of the Information Security Program Policies and Procedures document 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. To facilitate the development, administration, and maintenance of the Agency's information security policies, the Information Security Program Manager has proposed that the policies follow a logical hierarchy. There are three primary categories for the policies:

- *Security Program* – These policies provide guidance for development and operation of the core components of the Agency's information security program, and are derived from FISMA program requirements.
- *Information Resources* – These policies provide guidance on securing specific types of information resources, such as servers, applications, databases, and connectivity components.
- *Security Practices* – These policies provide guidance on implementation and operation of security protections that apply across all Agency information resources.

According to the Information Security Program Manager, each policy category aligns to and contains descriptions of the minimum control requirements as prescribed by the National Institute of Standards and Technology (NIST) Special Publication 800-53[3] control families and control categories. The revised policies are planned to cover the following categories: Acceptable Use of Information Resources, Information Resource Classification, Risk

[3] To comply with this Federal standard, agencies must first determine the security category of their information system in accordance with the provisions of Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.

Management, Security Awareness and Training, Incident Reporting, Incident Response, System Security Plans, Certification and Accreditation, Vulnerability Testing, Contingency Planning, Access Control, Identification and Authentication, Audit Trails, Antivirus, Encryption, Personnel Security, Physical and Environmental Controls, Change Control, Backup and Recovery, Patch Management and System Updates, Server Security, Mobile Computing, Network Security, Perimeter Security, Remote Access, Telephony Security, Wireless Security, Systems Development, Electronic Mail, Database Security, Media Management, Password Management, and Asset Management. These revised policies will address security procedures that had previously been identified as incomplete areas, such as logging and monitoring system administrator procedures; granting and removing access to TSP systems (i.e., networks, mainframe, and applications) and sensitive mainframe datasets; recertifying TSP system and mainframe user accounts; conducting background investigations and requiring non-disclosure agreements for accessing TSP-related information; handling electronic media; incident response handling and training; monitoring and using the Internet, personal software, and peer to peer software; handling personally identifiable information (PII) incidents; and establishing configuration requirements for all TSP system components.

2. TSP Security Controls Monitoring

The Agency monitors the TSP security program by evaluating security controls in operation and by implementing security controls designed to prevent and detect unauthorized security incidents. For example, the Agency uses a risk assessment process to aid in determining whether adequate security measures are in place to identify threats and vulnerabilities and in determining the effectiveness of current or proposed security safeguards. In addition, the Agency performs routine site visits to the production and backup data centers to evaluate the controls in operation. Routine site visits (scheduled or unscheduled) are incorporated in the statements of work for the data center contractors.

The Agency has also incorporated Plans of Action and Milestones (POA&Ms) to monitor weaknesses identified through assessments of systems and sites that are operated as part of the TSP. The POA&Ms include the details of the resources required to accomplish the plan to address the weaknesses, any milestones in meeting the task, and scheduled completion dates for the milestones.

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. These duties would typically be performed by the designated system or security administrator. Duties include granting, revoking and removing user access to systems; monitoring user access to sensitive system regions or data; evaluating the appropriateness of access privileges and actions performed on the system; and monitoring the actions and events of users.

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. However, temporary access can be granted pending the successful results of a background investigation with permanent access being granted upon completion of a successful background investigation. After initial access has been authorized by the Agency, the Security Administrator will request additional access with the individual administrators to the authorized subsystems.

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 are 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 PII), application controls are designed to protect the TSP subsystems by restricting direct access to the DBMS. Restricting access of the security administrator functions to designated personnel protects the confidentiality, integrity, and availability of the resident data. Security administrator access and responsibilities are to be controlled by assigning a primary and backup administrator to the LANs, TSP subsystem applications, and the TSP DBMS.

(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. Access to these sensitive datasets is assigned on a least-privilege basis by the Security Administrator. Full access (i.e., ALTER or UPDATE) to these datasets is typically restricted to system programmers and security administrators. Restricted access (i.e., READ) is granted only to those with a need-to-know. The mainframe also contains configurable settings for general system-wide mainframe security. These settings help 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 an 8-character Web password. Each account number is linked to a participant's social security number to create the proper credential (in addition to providing the correct password). The account number must be truly unique at the time it is assigned or changed by the participant, meaning that it can not be associated with another participant at the same point in time that it is being requested. Access to the web site and Thriftline uses the same account credentials, which also include a personal identification number (PIN) to further supplement the authentication of the participant. The Agency posts security-related information in the frequently asked questions (FAQs) on the TSP web site to inform participants about Internet browser security and account access risks with security precautions for accessing their accounts over the Internet.

As part of strengthening the Agency's risk management strategy for the TSP Web, the Agency engaged a consulting firm to assist in a widespread evaluation of current IT security technologies

and services that can help prevent or detect the vulnerabilities exploited through current and emerging threats, including social engineering. This evaluation included the assessment of multiple account access authentication methods. The Agency has purchased adaptive authentication software that will monitor risk behavior and is currently evaluating implementation options for the software with the current TSP Web redesign effort, which is scheduled for completion by September 30, 2010.

4. Agency Laptops and Portable Device Security

The Agency has made an investment in its ongoing efforts to implement a security program designed to protect access through portable devices to TSP resources and the privacy of participant and TSP-related data. At the Agency, laptops and other portable devices (e.g., Blackberry devices) are used by authorized individuals to perform their duties on an as needed basis. Biometric Universal Serial Bus (USB) flash drives are also used on an as needed basis to store and secure data. The Agency controls the manner by which laptops and portable devices are distributed and accessed through various operational and technical controls. The Agency has invested in improving encryption of hard drives on laptops that have been issued by the Agency, enforcing the use of virus scanning on all external laptops and portable devices prior to being allowed connection to the Agency's network, evaluating the use of cable locks and other anti-theft techniques for Agency-issued laptops, strengthening the password composition rules for portable devices, and finalizing and disseminating the PII Incident Response and Notification Plan.

The Agency implemented the Utimaco SafeGuard Enterprise (Utimaco) software[4] for laptops. This software is configured to require Power-On-Authentication prior to permitting the device to boot and also is configured to encrypt transmissions using Advanced Encryption Standard (AES). The Agency requires that all laptops contain this software prior to issuing them for use.

[4] The Utimaco software provides data protection against unauthorized access, loss or theft of stationary and mobile devices with full disk encryption.

With regard to scanning laptops and portable devices prior to being used at the Agency, the Agency currently directs all contractor or visitor laptops to a "guest" network that has Internet access but does not have access to internal systems or the primary Agency network. This procedure allows the Agency to protect its network from unauthorized access or accidental corruption.

Related to portable device security, password requirements for Blackberries have now been set to have a minimum of eight characters that includes at least one numeric character. Additionally, the Blackberry password must be changed every 90 days, which is consistent with the Agency's requirements for passwords.

The Agency is in the process of revising and drafting policies and procedures that will support the information security and privacy program. The PII Incident Response and Notification Plan is one of the procedures that are under evaluation and revision.

D. TSP Privacy Program

The Agency recognizes that participant information protection is a critical part of its responsibilities. 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. In order to address the Agency's response to potential breaches in releasing PII, the Agency's Information Security Program Manager is revising the PII Incident Response and Notification Plan as part of the overall policy and procedure implementation effort at the Agency.

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) mainframe operations, computer access and technical security, and laptop security at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency). This performance audit consisted of reviewing applicable policies and procedures, and testing manual and automated processes and controls, which included interviewing key personnel (Appendix A), reviewing key reports and documentation (Appendix B), and observing selected procedures. Exhibit III-1 summarizes each recommendation. We discussed these recommendations with the appropriate Agency representatives (Appendix C). The Agency's comments are included as an appendix within this report (Appendix D).

Specifically, we assessed the status of following prior year recommendations:

- One was reported in the "Post Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005";
- One was reported in the "Review of the Policies and Procedures of the Federal Retirement Thrift Investment Board Administrative Staff, June 30 2007";
- Four were reported in the "Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, March 30, 2007"; and
- Two were reported in the "Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, April 16, 2008."

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.

Section III.B documents the status of the prior year recommendations noted above. In summary, while the Agency has made progress to implement these recommendations, we report that seven recommendations have been partially implemented and remain open, and one recommendation has not been implemented and remains open. Exhibit III-1 (next page) summarizes each open recommendation.

EXHIBIT III-1

SUMMARY OF OPEN RECOMMENDATIONS

FUNDAMENTAL CONTROL RECOMMENDATIONS

2005 Mainframe Operations Recommendation:

1. The Agency's Senior Information Security Officer (SISO) should implement service level reporting for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management, consistent with contract requirements.

2007 Federal Retirement Thrift Investment Board Administrative Staff Recommendation:

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

2007 Computer Access and Technical Security 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 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 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 the 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 signoff), 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 Computer Access and Technical Security 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 systems 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.

SUMMARY OF OPEN RECOMMENDATIONS

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 the OmniPlus recordkeeping system.

B. Findings and Recommendations from Prior Reports

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 through October 7, 2009.

2005 Mainframe Operations Recommendation No. 1:

Original Recommendation: The Agency's Senior Information Security Officer (SISO) should implement service level reporting for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management, consistent with contract requirements.

Reason for Recommendation: The Agency's prior Chief Information Officer (CIO) retired in July 2005, and a new CIO was appointed in August, 2005. The TSP systems have been in a state of change since June 2003. The new daily-valued TSP systems were implemented at that time, the OS/390 IBM mainframe was transitioned to a zOS IBM mainframe, and the mainframe operations and disaster recovery locations were transferred to new sites. After the Hurricane Katrina disaster, a sole source contract was awarded to SI International[4] to stand up a new data center. As part of this contract, service level reporting was required but never materialized into contractor deliverables to evaluate the contractor's performance.

October 2009 Status: **Not Implemented.**

The Agency has decided not to enforce service level reporting until it re-competes its mainframe services contract for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management. The Agency plans to include key service level reporting requirements in the new services contract when it is re-competed and awarded, which is

[4] SI International was purchased by Serco Inc. during calendar year 2008.

currently planned for mid-year 2011.

Disposition: **Recommendation Open.**

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 that have been issued by the Agency.
b) Enforce the use of virus scanning 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.
e) Finalize and disseminate the 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.

October 2009 Status: **Partially Implemented.**

a) The Agency has implemented the Utimaco SafeGuard Enterprise (Utimaco) software[5] for laptops. This software is configured to require

[5] The Utimaco software provides data protection against unauthorized access, loss or theft of stationary and mobile devices with full disk encryption.

Power-On-Authentication prior to permitting the device to boot and also is configured to encrypt transmissions using Advanced Encryption Standard. The Agency's policy required that all laptops contain this software prior to issuing for use. As a result, this portion of the recommendation has been implemented.

b) We confirmed that the Agency has relocated network jacks in public spaces (conference and training rooms) onto a "guest" network that has Internet access, but no access to internal systems or networks. The Agency continues to evaluate automated technology solutions that would allow the Agency to shift unauthorized and non-compliant (e.g., out of date antivirus signatures) computers to a remediation network regardless of which network jack the device is connected; however, the "guest" network is adequate to control unauthorized devices from connecting to the Agency network. As a result, this portion of the recommendation has been implemented.

c) The Agency determined that cable locks are not required since encryption is viewed as the Agency's primary control to protect the data on laptops. As noted in a) above, we confirmed that laptops are protected by full disk encryption, thus reducing the risk of unauthorized access to data if a laptop is stolen. The Agency has accepted the risks associated with the flexibility of using the portable devices. As a result, this portion of the recommendation has been implemented.

d) The Agency now requires Blackberry passwords to have a minimum of eight characters, and at least one character must be a number. In addition, the password is required to be changed every 90 days. We confirmed the password composition rule settings during our testing. As a result, this portion of the recommendation has been implemented.

e) The PII Incident Response and Notification Plan is being revised and has not been finalized and approved. 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.

October 2009 Status: **Partially Implemented.**

The security program requirements are currently being updated through a primary directive to outline the security requirements, roles and responsibilities. This directive will be supplemented by individual policies and procedures that will align to the NIST SP 800-53 control categories[6]. The directive and procedures are currently being drafted and are scheduled for completion in January 2010.

---

[6] Control categories include Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Certification, Accreditation, Security Assessments (CA), Configuration Management (CM), Contingency Plan (CP), Identification and Authentication (IA), Media Protection (MP), Physical and Environmental Protection (PE), Planning (PL), Personnel Security (PS), Risk Assessment (RA), and Systems and Services Acquisition (SA).

The media management and incident response policies are being updated as part of the overall security program updates using the NIST SP 800-53 control categories. The documentation is also scheduled for completion in January 2010.

Disposition: **Recommendation Open.**

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

Original Recommendation: To strengthen the controls over the TSP 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.

October 2009 Status: **Partially Implemented.**

a) For networks, and devices connected to the network, the Agency plans to create standard images and configuration standards for Windows, Cisco routers, switches and firewalls during the modernization project which is currently underway. According to the Agency, most of the

network devices, with the exception of the virtual private network (VPN) gateways, have been configured according to Center for Internet Security (CIS) and National Security Agency (NSA) benchmarks for Cisco Internetwork Operating System (IOS) and firewalls. However, current procedures for monitoring and logging of activities are in draft form and will reflect NIST SP 800-53 controls. The documentation is scheduled for completion in January 2010. As a result, this portion of the recommendation remains open.

b) The Agency is currently utilizing "CA Clean-up"[7] to generate reports of Usage and Non-Usage of Accessor ID (ACID) accounts. The reports have provided management with the ability to determine which ACID accounts need access to resources by observing the action performed by the ACID accounts. The review process is currently ad-hoc as the formal procedures are still in draft. As a result, this portion of the recommendation remains open.

c) During our test procedures, we selected thirty-two (32) individuals and reviewed documentation to verify whether their background investigations were completed and non-disclosure agreements were signed. We did not identify any exceptions with background investigation results and non-disclosure agreements. As a result, this portion of the recommendation has been implemented.

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

[7] Computer Associates (CA) Clean-up is a tool that provides automatic ongoing and comprehensive cleanup of security files. CA Clean-up identifies and removes privileges/entitlements and user IDs once un-referenced/used beyond a specified threshold (*Source: www.ca.com*).

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. 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.

October 2009 Status: **Partially Implemented.**

a) The logical access policy and procedures related to approving, disabling, and recertifying accounts are in the process of being drafted.

With regards to the mainframe, we selected fifteen (15) individuals to verify the approval of their access. Our 2009 test procedures reflect that the accounts reviewed during the audit were authorized and approved consistent with their associative access. As such, logical

access authorization has been addressed for the mainframe.

With regards to other TSP system components, we noted the following during our 2009 testing:

- For 14 of the 20 users selected with access to three TSP-related local area networks (LAN), documentation was not available or not provided to support access authorization.
- For 16 of 24 users selected with remote access to two TSP-related LANs, documentation was not available or not provided to support access authorization.
- For 1 of the 10 users selected with access to PowerImage and its supporting database, documentation was not available or not provided to support access authorization.
- For all 10 users selected with access to the OMNI Station, documentation was not available or not provided to support access authorization.
- 1 of 38 separated employees selected still had an active account on the PowerImage application and its supporting database.

As a result, this portion of the recommendation remains open.

b) The Agency is currently utilizing "CA Clean-up" to generate reports of Usage and Non-Usage of ACID accounts. The reports have provided management with the ability to determine which ACID accounts need access to resources by observing the action performed by the ACID accounts. The review process is currently ad-hoc as the formal procedures are still in draft. As a result, this portion of the recommendation remains open.

c) The Agency is drafting and policy and procedures to align to the NIST SP 800-53 control category for Identification & Authentication (IA). The documentation is scheduled for completion in January 2010. The Security Administration group is reviewing toolsets to monitor all accounts, particularly over the mainframe. The approving, disabling, and recertifying of accounts are procedures that are being documented and implemented. As a result, this portion of the recommendation remains open.

d) With regards to the database administrator and domain accounts, this issue has not been addressed. As a result, 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.

October 2009 Status: **Partially Implemented.**

a) For networks and devices connected to the network, the Agency plans to create standard images and configuration standards for Windows, Cisco routers, switches and firewalls during the modernization project which is currently underway. According to the Agency, most of the network devices, with the exception of the VPN gateways, have been

configured according to CIS and NSA benchmarks for Cisco IOS and firewalls. However, current procedures for establishing settings for TSP system components are in draft form and will reflect NIST SP 800-53 controls. The documentation is scheduled for completion in January 2010. As a result, this portion of the recommendation remains open.

b) During our 2009 test procedures, we evaluated the mainframe configuration settings that provide access to sensitive functions and data sets and confirmed that management has modified system security settings to be more restrictive. Additionally, the Agency communicated that it has established a mainframe configuration baseline with the migration of the z/OS from version 1.7 to 1.9 in September 2009. However, at the time of this report, we did not receive documentation to substantiate this activity. As a result, 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 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 systems 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 have 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.

October 2009 Status:

Partially Implemented.

a) The Agency is in the process of updating security policies and procedures that will establish the risk management and security planning needs for the TSP systems that will align to the NIST SP 800-53 control categories. This will also require the TSP system to undergo a new risk assessment the correlates to the NIST and Federal Information Processing Standards (FIPS) identified in the policies. The documentation is scheduled for completion in January 2010. As a result, this portion of the recommendation remains open.

b) The Agency has communicated that it understands the importance of

the PIA as an integral part of the Agency's overall risk assessment process. However, a formal PIA has not been performed. As a result, this portion of the recommendation remains open.

c) The Agency has communicated that it is not subject to the requirement to designate a Chief Privacy Officer. The Office of General Counsel has taken over the responsibility for training and compliance with the Privacy Act. Protecting sensitive personally identifiable information (PII) in the TSP systems is the ongoing responsibility of the Information Security Program Manager. Formally documenting the roles and responsibilities of protecting PII is part of the Information Security Program Manager's current responsibilities. The documentation is scheduled for completion in January 2010. As a result, this portion of the recommendation remains open.

d) Protecting sensitive PII information in the TSP systems is an ongoing responsibility of our Information Security Program Manager. The Agency is in the process of updates security policies and procedures for incident handling to include handling incidents related to the breach of information such as PII. These procedures will align to the NIST SP 800-53 control categories. The documentation is scheduled for completion in January 2010. As such, this portion of the recommendation remains open.

e) The Agency has started tracking POA&Ms for the Virginia data center and the Maryland call center. The POA&Ms being used currently are more site-specific but will be moving to system-specific in the future. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

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

Original To strengthen the controls over participant identity management, we

Recommendation: 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 the 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.

October 2009 Status: **Partially Implemented.**

The Agency acquired RSA's[8] adaptive authentication to monitor risky behavior on the web site and will implement it with the current TSP Web redesign effort, which is scheduled for completion on September 30, 2010. The Agency has decided to use this technology and not perform an E-Authentication risk assessment until the corresponding risk management and security planning policy and procedures are finalized, which are scheduled for completion in January 2010. The account credentials in question are protected through access rules; however, the Agency continues to evaluate technologies in encryption at rest software for all TSP data.

Disposition: **Recommendation Open.**

[8] RSA is a provider of security solutions.

KEY PERSONNEL INTERVIEWED

A. Serco, Inc.

Lori Hogan-Waterman	Security Administrator
Glenn Meyers	Data Center Operations Manager

B. Federal Retirement Thrift Investment Board - Agency Staff

Mark Hagerty	Chief Information Officer (CIO)
Roy Friend	Deputy CIO, Infrastructure and Operations
Troy Poppe	Information Security Program Manager
Mark Allen	IT Specialist and Board Continuity of Operations Planning (COOP) Coordinator

KEY DOCUMENTATION REVIEWED

Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, Employee Benefits Security Administration, October 7, 2005

Review of the Thrift Savings Plan Disaster Recovery and Continuity of Operations, Employee Benefits Security Administration, March 3, 2006

Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, Employee Benefits Security Administration, March 30, 2007

Performance Audit of the Computer Access and Technical Security Controls over the Thrift Savings Plan System, Employee Benefits Security Administration, April 16, 2008

Security policy and procedure documentation

- Thrift Savings Plan (TSP) system security plan (May 2007)
- Draft TSP data security policy (May 2007)
- FRTIB background investigation review (selection range from October 1, 2008 to March 31, 2009)
- FRTIB non-disclosure agreement example (selection range from October 1, 2008 to March 31, 2009)

Logical access control documentation

- Draft security applications' access granting procedures (March 30, 2009)
- Random selection of mainframe ACID accounts (July 25, 2008 through May 6, 2009)
- ACID account email authorizations (July 25, 2008 through May 6, 2009)
- Selection of termination ACIDs
- Selected terminated ACIDs modification date
- Mainframe removal access review emails (October 23, 2008 through June 3, 2009)
- Mainframe access review samples (October 23, 2008 through June 3, 2009)
- Sample of security violation reports (selection range from April 2008 to February 2009)
- Sample of follow-up actions per violations (selection range from April 2008 to February 2009)
- Sample of Top Secret Security (TSS) critical datasets (June 12, 2009)
- Sample of who has access to critical datasets (June 12, 2009)
- List of users connected to selected profiles on the mainframe (June 12, 2009)
- List of ACIDs with associated user name (June 12, 2009)
- Modify Status Report (June 10, 2009)
- List of users with system admin privileges (June 10, 2009)

KEY DOCUMENTATION REVIEWED, CONTINUED

- List of users with Bypass Privilege access to critical data sets (June 10, 2009)
- List of users connected to the JASI profile (June 10, 2009)

APPENDIX C

ENTRANCE AND EXIT CONFERENCE ATTENDEES

An overall entrance conference, covering the entire FY 2009 Thrift Savings Plan audit plan and proposed schedule, was held at the Agency on November 19, 2008. Attendees were as follows:

A. Federal Retirement Thrift Investment Board - Agency Staff

Mark Hagerty	Chief Information Officer (CIO)
James Petrick	Chief Financial Officer
Anne Beemer	Controller, Office of Finance
Roy Friend	Deputy CIO, Infrastructure and Operations
Susan Smith	Deputy CIO, Software and Applications Management
Penny Moran	Director, Office of Participant Services
Bonnie Parazinksi	Call Center Manager
Troy Poppe	Information Security Program Manager

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance

C. KPMG LLP

Heather Flanagan	Partner
Don Farineau	Partner
Derek Thomas	Manager
Mark Munster	Computer Systems Analyst
Alexander Sultan	Computer Systems Analyst

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

An entrance conference covering the scope and objectives of the Computer Access performance audit was held at Agency headquarters in Washington, DC on March 19, 2009. Attendees were as follows:

A. Federal Retirement Thrift Investment Board – Agency Staff

Mark Hagerty	Chief Information Officer (CIO)
James Petrick	Chief Financial Officer
Roy Friend	Deputy CIO, Infrastructure and Operations
Troy Poppe	Information Security Program Manager
Anne Beemer	Controller, Office of Finance

B. KPMG LLP

Mark Munster	Computer Systems Analyst
David Strich	Computer Systems Analyst
Evans Bannor	Computer Systems Analyst

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

An exit conference was held on November 30, 2009 at Agency headquarters in Washington, DC. Attendees were as follows:

A. Federal Retirement Thrift Investment Board – Agency Staff

Jim Petrick	Chief Financial Officer
Mark Hagerty	Chief Information Officer (CIO)
Anne Beemer	Controller, Office of Finance
Roy Friend	Deputy CIO, Infrastructure and Operations
Troy Poppe	Information Security Program Manager

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance

C. KPMG LLP

Mark Munster	Computer Systems Analyst

APPENDIX D

AGENCY'S COMMENTS TO FINAL REPORT