



# **Employee Benefits Security Administration**

## **Performance Audit of the Thrift Savings Plan Participant Support Process**

**As of November 19, 2012**

## TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
<b>EXECUTIVE SUMMARY</b>	i
<b>I. BACKGROUND OF THE TSP AND THE PARTICIPANT SUPPORT PROCESS</b>	
A. The Thrift Savings Plan	I.1
B. Overview of the TSP Participant Support Process	I.1
C. Description of the TSP Call Centers	I.5
<b>II. OBJECTIVE, SCOPE AND METHODOLOGY</b>	
A. Objective	II.1
B. Scope and Methodology	II.1
<b>III. FINDINGS AND RECOMMENDATIONS</b>	
A. Introduction	III.1
B. Findings and Recommendations from Prior Reports	III.2
C. 2012 Findings and Recommendations	III.12
<u>Appendices</u>	
A. Agency's Response to the Final Report	
B. Key Documentation and Reports Reviewed	

## EXECUTIVE SUMMARY

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

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

As a part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit of the Federal Retirement Thrift Investment Board's Staff's (Agency) Thrift Savings Plan (TSP) participant support process. Our fieldwork was performed from March 26, 2012 through November 19, 2012, primarily at the Agency's headquarters in Washington, D.C., and the two TSP call centers located in Virginia and Maryland. Our scope period for testing was January 1, 2011 through December 31, 2011.

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

The objectives of our audit over the TSP participant support process were to:

- Determine if the Agency implemented certain procedures to: 1) provide timely and accurate information to participants concerning the TSP, including their statement of account activity; 2) prepare quarterly statements for participants that reflected the activity for the period; 3) prepare annual statements for participants that summarized all transactions made during the previous calendar year by transaction type; 4) respond to participants' and Congressional inquiries in an accurate and timely manner; 5) process confirmation and reject notices

accurately, and distribute them in a timely manner; and 6) monitor the call centers' contractors to ensure they were in compliance with the terms of the contract;

- Test compliance of the TSP participant support process with 5 USC 8439c (hereinafter referred to as FERSA), and 5 CFR 1640, 5 CFR 1630.7b, and 5 CFR 1630.7c (hereinafter referred to as Agency Regulations); and
- Determine the status of all prior EBSA TSP participant support open recommendations reported in *Performance Audit of the Thrift Savings Plan Participant Support Process as of August 14, 2009*.

Our audit resulted in eight new findings and recommendations related to the TSP participant support process, all addressing fundamental controls. Fundamental control recommendations address significant procedures or processes that have been designed to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Section III.C presents the details that support the current year findings and recommendations.

Based upon the performance audit procedures performed and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2011 through December 31, 2011 the Agency implemented certain procedures to (1) provide timely and accurate information to participants concerning the TSP, including their statement of account activity; (2) prepare quarterly statements for participants that reflected the activity for the period; (3) prepare annual statements for participants that summarized all transactions made during the previous calendar year by transaction type; (4) respond to participants' and Congressional inquiries in an accurate and timely manner; (5) process confirmation and reject notices accurately, and distribute them in a timely manner; and (6) monitor the call centers' contractors to ensure they were in compliance with the terms of the contract. However, we noted internal control weaknesses in certain areas that could adversely affect the TSP participant support process. As a result of our compliance testing, we did not identify any instances of noncompliance with FERSA or Agency Regulations in the TSP participant support process.

We also reviewed nine prior EBSA recommendations related to the TSP participant support process to determine their current status. These prior year recommendations were reported in *Performance Audit of the Thrift Savings Plan Participant Support Process as of August 14, 2009*. Section III.B documents the status of these prior recommendations. In summary, one of the

recommendations has been closed, four recommendations have been partially implemented and remain open, and four recommendations have not been implemented and remain open.

The Agency's responses to the recommendations, including the Executive Director's formal reply, are included as an appendix within the report (Appendix A). The Agency concurred with all recommendations.

This performance audit did not constitute an audit of the TSP's financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not render an opinion on the Agency's internal controls over financial reporting or over financial management systems (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

March 14, 2013

## **I. BACKGROUND OF THE TSP AND THE PARTICIPANT SUPPORT PROCESS**

### **A. The Thrift Savings Plan**

Public Law 99-335, the Federal Employees' Retirement System Act of 1986 (FERSA), as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS) and provides a Federal (and, in certain cases, state) income tax deferral on employee contributions and related earnings. The TSP is available to Federal and Postal employees, members of Congress and certain Congressional employees, and members of the uniformed services. For FERS participants, the TSP also provides agency automatic 1 percent and matching contributions. The TSP began accepting contributions on April 1, 1987, and as of September 30, 2012, had approximately \$326 billion in assets and approximately 4.6 million participants<sup>1</sup>.

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

### **B. Overview of the TSP Participant Support Process**

Participant support involves providing TSP participants and beneficiaries with information about their TSP accounts and plan benefits. This process includes distributing participant statements and other communications materials as well as answering participant inquiries.

#### **1. Participant Inquiries<sup>2</sup>**

Generally, Federal employees and uniformed services members are initiated to the TSP through contact from their employers' personnel offices. Federal agency and uniformed service personnel offices are the primary TSP contact point for actively employed TSP participants. Inquiries that the Federal agency and uniformed service personnel or payroll office cannot answer and inquiries from separated participants or beneficiaries are directed primarily to one of the two TSP call centers. With respect to active participants, either personnel or payroll offices

---

<sup>1</sup> Source: Minutes of the October 22, 2012 Federal Retirement Thrift Investment Board meeting, posted on [www.frtib.gov](http://www.frtib.gov).

<sup>2</sup> Source: Call Center Correspondence Procedures and Serco Standard Operating Procedures.

can contact the call centers or the Agency on behalf of the participants or the participants can contact the TSP call centers directly, depending on the issue. Both the Agency and the call centers have direct contact with participants and beneficiaries by mail and by telephone. The Agency works with the call centers to coordinate information needed to answer participants' inquiries.

The TSP correspondence unit at the Virginia call center is responsible for responding to written inquiries received from participants, beneficiaries, and third parties (e.g., financial institutions, attorneys, and other Federal agencies). While some inquiries (e.g., those involving contribution issues) from active participants are referred to their employing agencies or services for assistance, many others (e.g., questions about interfund transfers, contribution allocations, loans, or in-service withdrawals) are handled by the call center since the employing agencies and services have little or no involvement in these program areas. In cases of third party inquiries, information is released consistent with the Privacy Act requirements as provided by the Agency.

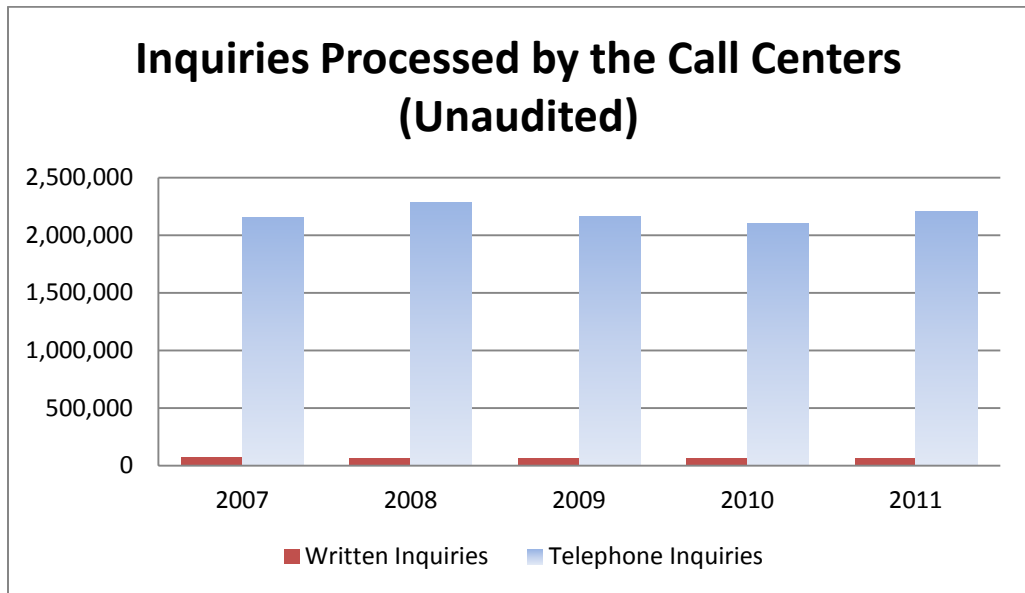
Once the assigned correspondence agent begins work on the correspondence, he or she is responsible for resolving the inquiry and responding to the participant, either via a phone call or letter. The correspondence agent first reviews the correspondence for completeness. Participants who do not adequately complete their inquiry requests are sent form letters requesting more information. However, if an inquiry is only missing the participant's account number (or Social Security Number), the correspondence agent performs a search through the Participant Service Representative (PSR) application using the participant's name. The correspondence agent then researches the inquiry and returns an appropriate response to the participant. Third party inquiries are completed under different rules, depending upon the nature of the request, but the process is generally the same.

Congressional inquiries are those inquiries made by members of Congress, or their staff, usually on behalf of a constituent. The Agency handles all Congressional inquiries. The Agency logs these inquiries into an internal tracking system. Although most of the correspondence is referred to the Office of External Affairs for response, the Office of Participant Services may assist with research and resolving issues or drafting the letters, as needed.

During calendar year 2011, the TSP call centers processed approximately 2.2 million TSP participant telephone and approximately 65,000 written inquiries<sup>3</sup>. The TSP most frequently processes inquiries regarding withdrawal information. During calendar year 2011, inquiries related to this area accounted for 40 percent of all inquiries processed by the TSP<sup>4</sup>.

Exhibit I-1<sup>3</sup> illustrates the number of written and telephone inquiries processed by the TSP call centers during calendar years 2007 through 2011. Exhibit I-2<sup>4</sup> divides the total telephone inquiries processed by the TSP during calendar year 2011 into type of transaction.

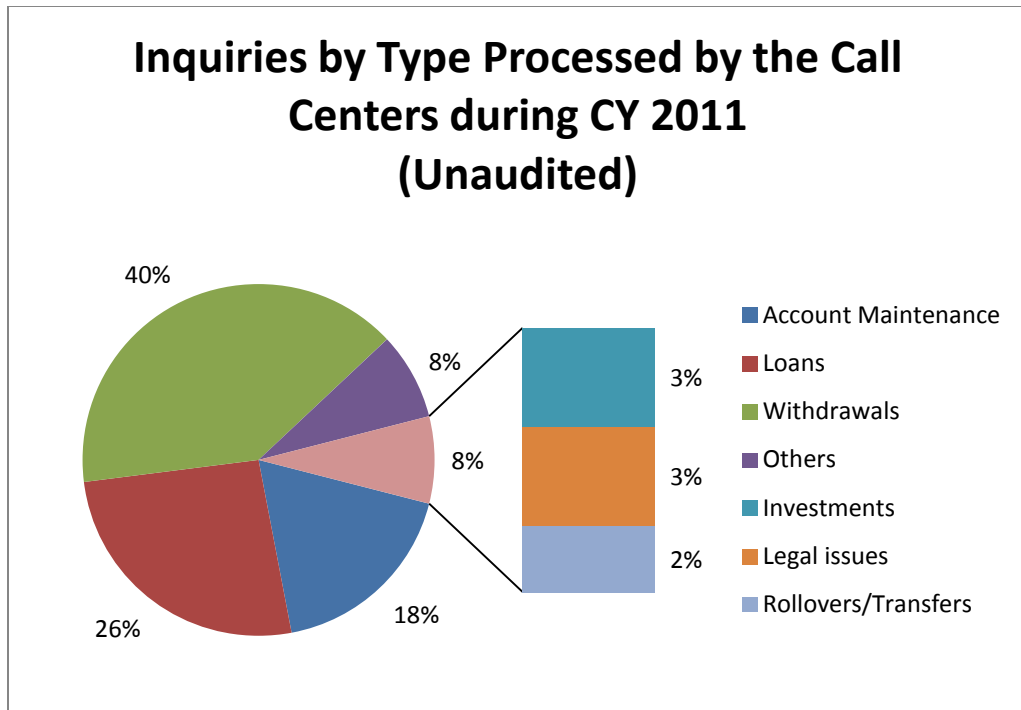
*Exhibit I-1*



<sup>3</sup> Source: Thrift Savings Plan Civilian and Uniformed Services Inquiries for Clintwood, Spherix (Report No. TSP 6011)

<sup>4</sup> Source: Thrift Savings Plan Phone Inquiry Report





**2. Participant Statements<sup>5</sup>**

The TSP issues quarterly statements to participants each year in January, April, July, and October. The quarterly statements cover all transactions in a participant’s accounts that occurred during the previous three months. The statements also summarize the loan activity for those TSP participants with loans. Quarterly statements are available to participants online via the TSP website unless the participant specifically requests that a paper statement be mailed.

The TSP also issues annual statements each year in February. The annual statement summarizes the financial activity in the participant’s account for the previous calendar year and provides other important information such as a participant’s personal investment performance and the participant’s primary beneficiary information. The annual statements are available online via the TSP website and are also mailed to the participants unless they request to only receive their annual statements electronically.

<sup>5</sup> Source: Summary of the Thrift Savings Plan

## **C. Description of the TSP Call Centers<sup>6</sup>**

### **1. Overview of the Call Center Operations**

Participants with questions concerning their TSP accounts (e.g., account status, loan request status, interfund transfers, and contribution allocation changes) access the automated ThriftLine, access the TSP web site, or mail correspondence to the TSP. By dialing the ThriftLine's toll-free number, a participant can opt to talk to a call center PSR. The call is routed to one of the two call centers, based on an Agency pre-determined call-volume load setting, through its telecommunications provider. The Agency (and for emergency/business continuity purposes, each call center) has the ability to change the percent of program traffic for toll-free incoming calls for each call center via a web browser. For this purpose, the telecommunications provider supplies a dedicated web site that is only accessible through a unique user ID and password. While the inbound call volumes generally are divided between the two call centers, the Maryland call center exclusively handles the Telecommunications Device for the Deaf (TDD) calls since the service has a unique telephone number.

The two competitively-selected call centers are staffed by a call center manager, deputy call center manager, supervisors, team leads, helpdesk personnel, quality assurance (QA) coordinators, trainers, PSRs, and administrative and information technology (IT) support personnel. The contractor for each call center determines its own staffing complement based on forecasted call volumes, management requirements, and work to be performed. Depending upon the call center, IT support personnel may be fully dedicated to the TSP project or shared with other contracts. The Virginia call center is a Government owned/Contractor operated (GOCO) facility while the Maryland facility is a Contractor owned/Contractor operated (COCO) facility. As a result, some operational differences exist. However, wherever possible, both centers operate the same, using the same performance metrics and requirements, call center technology, knowledge database, and materials. The goal of the Agency is to achieve transparency for participants so that they receive a consistent experience regardless of which call center they reach.

The PSR's primary task is to answer inbound inquiries from the TSP participants. Before a PSR can take live phone calls, he or she must successfully complete a training course consisting of

---

<sup>6</sup> Sources: TSP Telephone Service Quality Assurance Program, TSP Call Center Standard Operation Procedures, and Serco Standard Operating Procedures.

TSP program specific information, use of the TSP applications (e.g., PSR and EXP AG<sup>7</sup>), and additional customer service skills training. Team leads and helpdesk personnel are primarily responsible for performing research requests for issues that cannot be resolved on first contact and handling escalations. They also answer initial inbound inquiries as needed. The primary responsibility of supervisors is to oversee floor operations, which includes managing performance metrics (i.e., service level is being achieved) that are reported via the Symposium Automated Call Distribution (ACD) software and directing the PSRs. In addition, supervisors monitor live and recorded phone calls, document personnel actions and coaching sessions, take escalated calls, supervise research and fulfillment functions, and schedule work shifts. Supervisors are supplemented with team leads who can assist them in carrying out their responsibilities. The deputy call center manager serves as a backup to the call center manager and is responsible for floor operations, management of the QA function (e.g., the monitoring of phone calls, follow-up coaching, and performance appraisals), management of the research and fulfillment functions, and reporting of technical issues. The call center manager is responsible for the overall contract performance. Processes are in place for the call center manager to evaluate operations performance as it pertains to the achievement of contract performance standards.

a. Technology Infrastructure

The call centers each house the application servers for workforce forecasting, call volume and performance monitoring, and call recording and archiving software. In addition, each center has two Voice Response Unit (VRU) servers which handle inbound calls with a maximum call handling capacity of 164 concurrent calls as of April 2012. One server is active at any time with the other VRU serving as a backup. Physical access to the data centers is controlled through the use of electronic badges.

As toll-free calls arrive at the telecommunications provider network, the call is presented to a Nortel Meridian 1 private branch exchange (PBX), and the participant is offered to the ThriftLine VRU. Participants have the option to stay within the ThriftLine or opt out to speak with a PSR. If the participants stay within the ThriftLine, they may conduct their business through automated functions. If the participants choose to speak with a PSR, several processes occur using the VRU, Computer Telephony Integration (CTI) software, and Nortel Symposium software to transfer the call to the PSR:

---

<sup>7</sup> EXP AG is the Agency's document imaging system that replaced PowerImage in 2011.

- The VRU uses information provided by the participant to access OMNIPlus<sup>8</sup>. When the participant information is retrieved from the VRU request after the participant enters his account number, the information is queued in the CTI software.
- The CTI software queues the record for the PopPSR software to provide the PSR with a “screen-pop” of the participant’s account information.
- After this information is retrieved, the Nortel Symposium system routes the call to the next available PSR.

Participant calls are recorded by the Versadial server. All calls to the Virginia call center are recorded and stored on removable hard drives and taken offsite to a safety deposit box at a nearby financial institution. The Maryland calls are recorded to CD/DVDs and are kept onsite.

#### b. Human Resources

Each call center employs its company’s global processes for hiring, recruiting, and performance evaluation. These human resource processes are not specific to the TSP account; they apply to all company employees consistent with their contracts. Generally, the call centers fill PSR positions for the TSP’s call center functions using both outside applicants and current employees who may be working on other contracts, as appropriate. The Virginia call center uses a local government employment office as well. Applicants complete an application and receive an aptitude test, and are either interviewed by supervisors or human resource personnel, or a team of interviewers consisting of members of staff/supervisor and/or human resource personnel. Interview sessions focus on identifying the candidate’s suitability for the position. An emphasis is placed on proficiency with computers, handling difficult customers, work history, additional skills or experience (e.g., previous positions in the financial sector), and start date availability, to determine if the candidate is qualified for the position. Once a candidate is considered for employment, a background investigation is required for that individual to work on the TSP contract. In addition, all new hires must sign the Agency’s nondisclosure/confidentiality agreement.

Job descriptions contain minimum experience requirements and/or special skills. A PSR must have prior call center experience or complex customer service experience and must have earned a high-school degree or equivalent diploma. Experience requirements become progressively

---

<sup>8</sup> OMNIPlus is the core record keeping engine for the TSP system.

more rigorous for helpdesk, team lead, supervisory, operations, and management positions. All new hires receive an employee handbook containing the company's human resource policies and procedures.

All new PSRs are subject to a 90-day probation period after they are hired. The 90-day probationary review focuses on three areas: performance (i.e., quantity and quality of work); adaptability (i.e., to the work environment and co-workers); and dependability (i.e., arrives to work on time and no excessive leave). This standard set of probationary evaluation criteria is used by both call centers. If deficiencies are identified during the probationary period review, additional coaching is provided to the PSR in an effort to improve his or her performance.

At the completion of the probationary period, the PSR's supervisor and the call center manager review his or her performance and determine whether to continue employment, extend the probationary period, or terminate employment.

## **2. Customer Service Delivery**

The TSP's call centers' service delivery and customer service capabilities and performance can be separated into the following areas: a) Customer Feedback; b) Service Delivery Procedures; c) Performance Standards; d) Training and Personnel Programs; and e) Technology Support.

### **a. Customer Feedback**

The Agency has a Customer Satisfaction survey process and a QA program to collect and analyze customer feedback through the call centers to assess customer satisfaction levels with the TSP. Both programs were initially developed with the assistance of the International Customer Management Institute (ICMI) consulting group and are maintained with the assistance of a vendor.

The QA program consists of quality monitoring sessions performed by QA coordinators. QA coordinators randomly select a pre-determined number of recorded calls to listen to so they can review each PSR's activity each month (e.g., 3 to 5 per month for new hires and 2 per month for experienced PSRs). The Envision quality monitoring software, Click2Coach, records the audio and screen shot activity of the call. Every third call is recorded daily for each PSR. The QA coordinator selects and evaluates calls using his or her experience with the program and customer service training, and scores attributes of the call under the categories of foundation

skills (i.e., opening/greeting, data quality, professional etiquette, and the conclusion) and finesse skills (i.e., call management/listening, program knowledge, and communication skills/customer responsiveness).

Calls are scored using a rating scale of 0 = unsatisfactory; 1 = needs improvement; 2 = satisfactory; 3 = outstanding; and N/A = not applicable for this call. In addition, QA coordinators and supervisors conduct periodic calibration sessions where all personnel who perform quality monitoring duties will listen to and score a call, compare the results, and discuss the differences in monitoring approach. Monthly, a joint calibration session is conducted with Agency staff and personnel from both call centers. The calibration sessions are intended to create a common baseline for evaluating and scoring the calls regardless of the individual who performs the monitoring. Once the calls have been monitored and scored, the evaluation form is given to the PSR's supervisor for follow-up coaching.

The designated manager, QA staff member, or supervisor also conducts an outbound telephone customer satisfaction survey for a selection of the calls monitored. Surveys are only conducted on those calls that have been monitored for QA purposes. The results of the monitored call are compared to the results of the survey performed for the same call. Surveys are to be initiated within 72 hours of the participant's contact with the call center. If the participant cannot be reached within three days of the initial contact, then the call will not be included in the survey.

Semi-annually, the Agency prepares a Customer Satisfaction Report, which provides information regarding both the customer satisfaction surveys and the QA scores as well as any correlation between participant scores and the corresponding foundation and finesse attribute scores. The Agency uses the report to track the level of satisfaction with the call center services and to identify areas of opportunity for improvement in the two programs.

#### b. Service Delivery Procedures

Service delivery processes include managing call center goals and participant expectations and providing proactive communication. A call center's goals are typically created to support the mission and objectives of the sponsor organization. Staffing, scheduling, and performance monitoring are all focused on the call center's ability to appropriately achieve the contractual performance standards.

The call centers track and monitor metrics that influence participant perceptions, such as service level, hold time, and first contact resolution percentage. The call centers' PSRs attempt to resolve participant inquiries on the first call. If a call is not resolved on first contact, or if a participant requests escalation, a research request form is completed, a PSR call note is added to the system, and the information is provided to a research analyst (i.e., an experienced PSR). Research analysts attempt to resolve issues within 72 hours of receipt, and then the participants are called back with an update. A PSR call note is added for each interaction with the participant.

The TSP call handling procedures are designed to address all potential scenarios that may occur. Examples of these procedures include logging issues in a consistent manner for accuracy and completeness; escalating issues through the proper channels when a participant requests escalation or when a difficult inquiry cannot be resolved; properly placing the participant on hold or transferring the call; setting the expectations for service delivery from the beginning of the call through the call's completion; handling TDD calls (as appropriate); finding resolutions from a knowledge management tool; and demonstrating proper phone etiquette skills.

The TSP call handling procedures are communicated through formal training and coaching. Prior to the PSR handling live calls, PSRs conduct "link-up" sessions with an experienced PSR listening in on the call and sitting next to the PSRs or observing the call within a controlled environment. This technique is used to prepare the new PSRs to take live calls on their own. Call handling procedures are also available to PSRs in hard copy from their training courses, which can be kept in a station binder (i.e., a compilation of training materials that the PSR uses as reference material).

#### c. Performance Standards

The performance standards are contractual requirements of the TSP call centers. The standards used to measure the call centers' effectiveness include the abandonment rate, adherence, average handle time, blocked calls, occupancy, and the telephone service factor (TSF).

The Agency monitors multiple reports throughout the year to discern the call centers' achievement of performance. In the event of an anomaly in performance, the Agency call center program manager and the call center manager(s) discuss the issue and determine the cause of the problem and a resolution. The Agency reviews the following reports, with the corresponding frequency:

### Daily

- Average daily volumes

### Weekly

- Week to Date ThriftLine and PSR calls comparison of call centers

### Monthly

- Monthly totals and comparisons of ThriftLine and PSR calls
- Monthly performance summary of selected performance standards for each call center
- Monthly summary of ThriftLine and PSR calls
- Staffing monthly report for each call center
- Research request report

### Annually

- Performance standards call center comparison from January to December

Each call center's management also monitors their performance standards. Supervisors and operations staff perform real-time monitoring of performance standards via the Symposium software display. Any disparity from the standards may lead supervisors and operations staff to review the staff schedule and call volume spikes, and may lead to a discussion with the Agency call center program manager concerning potential issues that have impacted performance (e.g., excessive sick leave, weather conditions, and queuing). The Agency call center program manager may consider changing call volume loads at the telecommunications provider switch level in an effort to improve the performance. Additionally, the centers may consider changing workforce variables through the workforce scheduling and forecasting software.

The Agency performs a bi-annual analysis, with the assistance of ServiceAgility, to evaluate the customer satisfaction survey results across both call centers. Additional correlations are made between the satisfaction survey responses and the quality monitor forms used to evaluate the corresponding calls. This information is used to refine the survey questions or administration, and also to refine the methods by which calls are being monitored.

#### d. Training and Professional Development Programs

In addition to orientation sessions provided to all company employees, all PSRs are subject to a 4-6 week comprehensive training program prior to taking live phone calls. The course consists



of TSP program specific course work related to the following areas: eligibility and contributions, investments, spousal rights, loans, in-service withdrawals, post-service withdrawals, annuities, transfers/rollovers, court orders, death benefits, beneficiaries, and account access; supplemental training, including customer service standards and techniques and application training; “link up” sessions; and sessions using the TSP Web site, PSR and EXP AG software. A final exam is administered which focuses on all program-specific areas and the TSP system. In order to pass the exam, PSRs must obtain a score of 90% or better.

Ongoing training programs exist at both centers. In addition to refresher training and ad hoc sessions throughout the year, the Agency also provides annual Privacy Act training and sessions on topics of relevance (e.g., investments and required minimum distributions). The other operational units (Legal Processing Unit, Death Benefits Processing Unit, and Mail Management/Data Entry) also provide training for the PSRs in their specialty areas. Annual security training is provided via Agency-sponsored Computer Based Training sessions.

In addition, as reported earlier, QA monitoring and coaching provide PSRs with information on their performance related to program requirements, proper phone etiquette, and call handling techniques.

#### e. Technology Support

The PSR’s ability to serve participants is directly related to the performance of the information system. Performance is defined in terms of a system that provides PSRs with accurate and timely information that is readily available.

The core applications used by the PSRs include the PSR application, EXP AG, and the Talisma KnowledgeBase. The PSR application is the customer account history and inquiry logging software used to provide participants with information related to their accounts (e.g., account balance, loan, contribution, and withdrawal information). The EXP AG application is used by PSRs for functions including identification of work-in-process loan and withdrawal requests, research, and transmittal of fax-back materials to participants at their request. The Talisma KnowledgeBase, which is used by the Agency and both call centers, provides the ability to keyword search a database of common inquiries and resolutions. In addition, the tool contains a bulletin board feature that contains links to common questions and answers or upcoming events and program changes. Maintenance of the knowledge database is a collaborative effort by the Agency and the call centers.

The core applications used by supervisors include the Symposium workbench, Verint, and Click2Coach. The Symposium software is used to monitor the achievement of performance standards in real-time and provide historical reporting. The Symposium real-time display provides service level achievement as it occurs, providing the supervisor with information such as calls on hold, calls abandoned, and TSF (i.e., the percentage of calls answered with a given time period (e.g., 90% within 20 seconds)).

The Verint software is used to forecast workforce requirements corresponding to pre-established service levels. It also provides the schedule required to fulfill the work forecast in order to meet the demand of the service level variables. Each week, a dedicated workforce manager creates a work schedule based on the following service levels:

**Service level** = 90% of calls answered in 20 seconds

**Maximum abandons** = 2%

**Average Talk Time** = 210 - 270 seconds/call

**Average wrap-up time** = 60 - 120 seconds/call

The software uses these figures to create a weekly work schedule for the designated hours of operation, the number of seats (i.e., PSRs) needed to achieve the service level goals, and the times scheduled for on the phone activity, breaks, and lunches. Any changes to the schedule must be communicated to the workforce manager to recast the schedule.

Call center supervisors and team leads use the Click2Coach software for the quality monitoring process as described in the Customer Feedback section above. A sample of calls and screenshots is recorded and temporarily stored on disk on the Click2Coach server, and is used to provide performance feedback to PSRs.

## **II. OBJECTIVE, SCOPE AND METHODOLOGY**

### **A. Objective**

The U.S. Department of Labor (DOL) Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit of the Federal Retirement Thrift Investment Board's Staff's (Agency) Thrift Savings Plan (TSP) participant support process.

The objectives of our audit over the TSP participant support process were to:

- Determine if the Agency implemented certain procedures to: 1) provide timely and accurate information to participants concerning the TSP, including their statement of account activity; 2) prepare quarterly statements for participants that reflected the activity for the period; 3) prepare annual statements for participants that summarized all transactions made during the previous calendar year by transaction type; 4) respond to participants' and Congressional inquiries in an accurate and timely manner; 5) process confirmation and reject notices accurately, and distribute them in a timely manner; and 6) monitor the call centers' contractors to ensure they were in compliance with the terms of the contract;
- Test compliance of the TSP participant support process with United States Code Title 5, Section 8439c; Code of Federal Regulations (CFR) Title 5, Part 1640; 5 CFR 1630.7b; and 5 CFR 1630.7c; and
- Determine the status of all prior EBSA TSP participant support open recommendations reported in *Performance Audit of the Thrift Savings Plan Participant Support Process as of August 14, 2009*.

### **B. Scope and Methodology**

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States using EBSA's *Thrift Savings Plan Fiduciary Oversight Program*. Our scope period for testing was January 1, 2011 through December 31, 2011. We performed the audit in four phases: (1) planning, (2) arranging for the engagement with the Agency, (3) testing and interviewing, and (4) report writing.

The planning phase was designed to assist team members to develop a collective understanding of the 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 tests of controls and compliance. We conducted these test procedures primarily at the Agency's headquarters in Washington, D.C., and the two TSP call centers located in Maryland and Virginia. In Appendix B, we identify the key documentation provided by Agency and contractor personnel that we reviewed during our performance audit.

Our performance audit procedures included testing a statistical sample of Congressional inquiries, which was used to determine if Congressional inquiries were tracked, forwarded to the Agency (if received by the contractor), and responded to in an accurate and timely manner. The objective of this statistical testing was to estimate the error rate for the population, as applicable, based on the error rate for a selected sample of such transactions.

Additionally, our performance audit procedures included testing non-statistical samples of the following:

- Participant statements, to determine if participants received accurate account information;
- Written inquiries, to determine if participant written inquiries were tracked and responded to in an accurate and timely manner;
- Confirmation notices, to determine if confirmation notices were processed accurately and distributed in a timely manner;
- Reject notices, to determine if reject notices were processed accurately and distributed in a timely manner;
- New hires, individuals with access to the TSP-dedicated portion of each call center's Local Area Network, individuals with physical access to the TSP-dedicated sections of the call centers, and separated individuals, to assess logical and physical access controls at both call centers;
- Call center employees, to assess the enforcement of certain training and Agency on-boarding requirements at both call centers; and

- Calls authenticated and transactions processed by call center representatives, to verify that authentication procedures were performed and to determine if transactions were processed accurately.

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

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

### **III. FINDINGS AND RECOMMENDATIONS**

#### **A. Introduction**

We performed procedures related to the Thrift Savings Plan (TSP) participant support process while conducting a performance audit at the Federal Retirement Thrift Investment Board's Staff (Agency) headquarters and the TSP call centers. Our scope period for testing was January 1, 2011 through December 31, 2011. This performance audit consisted of reviewing applicable policies and procedures and testing manual and automated processes and controls, which included interviewing key personnel, reviewing key reports and documentation (Appendix B), and observing selected procedures.

Based upon the performance audit procedures performed and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2011 through December 31, 2011 the Agency implemented certain procedures to (1) provide timely and accurate information to participants concerning the TSP, including their statement of account activity; (2) prepare quarterly statements for participants that reflected the activity for the period; (3) prepare annual statements for participants that summarized all transactions made during the previous calendar year by transaction type; (4) respond to participants' and Congressional inquiries in an accurate and timely manner; (5) process confirmation and reject notices accurately, and distribute them in a timely manner; and (6) monitor the call centers' contractors to ensure they were in compliance with the terms of the contract. However, we noted internal control weaknesses in certain areas that could adversely affect the TSP participant support process. As a result of our compliance testing, we did not identify any instances of noncompliance with United States Code Chapter 5, Section 8439c; Code of Federal Regulation (CFR) Title 5, Part 1640; 5 CFR 1630.7b; or 5 CFR 1630.7c in the TSP participant support process.

We present eight new recommendations related to the TSP participant support process, 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 participant support process. 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 A).

We also reviewed nine prior U.S. Department of Labor Employee Benefits Security Administration (EBSA) recommendations related to the TSP participant support process, identified in Section III.B, to determine their current status. These prior year recommendations were reported in *Performance Audit of the Thrift Savings Plan Participant Support Process as of August 14, 2009*. Section III.B documents the status of these prior recommendations. In summary, one of the recommendations has been closed, four recommendations have been partially implemented and remain open, and four recommendations have not been 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.

### **2009 Participant Support Process Recommendation No. 1:**

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

- a. Implement a vulnerability management program that identifies and implements corrective action plan requirements for the call center.
- b. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
- c. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
- d. Remove the Local Area Network (LAN) access for those individuals identified as separated or transferred, and enforce the requirements for removing separated and transferred employees' access timely.
- e. Disable Universal Serial Bus (USB) ports as required by the TSP security program on all required call center workstations.

Reason for Recommendation: During our 2009 testing at the Maryland call center, we identified several weaknesses related to logical access controls. Specifically, we noted that

a comprehensive vulnerability management program that monitors and patches technical security weaknesses was not in place over the technical infrastructure that supported the call center. Several high risk vulnerabilities were identified during the Agency's results of its internal scanning activities over the call center; however, no corrective action plans were developed and implemented. In addition, we identified several other vulnerabilities based on our external vulnerability scanning procedures over the call center. The Agency lacked the contractual requirements with the Maryland call center to enforce minimum information and technical security requirements.

We also identified control weaknesses in the processes for removing access for separated or transferred individuals, and disabling USB ports.

Status:

**Partially Implemented**

- a. and b. Weaknesses continue to exist in the Agency's process for monitoring the corrective actions taken to resolve vulnerabilities identified during periodic scans of the Maryland call center. Specifically, we noted during our 2012 audit procedures that the Agency did not require the Maryland call center to develop and submit a corrective action plan so it could track the status of mitigation activities. We also noted that the Agency was unable to determine if vulnerabilities identified during previous scans were being resolved as they were not tracked and monitored. Additionally, the Maryland call center was unaware of the vulnerabilities identified in its environment during the April 2012 vulnerability scan because the scanning application purged the results because of memory constraints. Therefore, these portions of the recommendation remain open.
- c. The existing contractual agreements with the call center contractor were not updated to incorporate information and technical security requirements. Therefore, this portion of the recommendation remains open.
- d. During our 2012 testing over logical access controls, we tested all 91 individuals who separated or transferred, and we did not identify any instances where the LAN access of these individuals was not properly removed. Therefore, this portion of the recommendation is considered



closed.

- e. The CD writing functionality had not been disabled for team lead workstations at the Maryland call center. Additionally, no Group Policy Object settings were in place to restrict USB ports or remove CD writing functionality for supervisors. Therefore, this portion of the recommendation remains open.

Disposition:            **Recommendation Open**

**2009 Participant Support Process Recommendation No. 2:**

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

- a. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
- b. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
- c. Remove LAN access for those individuals identified as separated or transferred, and enforce the requirements for removing separated and transferred employees' access timely.
- d. Disable USB ports as required by the TSP security program on all required call center workstations.

Reason for Recommendation:        During our 2009 testing at the Virginia call center, we identified several weaknesses related to logical access controls. Specifically, one vulnerability was identified during our external vulnerability scanning procedures at the call center. In addition, we identified control weaknesses in the processes for removing access for separated or transferred individuals, and disabling USB ports.

Status:                            **Partially Implemented**

- a. Weaknesses continue to exist in the Agency's process for monitoring the corrective actions taken to resolve vulnerabilities identified during periodic scans of the Virginia call center. Specifically, we noted

during our 2012 audit procedures that the Agency did not require the Virginia call center to develop and submit a corrective action plan so it could track the status of mitigation activities. We also noted that the Agency was unable to determine if vulnerabilities identified during previous scans were being resolved as they were not tracked and monitored. Therefore, this portion of the recommendation remains open.

- b. The existing contractual agreements with the call center contractor were not updated to incorporate information and technical security requirements. Therefore, this portion of the recommendation remains open.
- c. During our 2012 testing over logical access controls, we tested all 29 individuals who separated or transferred, and we did not identify any instances where the LAN access of these individuals was not properly removed. Therefore, this portion of the recommendation is considered closed.
- d. No settings were established in the Utimaco<sup>9</sup> policy to disable CD drives for Virginia call center workstations. Therefore, this portion of the recommendation remains open.

Disposition:            **Recommendation Open**

**2009 Participant Support Process Recommendation No. 3:**

Original            To address technology weaknesses at the Maryland call center, we  
Recommendation: recommend that the Agency:

- a. Monitor the call center’s plan to proceed with setting up an alternate storage site for Versadial backup media and to identify, select, and implement a method to encrypt the backups when stored off-site.
- b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).

---

<sup>9</sup> The Utimaco software provides data protection against unauthorized access, loss or theft of stationary and mobile devices with full disk encryption.

- c. For Internet browser settings at the call center, monitor to ensure that the auto-complete setting is “disabled” to prevent storing of usernames and passwords of the HelpLine system.
- d. Monitor the call center’s plan to proceed with upgrading the Windows NT environment to the Active Directory network.

Reason for

Recommendation:

The Maryland call center’s Versadial backups did not have an alternate storage site, and the password character length settings for Versadial were inconsistent with Agency requirements. We also noted that the Maryland’s call center HelpLine system, a custom application, contained personally identifiable information (PII) (e.g., social security numbers) and stored the username and password of the user. In addition, call center infrastructure continued to use Windows NT, which was no longer supported by Microsoft.

Status:

**Partially Implemented**

- a. The Maryland call center did not store its Versadial backup DVDs off-site during our scope period. Therefore, this portion of the recommendation remains open.
- b. The password length setting for the Versadial system at the Maryland call center was not compliant with TSP requirements, and the Agency did not document its acceptance of this risk. Therefore, this portion of the recommendation remains open.
- c. The auto-complete setting for the HelpLine system was changed to “disabled.” Therefore, this portion of the recommendation is considered closed.
- d. The Maryland call center upgraded its infrastructure to Windows 2003 and was no longer using Windows NT. Therefore, this portion of the recommendation is considered closed.

Disposition:

**Recommendation Open**

## **2009 Participant Support Process Recommendation No. 4:**

Original Recommendation: To address technology weaknesses at the Virginia call center, we recommend that the Agency:

- a. Identify, select, and implement a method to encrypt Versadial hard drive discs stored off-site and build redundant capabilities for Versadial servers at the call center. In addition, the Agency should ensure that unique user IDs and passwords for individuals performing administrative duties over Versadial are established.
- b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).

Reason for Recommendation: The Virginia call center's Versadial removable hard drive discs used to record audio calls were not encrypted when stored off-site. We also noted that the Versadial application login and password for the Versadial recorder were being shared by individuals performing administrative duties, and the password character length settings for Versadial were inconsistent with Agency requirements.

In addition, the Virginia call center's Versadial servers recorded phone calls on individual hard drives without redundant capabilities. In the event of hard drive failure, the Versadial server connected to the hard drive would stop recording phone calls, resulting in a single point of failure for that Versadial server recording calls.

Status: **Not Implemented**

- a. The Virginia call center's Versadial backup tapes were not encrypted when stored off-site during the scope period despite containing PII. Additionally, unique user IDs and passwords were not used for individuals performing administrative duties over the Versadial system at the Virginia call center. Therefore, this portion of the recommendation remains open.
- b. The password length setting for the Versadial system at the Virginia call center was not compliant with TSP requirements, and the Agency

did not document its acceptance of this risk. Therefore this portion of the recommendation remains open.

Disposition:            **Recommendation Open**

**2009 Participant Support Process Recommendation No. 5:**

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

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

Status:                            **Not Implemented**

During our 2012 audit procedures, we noted that weaknesses in physical access controls at the Maryland call center continued to exist. Specifically, we noted the following:

- Physical access forms or evidence of access recertification were not provided for any of the 10 new hires selected for testing.
- Evidence to support that datacenter access permissions were authorized and approved for 5 individuals selected for testing was not provided; evidence of access recertification was also not available for these individuals.
- Evidence to demonstrate that physical access permissions to the TSP doors at the call center were appropriately authorized and approved was not provided.
- One current call center employee and 13 terminated call center employees had access to the TSP doors but were not authorized to work on the TSP contract.

As a result of the items noted above, this recommendation remains open.

Disposition:            **Recommendation Open**

**2009 Participant Support Process Recommendation No. 6:**

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

- a. Monitor implementation of any corrective actions taken at the call center to improve physical security controls of the door to the supply room and external surveillance systems, and ensure that the selected option restricts access to the controlled areas as necessary and in accordance with the contract requirements for protecting sensitive equipment and participant information.
- b. Monitor implementation of any corrective actions taken at the call center to improve physical security controls for programming or replacing the A-cast badge access software system. The badge access system should contain the capability to separate general work areas from sensitive work areas at the individual access level.

Reason for Recommendation:        During our 2009 testing over physical access controls at the Virginia call center, we noted that one of the doors at the call center led to the power supply for the building. This door did not have adequate protection to deter forcible entry nor was it alarmed. In addition, the exterior of the building was not monitored through surveillance cameras.

We also noted that the proximity card reader system at the call center provided users with total access rather than restricting users' access to specific rooms. Therefore, individuals could be granted access to sensitive areas that may not have been necessary to fulfill their job responsibilities.

Status:                    **Partially Implemented**

- a. The three exterior doors to the Virginia call center with key locks were not alarmed and were not monitored by surveillance equipment. Therefore, this portion of the recommendation remains open.

- b. The A-cast badge access system was updated to include a separate access level for sensitive work areas. Therefore, this portion of the recommendation is considered closed.

Disposition:           **Recommendation Open**

**2009 Participant Support Process Recommendation No. 7:**

Original Recommendation:       The Agency should enforce the call center requirements for maintaining adequate evidence of privacy training.

Reason for Recommendation:   We identified weaknesses in the enforcement of privacy training requirements at both call centers. Specifically, we noted the Maryland call center did not retain evidence to support that 13 call center employees completed the Privacy Act Training. In addition, sign-in logs were not maintained for the Virginia call center’s Privacy Act Training. Therefore, we were unable to verify whether the training was provided to all call center employees.

Status:                   **Not Implemented**  
During our 2012 audit procedures, no documentation was available to demonstrate that personnel at either call center completed Privacy Act training during our scope period. Therefore, this recommendation remains open.

Disposition:           **Recommendation Open**

**2009 Participant Support Process Recommendation No. 8:**

Original Recommendation:       The Agency should re-evaluate the contractual provisions that require the contractor to respond to 90% of written inquiries within five business days to ensure the provision is reasonable, the response time is acceptable to maintain participant satisfaction, and any allowable exceptions to the requirement are clearly identified so that they may be tracked. The Agency should then monitor the contractor to ensure that the contractual

provisions are being met.

Reason for Recommendation: During our 2009 audit procedures, we randomly selected a sample of 58 written inquiries. For 12 of the written inquiries selected, we noted that a response was not provided within five business days. This represented 20.6% of our total sample size.

Status: **Not Implemented**  
During our 2012 audit procedures, Agency management indicated that they continue to deem reasonable the contractual provisions that require the contractor to respond to 90% of written inquiries within five business days. However, we randomly selected a sample of 58 written inquiries received during the period January 1, 2011 to December 31, 2011. For 13 of the written inquiries selected, we noted that a response was not provided within five business days. This represented 22.4% of our total sample size. Therefore, this recommendation remains open.

Disposition: **Recommendation Open**

**2009 Participant Support Process Recommendation No. 9:**

Original Recommendation: The Agency should enhance its monitoring procedures over Congressional inquiries to ensure that inquiries are responded to in a timely manner.

Reason for Recommendation: We randomly selected a sample of 58 Congressional inquiries for testing during our 2009 audit procedures. For 3 of the 58 items selected, we noted that a response was not provided by the Agency within 30 days.

Status: **Implemented**  
During our 2012 audit procedures, we randomly selected a sample of 58 Congressional inquiries for testing. Based on our testing, we noted that that the Agency provided responses for 54 of 58 Congressional inquiries tested within 30 days. The Agency responded to the remaining four Congressional inquiries within 33 days because of the nature of the



requests, which required additional time to research. The Agency's policy is to notify the inquiring Congressional office when the inquiry requires additional research and therefore cannot be responded to within 30 days. In each of the four cases, we noted that the Agency notified the Congressional office upon determining that additional research would be required. As a result, we concluded that the Agency had sufficient monitoring procedures in place over the timeliness of responses to Congressional inquiries. Therefore, this recommendation is considered closed.

Disposition:            **Recommendation Closed**

### **C.     2012 Findings and Recommendations**

While conducting our performance audit over the TSP participant support process, we identified eight new findings and developed related recommendations. EBSA requests appropriate and timely action for each recommendation.

#### **RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS**

##### **Additional Logical Access Control Weaknesses at the Call Centers**

During our current year audit procedures, we identified additional weaknesses in each call center's logical access controls. Specifically, we identified the following weaknesses at the Virginia call center:

- Internet access was not appropriately controlled at the call center. Specifically, three websites that Participant Support Representatives (PSRs) could access were not appropriate and were not necessary to perform their job functions.
- Call center network access approval e-mails were not available for any of the five new hires selected for testing.

In addition, we identified the following weaknesses at the Maryland call center:

- No evidence was provided that three of the ten employees selected from the call center new hire listing had a completed background investigation or non-disclosure agreement on file before being granted access to the Agency's virtual local area network (VLAN).
- No evidence was provided that six of the ten new hires selected at the call center had completed the required security awareness training before obtaining access to TSP resources.
- Network access approvals at the call center were not available for six of the ten new hires selected for testing.

With regard to Virginia call center, the network proxy server was configured to allow access to internet sites that were not necessary for employees to perform their job functions. In addition, the Virginia call center used e-mails to document network access approvals; however, call center management informed us that its e-mail server has limited storage capacity. As a result, old e-mails were purged. Therefore, the call center was unable to locate e-mails evidencing network access approval for the sample of newly hired employees.

Regarding the Maryland call center, the call center and the Agency did not follow protocol requiring that new employees obtain a background investigation and complete a non-disclosure agreement prior to being granted access to the Agency's VLAN. The Agency also informed us that the Maryland call center was responsible for ensuring that all employees completed security awareness training; however, the call center did not follow Agency protocol requiring that security awareness training be completed prior to granting access to TSP resources. In addition, the network access approvals were not available because the system used to track them was replaced during 2012 and the approvals were not retained when the new system was implemented.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, includes various relevant controls, as follows:

*SC-7: Boundary Protection*

“The information system:

- a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
- b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.”

In addition:

“(4) The organization:

- a. Implements a managed interface for each external telecommunication service;
  - b. Establishes a traffic flow policy for each managed interface;
  - c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;
  - d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
  - e. Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency]; and
  - f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
- (5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).”

*AC-2: Account Management*

“The organization manages information system accounts, including:

- a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary)...
- c. Identifying authorized users of the information system and specifying access privileges;
- d. Requiring appropriate approvals for requests to establish accounts;
- e. Establishing, activating, modifying, disabling, and removing accounts...
- i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions.”

*PS-6: Access Agreements*

“The organization:

- a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and
- b. Reviews/updates the access agreements [Assignment: organization-defined frequency].”

*PS-3 Personnel Screening*

“The organization...Screens individuals prior to authorizing access to the information system.”

*AT-3 Security Training*

“The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.”

- 1. To strengthen logical access controls at the Virginia call center, the Agency should:**
  - a. Review its proxy server periodically and remove all unnecessary internet sites.**
  - b. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.**
  
- 2. To strengthen logical access controls at the Maryland call center, the Agency should:**
  - a. Formalize and enforce the protocols that require all individuals to have a completed background investigation and sign non-disclosure agreements before they are granted access to the Agency portion of the VLAN.**
  - b. Develop and implement a monitoring process to ensure the call centers follow the Agency protocol that requires all individuals to complete security awareness training before they are granted access to any TSP information or information systems.**
  - c. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.**

Strengthening logical access controls would reduce the risk of unauthorized disclosure, modification, or destruction of TSP data and systems.

**Weaknesses in Call Center Controls over PII**

We identified weaknesses in the controls for storing and protecting PII data at both call centers. Specifically, we noted the following:

- The Maryland call center has modified the helpline log to store account numbers instead of social security numbers (SSNs); however, historical escalated call data that included participant SSNs had not been purged from the system.
- The Virginia call center stored participant SSNs in clear text in its escalated calls spreadsheet. The spreadsheet was stored on a shared network drive.

The Agency did not develop and implement a formalized policy addressing the protection of sensitive and PII information at each call center.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, section 4.1.1 Policy and Procedure Creation, identifies the following controls for protecting PII:

- “Organizations should develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level...
- Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways. One example is implementing role-based access control and configuring it so that each user can access only the pieces of data necessary for the user’s role. Another example is only permitting users to access PII through an application that tightly restricts their access to the PII, instead of permitting users to directly access the databases or files containing PII.”

NIST SP 800-122 also states:

- “An organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization’s business purpose and mission...
- If PII is no longer relevant and necessary, then PII should be properly destroyed. The destruction or disposal of PII must be conducted in accordance with any litigation holds and the Federal Records Act and records control schedules approved by the National Archives and Records Administration (NARA). Organizations should also ensure that retired hardware has been properly sanitized before disposal (e.g., no disk images contain PII, the hard drive has been properly sanitized). The effective management and prompt disposal of PII, in accordance with NARA-approved disposition schedules, will minimize the risk of unauthorized disclosure.”

3. **To strengthen controls over PII, the Agency should:**
  - a. **Develop guidelines for protecting PII data, and distribute them to the call center contractors for implementation.**
  - b. **Require the call center contractors to store all participant PII data within Agency-owned applications and databases.**
  - c. **Require the call center contractors to purge and sanitize all TSP participant data from contractor-owned systems and media when no longer required.**

Strengthening controls over PII data would reduce the risk that participant accounts may be compromised and PII data may be inappropriately disclosed.

### **Weaknesses in Call Center Configuration Management Controls**

During our current year audit procedures over call center configuration management controls, we noted the Agency had not established a standard workstation configuration for its call centers. In addition, we identified that the Virginia call center used Windows 2000 for Symposium and a SunGard EXP AG communications server. We also determined that the Maryland call center used Windows 2000 for Symposium and Oracle 8 for its helpline database. Windows 2000 and Oracle 8 are no longer supported by the vendor; as a result, no new patches will be released for these systems.

The Agency did not develop and implement a formalized policy which defines a standard workstation configuration for its call centers that is consistent with the United States Government Configuration Baseline. Additionally, both call centers used operating systems or databases that were no longer vendor-supported because they were waiting for a decision by the Agency regarding a replacement technology.

NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, includes the following relevant controls:

*CM-2 Configuration Management*

“The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.”

*CM-6: Configuration Settings*

“The organization:

- a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;
  - b. Implements the configuration settings;
  - c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and
  - d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedure.”
- 4. To strengthen configuration management controls at the call centers, the Agency should:**
- a. Establish a standard configuration baseline for its call center workstations that is consistent with the United States Government Configuration Baseline.**
  - b. Upgrade its TSP supporting systems at the call centers to vendor-supported software versions.**

The use of a standard baseline configuration would decrease the risk that security controls may not be uniformly applied to the call center operating environment and security vulnerabilities could be exploited. Additionally, the use of vendor-supported software would decrease the risk that TSP support systems may have exploitable security vulnerabilities that could allow malicious code or viruses to be introduced into the operating environment and security controls to be compromised.

#### **Weaknesses in Call Center Quality Monitoring Controls**

Call center management did not consistently perform quality monitoring of the PSRs in accordance with the Agency’s quality monitoring requirements. Specifically, we noted the following:

- A minimum of three quality monitoring results were not documented each month for Virginia call center PSRs in accordance with the Agency’s policy.
- At the Maryland call center, we identified eight instances in the five months selected where only two monitoring sessions were performed each month for PSRs, while Agency policy requires call centers to perform three to five monitoring sessions per PSR per month.

Each site had documented quality monitoring processes that were consistent with Agency requirements. However, the call centers did not follow the documented processes, and monitoring by the Agency did not identify this situation.

The *TSP Telephone Service Quality Assurance Program* dated July 21, 2006 states, “For program start-up, regular monitoring will consist of five calls per PSR per month. The intention is to eventually lower this to three per PSR per month as the PSR becomes more experienced and demonstrates consistent service delivery.”

**5. The Agency should develop and implement policies and procedures to periodically assess each call center to ensure call center management is performing quality monitoring in accordance with Agency requirements.**

Effective quality monitoring would assist the Agency in providing consistent, quality service to TSP participants; ensuring that Agency requirements are followed for participant authentication and dissemination of participant data; and identifying ways to improve services.

**Weakness in Maryland Call Center Contingency Planning Controls**

The Maryland call center did not have any redundancy built in to its Versadial server. Therefore, if any errors prevented the server from recording a call, call data would be lost. During our 2012 audit procedures, we noted that the Agency could not provide us with 6 of the 58 Maryland calls selected for testing because the Versadial system failed to record the calls.

As a part of the Maryland call center’s current backup strategy, participant calls were written to a DVD. When the DVD was full, an employee had to manually change the DVD to ensure that calls were being recorded. According to Maryland call center management, the DVDs were not changed at a regular interval because of staffing changes, resulting in calls not being recorded.

The call center was also using a tape backup system to record the participant call data instead of an additional Versadial server. However, the call center informed us that between February and May 2011, technical issues prevented the backup system from functioning correctly. As a result, the calls during this period were not backed up to tape.



NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, control CP 9 Information System Backup, states, “The organization:

- a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];
- b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives].”

**6. The Agency should work with the Maryland Call Center to implement mechanisms to ensure that Versadial data is consistently backed up and participant calls can be recovered from backups.**

Strengthening contingency planning controls would reduce the risk that the Agency would not be able to access critical data when needed.

**Weakness in Controls for Tracking Changes in Call Load Balancing**

The Agency did not have a mechanism in place to identify if the call centers made unauthorized changes to call load volumes. The Agency was using one vendor to provide phone service for its two call centers and to manage how call volumes were split between the call centers. In July 2011, the Agency transitioned from this vendor to a new vendor. However, the current vendor system has certain limitations and does not offer the functionality to track call load volume changes, and the Agency did not otherwise re-establish the tracking of call load volume changes.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, includes the following relevant controls:

*AU-3: Content of Audit Records*

“The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.”

*AU-6: Audit Review, Analysis, and Reporting*

“The organization:

- a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
- b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.”

**7. To strengthen controls for tracking changes in call load balancing, the Agency should:**

- a. Implement a mechanism to log and maintain call routing changes.**
- b. Develop and implement procedures to periodically review the logs for indications of unusual or unauthorized activity.**

The use of logging abilities decreases the risk that the Agency may not be aware of an inappropriate switch of call loads between the two call centers.

**Weaknesses in Call Center Controls for Media Handling and Disposal**

We identified weaknesses in media handling and disposal controls at both call centers. Specifically, we noted that the Agency had not identified and communicated to the call centers media protection requirements and media sanitization requirements.

According to Agency personnel, the Agency did not dedicate the resources needed to develop and implement a formal policy to address media protection and establish relationships with local contractors to dispose of media.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, includes the following relevant controls:

*MP-1: Media Protection Policy and Procedures*

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

- a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

- b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.”

*MP-6: Media Sanitization*

“The organization:

- a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
- b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.”

**8. The Agency should develop, implement, and communicate to its call center contractors media protection and sanitization policies and procedures.**

Media at the call centers potentially contains PII data related to TSP participants. As a result, implementing adequate media protection and sanitization requirements would decrease the risk that TSP participant data may be inappropriately disclosed.

**D. Summary of Open Recommendations**

**2009 RECOMMENDATIONS**

**FUNDAMENTAL CONTROL RECOMMENDATIONS**

- 1. To strengthen logical access controls at the Maryland call center, we recommend that the Agency:
  - a. Implement a vulnerability management program that identifies and implements corrective action plan requirements for the call center.
  - b. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
  - c. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
  - e. Disable USB ports as required by the TSP security program on all required call center workstations.

2. To strengthen logical access controls at the Virginia call center, we recommend that the Agency:
  - a. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
  - b. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
  - d. Disable USB ports as required by the TSP security program on all required call center workstations.
3. To address technology weaknesses at the Maryland call center, we recommend that the Agency:
  - a. Monitor the call center's plan to proceed with setting up an alternate storage site for Versadial backup media and to identify, select, and implement a method to encrypt the backups when stored off-site.
  - b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).
4. To address technology weaknesses at the Virginia call center, we recommend that the Agency:
  - a. Identify, select, and implement a method to encrypt Versadial hard drive discs stored off-site and build redundant capabilities for Versadial servers at the call center. In addition, the Agency should ensure that unique user IDs and passwords for individuals performing administrative duties over Versadial are established.
  - b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).
5. To strengthen physical access controls at the Maryland call center, we recommend that the Agency monitor implementation of any corrective actions at the call center that result from the evaluation of the physical access controls to prevent individuals from having more access than they need to perform their job functions.

6. To strengthen physical access controls at the Virginia call center, we recommend that the Agency:
  - a. Monitor implementation of any corrective actions taken at the call center to improve physical security controls of the door to the supply room and external surveillance systems, and ensure that the selected option restricts access to the controlled areas as necessary and in accordance with the contract requirements for protecting sensitive equipment and participant information.
7. The Agency should enforce the call center requirements for maintaining adequate evidence of privacy training.

#### **OTHER CONTROL RECOMMENDATION**

8. The Agency should re-evaluate the contractual provisions that require the contractor to respond to 90% of written inquiries within five business days to ensure the provision is reasonable, the response time is acceptable to maintain participant satisfaction, and any allowable exceptions to the requirement are clearly identified so that they may be tracked. The Agency should then monitor the contractor to ensure that the contractual provisions are being met.

#### **2012 RECOMMENDATIONS**

#### **FUNDAMENTAL CONTROL RECOMMENDATIONS**

1. To strengthen logical access controls at the Virginia call center, the Agency should:
  - a. Review its proxy server periodically and remove all unnecessary internet sites.
  - b. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.

2. To strengthen logical access controls at the Maryland call center, the Agency should:
  - a. Formalize and enforce the protocols that require all individuals to have a completed background investigation and sign non-disclosure agreements before they are granted access to the Agency portion of the VLAN.
  - b. Develop and implement a monitoring process to ensure the call centers follow the Agency protocol that requires all individuals to complete security awareness training before they are granted access to any TSP information or information systems.
  - c. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.
3. To strengthen controls over PII, the Agency should:
  - a. Develop guidelines for protecting PII data, and distribute them to the call center contractors for implementation.
  - b. Require the call center contractors to store all participant PII data within Agency-owned applications and databases.
  - c. Require the call center contractors to purge and sanitize all TSP participant data from contractor-owned systems and media when no longer required.
4. To strengthen configuration management controls at the call centers, the Agency should:
  - a. Establish a standard configuration baseline for its call center workstations that is consistent with the United States Government Configuration Baseline.
  - b. Upgrade its TSP supporting systems at the call centers to vendor-supported software versions.
5. The Agency should develop and implement policies and procedures to periodically assess each call center to ensure call center management is performing quality monitoring in accordance with Agency requirements.
6. The Agency should work with the Maryland Call Center to implement mechanisms to ensure that Versadial data is consistently backed up and participant calls can be recovered from backups.

7. To strengthen controls for tracking changes in call load balancing, the Agency should:
  - a. Implement a mechanism to log and maintain call routing changes.
  - b. Develop and implement procedures to periodically review the logs for indications of unusual or unauthorized activity.
8. The Agency should develop, implement, and communicate to its call center contractors media protection and sanitization policies and procedures.



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

March 14, 2013

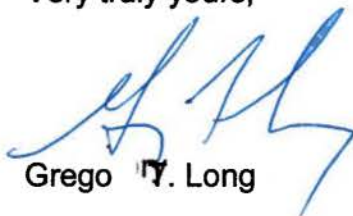
Mr. Ian Dingwall  
Chief Accountant  
Employee Benefits  
Security Administration  
United States Department of Labor  
Suite 400  
122 C Street, N.W.  
Washington, D.C. 20001-2109

Dear Ian:

This is in response to KPMG's email of March 11, 2013, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan Participant Support Process dated November 19, 2012. My comments with respect to this report are enclosed.

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

Very truly yours,



Gregory Long

Enclosure

A.1



Executive Director's Agency Staff Formal Comments on the  
Employee Benefits Security Administration's Performance of the  
Thrift Savings Plan Participant Support Process  
Dated November 19, 2012

**Prior Recommendations – Fundamental Control**

**2009 Recommendation No 1:**

1. To strengthen logical access controls at the Maryland call center, we recommend that the Agency:
  - a. Implement a vulnerability management program that identifies and implements corrective action plan requirements for the call center.
  - b. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
  - c. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
  - e. Disable USB ports as required by the TSP security program on all required call center workstations.

**Response:**

We concur with this recommendation. With respect to (a), the Agency issued the Risk Assessment (RA) policy on June 29, 2012. The Agency also has implemented an automated, centralized vulnerability management tool. Configuration of this tool to access the Maryland call center has been completed. Identified vulnerabilities have been reported to local support staff. The Plan of Actions and Milestones, "POA&M", document has been created and populated with outstanding weaknesses. The initial reviews of POA&M's for the Maryland call center will be completed by April 30, 2013. The additional action to modify the existing contract for the Maryland call center to incorporate standard security clauses, compelling the Contractor to cooperate with the FRTIB's Vulnerability Management program is expected to be completed by September 30, 2013.

With respect to subsection (b), the POA&M document has been created and populated with outstanding weakness. Upon completion of these initial reviews of POA&M's for the Maryland call center by April 30, 2013, we will consider subsection (b) to be closed.

With respect to (c), the Agency will modify the existing contract with the Maryland Call Center Contractor to incorporate the standard clauses required by the Enterprise Information System and Risk Management (EISRM) program policies by September 30, 2013. These clauses will compel the Contractor to establish a security program of their own which must comply with the EISRM. The Agency will also work with the Contractor to ensure that their security policies provide adequate protection for FRTIB and will provide guidance to the Contractor on how to implement the program. With the revision

to the contract to be completed by September 30, 2013, we will consider subsection (c) to be closed.

With respect to (e), we have taken steps to disable USB ports on all call center workstations; the USB ports at the Maryland call center were disabled by December 31, 2012. The Agency considers subsection (e) to be closed.

**2009 Recommendation No 2:**

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

- a. Monitor the implementation of corrective actions to address the high risk vulnerabilities identified at the call center.
- b. As necessary, assess and update existing contractual arrangements with the call center contractor to include all necessary compliance requirements for information and technical security.
- d. Disable USB ports as required by the TSP security program on all required call center workstations.

**Response:**

We concur with this recommendation. With respect to (a), the Agency issued the Risk Assessment (RA) policy on June 29, 2012. The Agency also has implemented an automated, centralized vulnerability management tool. Configuration of this tool to access the Virginia call center has been completed. Identified vulnerabilities have been reported to local support staff. The Plan of Actions and Milestones, "POA&M", document has been created and populated with outstanding weaknesses. Upon the Agency's completion of the initial POA&M's review for the Virginia call center by April 30, 2013, we will consider subsection (a) to be closed

With respect to (b), the Agency will modify the existing contract with the Virginia Call Center Contractor to incorporate the standard clauses required by the Enterprise Information System and Risk Management (EISRM) program policies by September 30, 2013. These clauses will compel the Contractor to comply with the EISRM in the performance of their work. With these revisions to the contract, we will consider subsection (c) to be closed. The contract modifications to include standard security clauses will be completed as we exercise option years.

With respect to (d), we have taken steps to disable USB ports. The Agency also has initiated a review of the implementation of the Utimaco configuration and will ensure that the configuration complies with the new EISRM policies. Agency staff are working with the Virginia contractor to implement the required controls. We expect subsection (d) to be closed by May 31, 2013.

### **2009 Recommendation No 3:**

To address technology weaknesses at the Maryland call center, we recommend that the Agency:

- a. Monitor the call center's plan to proceed with setting up an alternate storage site for Versadial backup media and to identify, select, and implement a method to encrypt the backups when stored off-site.
- b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).

### **Response:**

We concur with this recommendation. With respect to subsection (a), the Agency has asked the Contractor to submit a plan for the Agency's review by April 30, 2013. The Agency will work with the Contractor to document and implement proper security controls to address any identified issues. The Agency plans to complete its review by September 30, 2013.

With respect to subsection (b), the Agency's Identification and Authentication (IA) policy was issued on June 29, 2012. The Agency will modify the existing call center contract for the Maryland call center to incorporate standard security clauses, compelling the Contractor to conduct C&A's on Contractor-owned systems. Also, the Contractor will have to implement control requirements over passwords or develop compensating controls. The contract modification adding these security clauses is expected to be completed by September 30, 2013.

### **2009 Recommendation No 4:**

To address technology weaknesses at the Virginia call center, we recommend that the Agency:

- a. Identify, select, and implement a method to encrypt Versadial hard drive discs stored off-site and build redundant capabilities for Versadial servers at the call center. In addition, the Agency should ensure that unique user IDs and passwords for individuals performing administrative duties over Versadial are established.
- b. Evaluate and implement compensating controls over the minimum password length setting weakness of Versadial, or document the acceptance of this risk in appropriate security documentation (i.e., TSP System Security Plan).

### **Response:**

We concur with this recommendation. With respect to subsystem (a), the Agency issued the Identification and Authentication (IA) policy, the Media Protection (MP) policy, and the Access Control (AC) policies on June 29, 2012. The Agency will modify the existing call center contract for the Maryland call center to incorporate standard

security clauses, compelling the Contractor to implement EISRM requirements by September 30, 2013. The Agency is in the progress of designing and implementing protections for off-site call recording media and expects to complete this task by September 30, 2013. The Agency expects to implement separate user identifiers for individuals by April 30, 2013.

With respect to subsection (b), the Agency issued the Identification and Authentication (IA) policy, on June 29, 2012. The Agency will modify the existing call center contract for the Maryland call center to incorporate standard security clauses, compelling the Contractor to implement EISRM requirements by September 30, 2013. The Agency expects to complete implementing control requirements over passwords and/or developing compensating controls by April 30, 2013.

**2009 Recommendation No 5:**

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

**Response:**

We concur with this recommendation. The Contractor has removed the physical access for identified individuals. Going forward, the Agency will require the Contractor to perform regular reviews of its access control systems, including physical access, to ensure that only personnel authorized to work on the TSP contract are granted access to TSP systems and space. We will also require that the Contractor maintain records documenting the granting and removal of access to TSP space. We consider this recommendation to be closed.

**2009 Recommendation No 6:**

To strengthen physical access controls at the Virginia call center, we recommend that the Agency:

- a. Monitor implementation of any corrective actions taken at the call center to improve physical security controls of the door to the supply room and external surveillance systems, and ensure that the selected option restricts access to the controlled areas as necessary and in accordance with the contract requirements for protecting sensitive equipment and participant information.

**Response:**

We concur with this recommendation. The physical security deficiencies associated with the door have been corrected. The Agency has determined that installing intrusion detection sensors on the door and tying these sensors into the main building alarm

system is a more appropriate solution to implementing an external video surveillance system. Upon completion of these actions by April 30, 2013, we will consider the recommendation to be closed.

**2009 Recommendation No 7:**

The Agency should enforce the call center requirements for maintaining adequate evidence of privacy training.

**Response:**

We concur with this recommendation. We have required and confirmed that evidence of the 2012 privacy act training is available. In addition, each call center maintains a separate sign-in log to ensure all employees receive training. We consider this recommendation to be closed.

**2009 Recommendation No 8:**

The Agency should re-evaluate the contractual provisions that require the contractor to respond to 90% of written inquiries within five business days to ensure the provision is reasonable, the response time is acceptable to maintain participant satisfaction, and any allowable exceptions to the requirement are clearly identified so that they may be tracked. The Agency should then monitor the contractor to ensure that the contractual provisions are being met.

**Response:**

We concur with the recommendation. We re-evaluated the contract provisions and determined that the performance standard is appropriate. To meet this requirement, we augmented the staff working on written inquiries. As a result, the contractor was able to meet this metric in eight of twelve months during 2012. We continue to monitor this requirement. We consider this recommendation to be closed.

**2012 Recommendations to Address Fundamental Controls:**

**2012 Recommendation No 1:**

To strengthen logical access controls at the Virginia call center, the Agency should:

- a. Review its proxy server periodically and remove all unnecessary internet sites.
- b. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.

**Response:**

We concur with this recommendation, with respect to (a), the Agency has reviewed the proxy server configuration and removed unnecessary sites from the whitelist. In

A.6



A.7  
addition, the System Owner and the Information System Security Officer have established periodic reviews of the proxy server whitelist. We consider subsection (a) to be closed.

With respect to (b), the Agency has initiated a review of current access control procedures and will work with the Contractor to improve these procedures and ensure compliance with the EISRM policies. Review and revision of the current access control procedures will be completed by September 30, 2013. At that time, we will consider this recommendation to be closed.

### **2012 Recommendation No 2:**

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

- a. Formalize and enforce the protocols that require all individuals to have a completed background investigation and sign non-disclosure agreements before they are granted access to the Agency portion of the VLAN.
- b. Develop and implement a monitoring process to ensure the call centers follow the Agency protocol that requires all individuals to complete security awareness training before they are granted access to any TSP information or information systems.
- c. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.

### **Response:**

We concur with this recommendation. With respect to (a) and (c), the Agency notes that the individuals identified had completed background investigations and signed non-disclosure agreements prior to being hired; however, due to a change to the Contractor's ticketing program, which logs requests for systems access, the documentation to support the identified individuals was no longer retrievable. The Agency will require Contractor to improve existing procedures for maintaining network access documentation by March 1, 2014.

With respect to (b), security awareness training is completed prior to individuals taking calls; however we will require the Contractor to update its training procedures to require security awareness training during new-hire training. The Contractor has updated its training procedures to ensure security awareness training is completed prior to individuals taking calls. The Agency considers subsection (c) to be closed.

### **2012 Recommendation No 3:**

To strengthen controls over PII, the Agency should:

- a. Develop guidelines for protecting PII data, and distribute them to the call center contractors for implementation.
- b. Require the call center contractors to store all participant PII data within Agency-owned applications and databases.

- c. Require the call center contractors to purge and sanitize all TSP participant data from contractor-owned systems and media when no longer required.

**Response:**

We concur with this recommendation. The Agency will review the current contract and will modify the existing contract to incorporate the standard clauses required by the Enterprise Information System and Risk Management (EISRM) program policies by September 30, 2013. These clauses will require the Contractor to develop and implement a security policies and procedures in compliance with the Agency's EISRM. Upon modification of the contract; the Agency will consider this recommendation to be closed. The Data at Rest/Data in Motion procedures/guidelines will be completed by September 30, 2013.

**2012 Recommendation No 4:**

To strengthen configuration management controls at the call centers, the Agency should:

- a. Establish a standard configuration baseline for its call center workstations that is consistent with the United States Government Configuration Baseline.
- b. Upgrade its TSP supporting systems at the call centers to vendor-supported software versions.

**Response:**

We concur with this recommendation. With respect to subsection a, the Agency's CISO has promulgated the U.S. Government Configuration Baseline for Windows 7 as a standard configuration. We consider subsection (a) to be closed.

With respect to subsection b, the Agency is in the midst of a modernization effort of the telephony components supporting the call centers. The second phase of this project will eliminate the need for the legacy hardware and software that is completely out of support. The second phase of this project is anticipated to be completed by December 31, 2014.

**2012 Recommendation No 5:**

The Agency should develop and implement policies and procedures to periodically assess each call center to ensure call center management is performing quality monitoring in accordance with Agency requirements.

**Response:**

We concur with this recommendation. We have developed and implemented policies and procedures to periodically assess each call center to ensure call center

management is performing quality monitoring in accordance with Agency requirements. To clarify, the findings included PSR's who had limited telephone responsibilities and these PSR's received quality monitoring training based on other responsibilities, such as written correspondence. We have modified our Quality Assurance policies and procedures to ensure we have robust monitoring guidelines for agents who have limited telephone responsibilities. We consider this recommendation to be closed.

**2012 Recommendation No 6:**

The Agency should work with the Maryland Call Center to implement mechanisms to ensure that Versadial data is consistently backed up and participant calls can be recovered from backups.

**Response:**

We concur with this recommendation. The Versadial software at the Maryland Call Center has recently been updated. The Agency will require the contractor to document its back-up procedures and the Agency will review their procedures to ensure calls can be recovered as needed. These actions are expected to be completed by September 30, 2013. At that time, we will consider this recommendation to be closed.

**2012 Recommendation No 7:**

To strengthen controls for tracking changes in call load balancing, the Agency should:

- a. Implement a mechanism to log and maintain call routing changes.
- b. Develop and implement procedures to periodically review the logs for indications of unusual or unauthorized activity.

**Response:**

We concur with this recommendation. The Agency is in the process of modernizing the ThriftLine by bringing this system into the Agency's data center. As a result, all calls will be routed to the data center first and then to each call center. (Currently calls are routed to each call center by the telephone service provider.) With the modernization, changes to the call volume distribution will be handled within the Agency's ThriftLine system, instead of the telephone service provider. The Agency will ensure that the modernization to the ThriftLine will be able to provide sufficient reporting, such as a log of changes to the call routing. In the interim, changes are being logged on an Excel spreadsheet and activity history reports from the call provider website are being captured and reviewed on a bi-weekly basis. We consider this recommendation to be closed.

69



**2012 Recommendation No 8:**

The Agency should develop, implement, and communicate to its call center contractors media protection and sanitization policies and procedures.

**Response:**

We concur with this recommendation. The Agency's CISO promulgated the Media Protection policy on June 29<sup>th</sup>, 2012. The Agency will modify the existing contracts to incorporate the standard clauses required by the Enterprise Information System and Risk Management (EISRM) program policies by September 30, 2013. These clauses will compel the Contractor to comply with these policies. The Agency will work with the Contractor to achieve compliance. We will consider this recommendation to be closed upon modification of the contracts.

## KEY DOCUMENTATION AND REPORTS REVIEWED

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

- Quarterly Thrift Savings Plan (TSP) Meeting Agendas dated March, June, September, and December 2011
- Written Inquiry Quality Control Reports for the months of February, April, July, October, and December 2011
- Contract between the Agency and the Clintwood Call Center contractor (SI International)
- Report of all Congressional Inquiries for the time period January 1, 2011 to December 31, 2011
- Agency's Correspondence Processing Procedures dated August 1, 2007
- Written Correspondence Team Procedures Document Version 0.3 dated March 11, 2009
- Summary of Thrift Savings Plan dated February 2011
- TSP In Service Withdrawals dated July 2008
- TSP Payroll and Personnel Agency Representative meeting agendas for the months of January, March, June, and December 2011
- Report No. TSP 6011, *Inquiries for Clintwood, Spherix*, dated December 2009, December 2010, and December 2011
- Report No. TSP 6009, *Master Participant Notices Generated Summary Report*, for a sample of 58 dates between January 1, 2011 and December 31, 2011
- Report No. TSP 6017, *Participating Employees by Department*, as of September 30, 2011
- TSP calculator on the TSP website
- Annuity calculator on the TSP website
- Elective Deferral calculator on the TSP website
- Loan calculator on the TSP website
- 2011 Summary Monthly Performance Reports for February, April, July, October and December 2011
- Concurrent Sessions Setting for the OMNI application dated April 30, 2012
- ServiceAgility Customer Satisfaction Survey Report for surveys completed July 2011 to December 2011
- FRTIB Call Center Summary Monthly Reports for February, April, July, October, and December 2011
- AT&T Call Routing Process dated November 25, 2011
- 2011 Annual Summary of Issues
- TSP Call Center Operation Procedures Overview dated March 1, 2012

**KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED**

- Communication examples to participants
- Thrift Savings Plan Telephone Service Quality Assurance Program dated July 21, 2006

**Virginia Call Center Documents and Reports:**

- Serco Statement of Work dated July 20, 2011
- Serco Contractual Agreement (Addendum) dated March 31, 2011
- Standard Operating Procedures Operations Manual dated March 14, 2012
- Call Center Monthly Performance Reports, January 1 through December 31, 2011
- Escalated Call Listing, January 1 through December 31, 2011
- Call Verification Chart dated October 31, 2011
- Customer Satisfaction Survey Spreadsheet dated January to June 2011 and July to December 2011
- Call Volume Projection dated July 2011
- Employee Listing, January 1 through December 31, 2011
- Terminated Employee Listing, January 1 through December 31, 2011
- Active Network User Listing dated March 28, 2012
- Proximity Card (Physical Access) Listing dated May 10, 2012
- Group Policy Object for the Virginia Call Center Proxy Server dated May 16, 2012
- Proxy Server Whitelist dated April 26, 2012
- System Inventory Report dated May 1, 2012
- Software List dated May 1, 2012
- Utimaco Policy for Virginia Call Center Workstations dated May 16, 2012
- Refresher Training Records, 2011 and 2012
- New Hire Training Records dated March, August, and October 2011

**Maryland Call Center Documents and Reports:**

- Active Network Statement of Work dated April 30, 2008
- Forecasting and Scheduling Procedures dated June 3, 2010
- PSR Telephone Monitoring Form v 2.3 dated July 21, 2006
- 2011 QA Summary Results
- Call Center Monthly Performance Reports dated February, April, July, October and December 2011
- Escalated Call Procedures for PSRs dated March 1, 2012
- Escalated Call Listing, January 1 through December 31, 2011
- HelpLine Procedures dated March 1, 2012
- Call Verification Procedures dated March 2, 2012

**KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED**

- Quality Monitoring Spreadsheet dated February 2011, May 2011, July 2011, September 2011, and December 2011
- Current Employees Listing dated May 3, 2012
- New Hire Listing, January 1 through December 31, 2011
- Terminated Employee Listing, January 1 through December 31, 2011
- Facility Physical Access Listings dated April 2, 2012
- Proxy Server Whitelist dated April 4, 2012
- PSR Group Policy Objects dated April 4, 2012
- Team Lead Group Policy Objects dated April 4, 2012
- Hardware Inventory Listing dated April 4, 2012
- Software Listing dated May 9, 2012
- Training Procedures dated March 1, 2012
- Ongoing Training Records, January 1 through December 31, 2011
- New Hire Training Records, January 1 through December 31, 2011