Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Participant Support Operations

June 15, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

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

As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit of the Thrift Savings Plan (TSP) participant support process. Our fieldwork was performed from June 15, 2015 through December 22, 2015, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C., and at the two TSP call centers located in Virginia and Maryland. Our scope period for testing was January 1, 2014 through March 31, 2015.

We conducted this performance audit in accordance with the performance audit standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and the American Institute of Certified Public Accountants' *Standards for Consulting Services*. *Government Auditing 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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations;* United States Code (USC) Title 5, Chapter 84; and Code of Federal Regulations (CFR) Title 5, Parts 1630 and 1640.

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 are in compliance with the terms of the contract.

- Test compliance of the TSP participant support process with 5 USC, Section 8439(c) (hereinafter referred to as FERSA); and 5 CFR, Parts 1630.7(b), 1630.7(c), and 1640 (hereinafter referred to as Agency Regulations).

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of Thrift Savings Plan Participant Support Process as of November 19, 2012*.

We present 17 new recommendations, 13 addressing fundamental controls and 4 addressing other 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. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen the TSP participant support process. The Agency should review and consider these recommendations for timely implementation. Section III.C presents the details that support the current year findings and recommendations.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2014 through March 31, 2015, 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 are in compliance with the terms of the contract. 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. However, as indicated above, we noted internal control weaknesses in certain areas that could adversely affect the TSP participant support process.

We also reviewed 11 prior EBSA recommendations related to the TSP participant support process to determine their current status. Section III.B documents the status of these prior recommendations. In summary, six of the recommendations have been closed, four recommendations have been partially implemented and remain open, and one recommendation has not been implemented and remains 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, except for the following:

Recommendation Number	Auditors' Response
2009-7	Management concurred with the original recommendation but disagreed with the 2015 testing results, indicating that their process did not require new hires to document privacy training completion. However, without such evidence, the Agency was unable to support that the individuals identified had in fact completed the required training. As such, we did not revise this recommendation.
2015-10.a	Although management disagreed with the recommendation and asserted compliance of the Virginia call center System Security Plan (SSP) with NIST SP 800-53, Rev. 4, our testing indicated that the SSP provided to us during our audit did not comply with this requirement, as detailed in Section III.C of this report. As such, we did not revise this recommendation.
2015-10.b	Although management disagreed with the recommendation and asserted compliance of the Virginia call center SSP with NIST's minimum system security control requirements, our testing indicated that the Virginia call center SSP provided to us during our audit did not contain all minimum system security controls required by NIST SP 800-53, Rev. 4 for moderate systems, as detailed in Section III.C of this report. As such, we did not revise this recommendation.

Recommendation Number	Auditors' Response
2015-15	Although management disagreed with the finding, management indicated that actions were taken to address the recommendation. As such, we did not revise this recommendation.
2015-16	Management concurred with the finding but not the recommendation. However, management did not provide an alternative recommendation. As such, we did not revise this recommendation.

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

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

KPMG LLP

June 15, 2016

I. BACKGROUND OF THE TSP AND 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 the uniformed services, and members of Congress and certain Congressional employees. The TSP began accepting contributions on April 1, 1987, and as of March 31, 2015, had approximately $45 billion in assets and approximately 4.7 million participants[1].

The FERSA established the Federal Retirement Thrift Investment Board (the Board) and the position of Executive Director. The Executive Director manages the TSP for its participants and beneficiaries. The Board's Staff (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[2]

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 point of contact for actively employed TSP participants. Federal agency and uniformed service personnel offices provide the following participant support functions:

---

[1] Source: Minutes of the April 20, 2015, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

[2] Sources: Virginia Call Center Standard Operating Procedures (SOP), dated August 22, 2014 and Maryland Call Center SOP, dated January 4, 2013

- Inform all eligible employees/members of TSP options and benefits;
- Maintain adequate supplies of participant TSP election forms (if used by the employer)[3], booklets, and publications to facilitate participation;
- Determine retirement coverage;
- Provide and collect TSP election forms (Form TSP-1[4]);
- Process and submit TSP election forms to Federal agency and uniformed service payroll offices;
- Provide loan materials;
- Provide counseling and withdrawal information to TSP participants who are leaving Federal service; and
- Respond to inquiries about the TSP from active employees and members.

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 the TSP call centers. The centers also handle inquiries about loans, investment allocations, in-service withdrawals, and other benefits received from active participants. With respect to active participants, either personnel or payroll offices 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.

[3] Many agencies and services use automated self-service systems for enrollment in the TSP and other benefit programs. Therefore, activities associated with the processing of TSP election forms may vary among employers.

[4] Forms used by the uniformed service members are numbered the same as for civilians except they are denoted by a "U." For example, the Form TSP-1 for the uniformed services is Form TSP-U-1.

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 will receive 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 in the same manner as regular correspondence. Although most of the correspondence is referred to the Office of External Affairs for response, the Office of Participant Operations and Policy may assist with research and resolving issues or drafting the letters, as needed.

During calendar year 2014, the TSP processed approximately 2.2 million TSP participant telephone and approximately 76,000 written inquiries[5]. The TSP most frequently processes inquiries regarding withdrawal information. During calendar year 2014, inquiries related to this area accounted for 38 percent of all inquiries processed by the TSP[6].

Exhibit II-1[5] illustrates the number of written and telephone inquiries processed by the TSP during calendar years 2012 through 2014. Exhibit II-2[6] divides the total inquiries processed by the TSP during calendar year 2014 by type of transaction.

[5] Source: TSP 5003, *Inquiry Status Report,* for December 31, 2014, 2013, and 2012
[6] Source: TSP 6011, *Civilian and Uniformed Services Inquiry Report,* for December 2014

Exhibit II-1

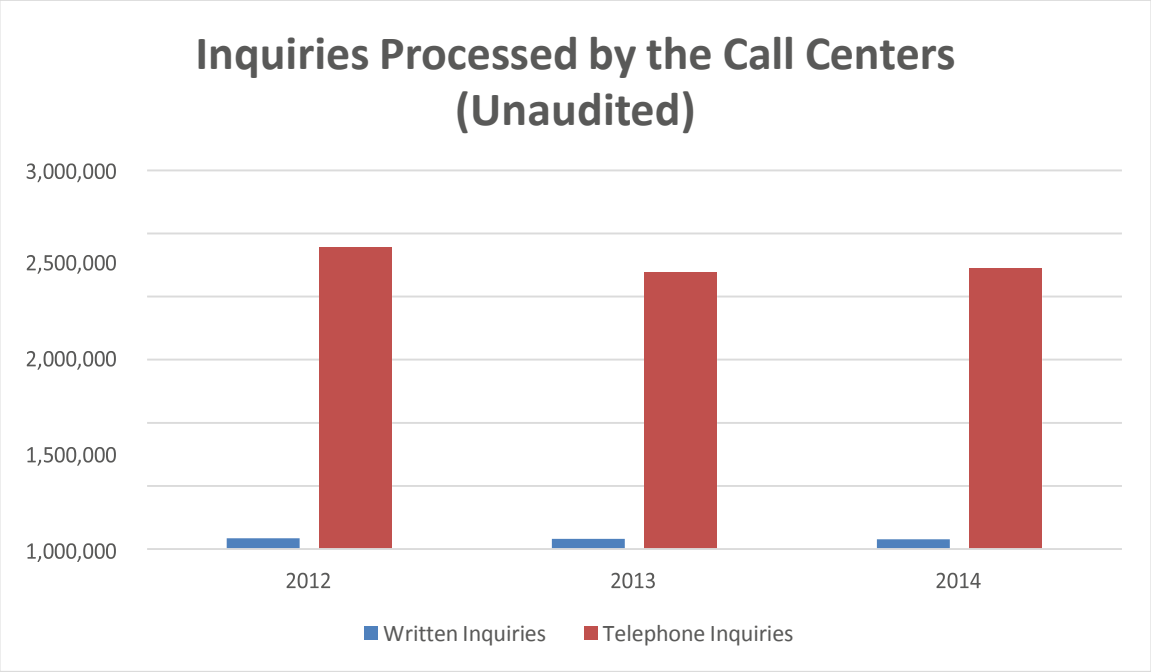
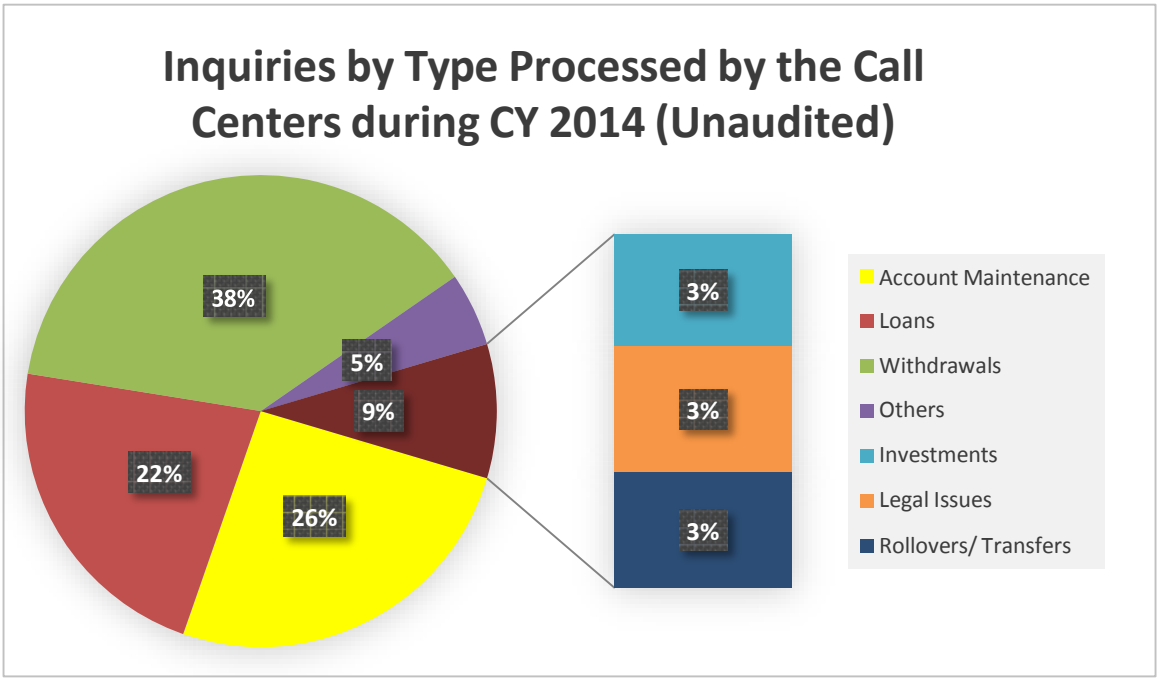


Exhibit II-2



2. Participant Statements[7]

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, and participants can request 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.

C. Description of the TSP Call Centers[8]

1. Overview of 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 website (www.tsp.gov), or mail correspondence to the TSP. By dialing the ThriftLine's toll-free number (1-877-968-3778), 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. While the inbound call volumes generally are divided between two call centers, the Maryland call center exclusively handles the Telecommunications Device for the Deaf (TDD) calls because the service has a unique telephone number. Participants can access a PSR during the hours of operation, which are 7:00 am to 9:00 pm eastern time, Monday through Friday.

The two competitively selected call centers are staffed by a call center manager and deputy, supervisors and team leads, helpdesk personnel, quality assurance coordinators, trainers,

---

7 Source: *Summary of the Thrift Savings Plan,* dated May 2012

8 Sources: TSP Telephone Service Quality Assurance Program, Virginia Call Center Standard Operating Procedures (SOP), dated August 22, 2014, and Maryland Call Center SOP, dated January 4, 2013.

workforce operations staff, and administrative support personnel. Depending upon the center, IT support may be dedicated to the TSP project or shared with other contracts. Each center determines its own staffing complement based on forecasted call volumes, management requirements, and work to be performed. The Virginia call center is a Government owned/Contractor operated (GOCO) facility, while the Maryland call center 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 TSP program specific information, use of the TSP applications (e.g., PSR and EXP AG[9]), and additional customer service skills training. Selected senior PSRs (e.g., team leads and the helpdesk personnel) hold additional responsibilities such as performing research requests for issues that cannot be resolved on first contact and handling escalations. The primary responsibility of supervisors is to supervise floor operations, which includes directing the PSRs and managing performance metrics (i.e., service level is being achieved) that are reported via the Symposium Automated Call Distribution (ACD) software. 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, which is a term used to describe senior PSRs who can perform supervisory duties related to assisting other PSRs, such as coaching, call monitoring, and handling escalations. The deputy call center manager serves as a backup to the call center manager and is responsible for floor operations, managing the quality assurance function (e.g., the monitoring of phone calls, follow-up coaching, and performance appraisals), managing the research and fulfillment functions, and reporting 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 contractual requirements (i.e., the achievement of contract performance standards).

[9] EXP AG is the Agency's document imaging system.

2. 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 current maximum call handling capacity of 168 concurrent calls (24 calls carried per T1-line at 7 T1-lines (i.e., one bundle). One server is active at any time with the other VRU serving as a backup. Physical access to the data centers containing these servers is controlled through the use of electronic badges.

As toll-free calls arrive at the AT&T network, the call is presented to a Nortel Meridian 1 private branch exchange (PBX) and 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**,** the following processes occur using the VRU, Computer Telephony Integration (CTI) software, and Nortel Symposium software to transfer the call to the PSR:

- The VRU uses information provided by the participant to access OMNIPlus[10]. When the participant information is retrieved from the VRU request, 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.

All participant calls are recorded by the Versadial server, which has five, 32-Gigabyte hard disk partitions. All calls are recorded and stored on one of the hard disk partitions and on CDs or DVDs. When a hard disk partition is full, Versadial automatically switches to a new hard disk partition. The hard disk partitions are backed up daily to the TSP primary data center.

3. Customer Service Delivery

The call center is an important option for participant interaction with the TSP. Each interaction directly influences the participant's perception of customer service; for example, the length of time

[10] OMNIPlus is the core record keeping engine for the TSP system.

it takes to talk with a PSR, the ability of a PSR to answer participant questions, and the quality of communication during the interaction can influence the participant's perceptions towards the quality of service. As such, the ultimate success of a call center operation depends on the proper blend of people, implemented processes, and enabled technologies, employed together towards consistent customer service. The TSP's call centers' service delivery and customer service capabilities and performance can be separated into the following areas: a) Quality Assurance and Customer Feedback Program; b) Service Delivery Procedures; c) Performance Metrics; and d) Technology Support.

a. Quality Assurance and Customer Feedback Program

The Agency has a Quality Assurance (QA) program and a Customer Satisfaction survey process to collect and analyze feedback through the call centers. Both programs were developed and maintained with the assistance of consulting groups.

The QA program consists of quality monitoring sessions performed by quality assurance coordinators. Quality assurance coordinators randomly select a pre-determined number of recorded calls to which to listen so that they can review each PSR's activity each month (e.g., three to five per month for new hires and 2 to 4 per month for experienced PSRs). The calls centers employ quality monitoring software, which records the audio and screen shot activity of the call. The quality assurance coordinators select and evaluate calls using their experience with the program and customer service training, and score attributes of the call under the categories of foundation skills and finesse skills.

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, quality assurance 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 the calls monitored. Surveys are only to be conducted on those calls that have been monitored for quality assurance 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.

b. Service Delivery Procedures

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 phone etiquette skills.

The TSP call handling procedures are communicated through formal training. 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 PSR or observing the call within a controlled environment. This technique is used to improve the PSRs' call handling capabilities before taking live calls on their own. Call handling processes 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 useful training materials that the PSR uses as reference material). In addition, as discussed above, QA monitoring and coaching provide PSRs with information on their performance related to program requirements, proper phone etiquette, and call handling techniques.

Providing information to participants about upcoming events or changes to the program prior to the event or change is an example of proactive communication. Being proactive allows the Agency to synchronize activities across the call centers in order to prepare in advance for known disruptions to service or program changes. The Agency has demonstrated proactive communication through Thrift Line information messages, TSP website postings, example questions and answers (Q's and A's), and TSP Highlights. The TSP website also provides forms, publications, and plan news, among other items. These communications can reduce the number of routine telephone calls that the call centers receive. In addition, a weekly call

among all TSP operational units is held to discuss, among other topics, issues that are impacting, or could impact, the volume of calls and repeat inquiries that the call centers have experienced.

c. Performance Metrics

Performance metrics manage, measure, and monitor the effectiveness and efficiency of the call centers in areas such as time to answer, time on hold, abandonment rate, first contact resolution, and staff productivity. The performance metrics are contractual requirements of the call centers.

The Agency monitors multiple reports monthly and 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.

Each call center's management monitors performance standards more frequently. 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 call centers may consider changing workforce variables through the workforce scheduling and forecasting software.

d. Technology Support

The PSR's ability to serve participants is directly related to the performance of the information system. Such performance is defined in terms of a system that provides PSRs with accurate, timely, and readily available information. All PSR workstations in the call centers are equipped with a standard PC configuration. The PC configuration includes Microsoft Windows 7 Professional x86, Microsoft Office 2010 (Word, Excel, PowerPoint, and Outlook), Adobe XI, Java 7 Update 79, Adobe Flash, Desktop Central Agent, McAfee Antivirus, Sophos Safeguard, Verint Popup Client, PopPSR, and Trustwave. PSR workstations have the ability to access the Internet; however, access is restricted to only websites that contribute to performing PSR duties

(i.e., government websites). E-mail is available at one of the centers. Supervisor and team lead workstations include full Internet access for purposes of performing research.

The core applications used by the PSR include the PSR application, EXP AG, and the Moxie knowledge database. The PSR application is the customer account history and inquiry logging software used to provide participants with information related to their accounts (such as account balance, loan, contribution, and withdrawal information). The PSR server resides in Virginia, and the Agency, via a contractor, performs user administration of the application.

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 EXP AG server resides in Virginia, and the Agency, via a contractor, performs user administration of the application.

The Moxie knowledge database 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 server on which it resides is located in Virginia.

The core applications used by supervisors include the Symposium workbench, Verint, and Versadial. The Symposium software is used to monitor 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 Telephone Service Factor. The Symposium servers are located locally at each of the centers, and each administers access to the software locally.

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 = 270 seconds/call

Average wrap-up time = 120 seconds/call
Shrinkage (absenteeism and other) = 10%

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. The Verient servers are located at each center, and each administers access to the software locally.

The Versadial software is used for the quality monitoring process as described in the Customer Feedback section above. Every call is recorded. The Versadial servers are located at each of the call centers, and each call center administers access to the software locally. The Versadial servers are incrementally backed up daily to the primary data center in Virginia. In addition, the Virginia call center uses the Envision software application to capture voice and screenshots.

II. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objective

The U.S. Department of Labor Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit of the Thrift Savings Plan (TSP) participant support process.

The objectives of this performance audit were to:

- Determine if the Federal Retirement Thrift Investment Board's Staff (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 are in compliance with the terms of the contract.

- Test compliance of the TSP participant support process with United States Code Chapter 5, Section 8439(c); and Code of Federal Regulations Title 5, Parts 1630.7(b), 1630.7(c), and 1640.

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of Thrift Savings Plan Participant Support Process as of November 19, 2012*.

B. Scope and Methodology

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and the American Institute of Certified Public Accountants' *Standards for Consulting Services*, using EBSA's *Thrift Savings Plan Fiduciary Oversight Program*. Our scope period for testing was January 1, 2014 through March 31, 2015. 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 the TSP participant support process. 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[11]. We conducted these test procedures at the Agency's headquarters in Washington D.C. and at the two TSP call centers located in Virginia and Maryland. 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 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;
- Congressional inquiries, 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;
- 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 (LAN), 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

[11] We obtained and utilized certain information technology system settings and user listings related to the participant support process subsequent to the scope period. The Agency represented that such settings were functionally and technically the same as those in place from January 1, 2014 through March 31, 2015.

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

Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the sample items 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 two TSP call centers located in Virginia and Maryland. Our scope period for testing was January 1, 2014 through March 31, 2015. This performance audit consisted of reviewing applicable policies and procedures and testing manual and automated processes and controls, which included interviewing key personnel, reviewing key reports and documentation (Appendix B), and observing selected procedures.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2014 through March 31, 2015, 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 are in compliance with the terms of the contract. As a result of our compliance testing, we did not identify any instances of noncompliance with United States Code Chapter 5, Section 8439(c); Code of Federal Regulations (CFR) Title 5, Parts 1630.7(b), 1630.7(c), or 1640. However, we noted internal control weaknesses in certain areas that could adversely affect the TSP participant support process.

We present 17 new recommendations, presented in Section III.C, related to TSP participant support process; 13 addressing fundamental controls and 4 addressing other 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. Other control recommendations address procedures or processes that are less significant than fundamental controls. 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 11 prior U.S. Department of Labor Employee Benefits Security Administration (EBSA) recommendations related to the TSP participant support process to determine their current status. Section III.B documents the status of these prior recommendations. In summary, six recommendations have been implemented and closed, four recommendations have been partially implemented and remain open, and one recommendation has not been implemented and remains open.

Section III.C presents the new 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. 3:

Title:	Call Center Technology Weaknesses Should Be Addressed
Original Recommendation:	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).

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:

Implemented.

Parts c and d of the original recommendation were closed in the report titled, *Performance Audit of the Thrift Savings Plan Participant Support Process as of November 19, 2012*. In addition, part b of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations as of June 23, 2014*. Therefore, these parts were not included in the scope of our 2015 performance audit.

a) The Maryland call center began backing up Versadial calls to the primary data center in Virginia during Quarter 4 (Q4) 2013. Versadial data is backed up nightly at the primary data center in Virginia on tapes using IBM Tivoli Storage Manager (TSM), and copies are sent off-site for storage. TSM tape backups of the Versadial information are encrypted using the AES set of encryption algorithms, a current National Institute of Standards and Technology (NIST)-approved encryption standard. Hard drive discs of TSM data are encrypted when sent

off-site for storage. As such, this portion of the recommendation is closed.

Disposition: **Recommendation Closed.**

2009 Participant Support Recommendation No. 4:

Title: Call Center Technology Weaknesses Should Be Addressed

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 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: **Partially Implemented.**

Part b of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations as of June 23, 2014;* therefore, it was not included in the scope of our 2015 performance audit.

a) The Virginia call center began backing up Versadial calls to the primary data center in Virginia during Q4 2013. Versadial data is backed up nightly at the primary data center in Vienna on tapes using IBM TSM, and copies are sent off-site for storage. TSM tape backups of the Versadial information are encrypted using the AES set of encryption algorithms, a current NIST-approved encryption standard. Hard drive discs of TSM data are encrypted when sent off-site for storage.

   While actions were taken to address backup storage and off-site storage encryption for current data, we noted that older copies of Versadial recordings on DVD/external hard drives remain offsite and unencrypted. These recording cover the period of 2005-2013. Additionally, we noted that Versadial had not been updated, and therefore, was not configured to require unique user IDs and passwords for administrative users as required by Agency policy. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

2009 Participant Support Recommendation No. 7:

Title: Information Privacy Requirements Should Be Enforced at the Call Centers

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: **Partially Implemented.**

For a selection of users tested at the Virginia call center, we noted no exceptions related to privacy training. However, although privacy trainings were offered during the year, the Maryland call center was unable to provide evidence of privacy training during our scope period for two of 15 individuals tested, as required by the contract.

Disposition: **Recommendation Open.**

2009 Participant Support Recommendation No. 8:

Title: Participant Written Inquiries Process Should Be Strengthened

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: **Implemented.**

During our 2015 testing, we determined that the Agency reviewed the related contractual provisions and believes that the provisions were reasonable with an understanding that some exceptions for extraordinary cases may occur. We also tested the Agency's monthly quality control review for January 2014, October 2014, and February 2015 to verify that the Agency was monitoring the provisions of the contract; we noted no exception on the design, implementation, or operating effectiveness of this control. Additionally, in our sample of written inquiries during the scope period, we noted that a response was provided within five business days for 89% of them, only 1% less than the contractual provision.

Disposition: **Recommendation Closed.**

2012 Participant Support Process Recommendation No. 1:

Title: Additional Logical Access Control Weaknesses at the Call Centers

Original Recommendation: 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.

Reason for Recommendation: During our 2012 performance audit, 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.

Status: **Not Implemented.**

a) During our 2015 testing, we identified that six websites, including some previously reported on the whitelist (i.e., list of websites allowed to be viewed), were not removed, were unnecessary for individual PSR job functions, and posed potential security risks to PSR workstations and participant data. As such, this portion of the recommendation remains open.
b) During our 2015 testing, evidence of approval for three of five new network requests selected were not provided. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

2012 Participant Support Process Recommendation No. 2:

Title: Additional Logical Access Control Weaknesses at the Call Centers

Original Recommendation: 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.

Reason for Recommendation: During our 2012 performance audit, 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.

Status: **Implemented.**

Part b of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations No. 2, November 18, 2014*. In addition, part c of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations, June 23, 2014*. Therefore, these parts were not included in the scope of our 2015 performance audit.

a) The Agency implemented procedures requiring individuals to have a background investigation and signed non-disclosure agreement completed before obtaining logical access to TSP systems. During our testing, we noted that background investigations were conducted and signed non-disclosure agreements were completed prior to obtaining logical access to PSR, EXP AG, and the Maryland call center VLAN for the five individuals selected. As such, this portion of the recommendation is closed.

Disposition: **Recommendation Closed.**

2012 Participant Support Process Recommendation No. 4:

Title: Weaknesses in Call Center Configuration Management Controls

Original Recommendation: 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.

Reason for Recommendation: During our 2012 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 and 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.

Status: **Partially Implemented.**

Part a of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations, June 23, 2014;* therefore, it was not included in the scope of our 2015 performance audit.

b) During our 2015 testing, we noted the Maryland call center upgraded its TSP supporting systems; however, both systems remained on unsupported platforms. Specifically, we noted the Knowledge database had been upgraded to the unsupported Oracle 9.2.040, and the Symposium server was still running on Windows 2000.

We noted the Virginia call center had upgraded its TSP supporting systems; however, one system remained on an unsupported platform. Specifically, the Symposium servers were running on Windows 2003. As such, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

2012 Participant Support Process Recommendation No. 5:

Title: Weaknesses in Call Center Quality Monitoring Controls

Original Recommendation: 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.

Reason for Recommendation: Call center management did not consistently perform quality monitoring of the PSRs in accordance with the Agency's quality monitoring requirements.

Status: **Implemented.**

During our 2015 testing, we noted that the Agency had developed and implemented a TSP Quality Assurance Plan and supporting monitoring guidance for the Maryland and Virginia call centers to use when performing quality monitoring reviews. Additionally, contractual requirements require both call centers to report the results of quality monitoring reviews monthly. We tested a sample of three months and determined that both call centers performed quality monitoring reviews and reported quality monitoring results in accordance with the TSP Quality Assurance Plan and contractual requirements.

Disposition: **Recommendation Closed.**

2012 Participant Support Process Recommendation No. 6:

Title:	Weaknesses in Maryland Call Center Contingency Planning Controls
Original Recommendation:	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.
Reason for Recommendation:	During our 2012 performance audit, we noted that 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. In our sample of 58 Maryland calls, we noted that the Agency could not provide us with 6 calls because the Versadial system failed to record the calls.
Status:	**Implemented**. During our 2015 testing, we noted that the Maryland call center implemented procedures to backup Versadial data nightly to servers in the primary data center in Virginia during Q4 2013. Further, we noted that for all three Maryland calls selected for testing, evidence of their backup and recording was available and provided.
Disposition:	**Recommendation Closed**.

2012 Participant Support Process Recommendation No. 7:

Title:	Weaknesses in Controls for Tracking Changes in Call Load Balancing
Original Recommendation:	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.

Reason for Recommendation: The Agency did not have a mechanism in place to identify if the call centers made unauthorized changes to call load volumes.

Status: **Implemented.**

Part a of the original recommendation was closed in the report titled, *Performance Audit of the Status of Certain Thrift Savings Plan Prior Year Recommendations, June 23, 2014;* therefore, it was not included in the scope of our 2015 performance audit.

b) During our 2015 testing, we noted that the Agency implemented procedures for switching call loads between the Maryland and Virginia call centers. Additionally, the Agency maintained and reviewed manual call logs periodically for indications of unusual or unauthorized activity. As such, this portion of the recommendation is closed.

Disposition: **Recommendation Closed.**

2012 Participant Support Process Recommendation No. 8:

Title: Weaknesses in Call Center Controls for Media Handling and Disposal

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

Reason for Recommendation: 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.

Status: **Partially Implemented.**

During our 2015 testing, we noted that although policy and procedures were developed and implemented at the Agency level, detailed media protection and sanitization procedures did not consider call center specific processes.

Disposition: **Recommendation Open**.

C. 2015 Findings and Recommendations

While conducting our performance audit over TSP participant support process, we identified 17 new findings and developed related recommendations. EBSA requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Control Weaknesses in Administering Logical Access to Agency Systems

During our audit procedures, we noted certain logical access control weaknesses in the provisioning and removal of logical access at each call center, particularly to the PSR application, SunGard EXP AG, and call center-specific local area networks (LANs). Specifically, we identified the following weaknesses:

At the Maryland call center:

- Two of five individuals selected for test procedures obtained local LAN access prior to obtaining appropriate management approval;
- Four of 190 PSR users selected for test procedures retained access to PSR after 180 days of inactivity;
- Twenty-nine of 259 SunGard EXP AG users selected for test procedures retained access to SunGard EXP AG after 180 days of inactivity;
- Eleven of 194 LAN accounts retained access to the local LAN after 180 days of inactivity; and
- Ten of fifteen SunGard users selected for test procedures retained access to SunGard EXP AG after termination.

At the Virginia call center:

- Fourteen of 185 SunGard EXP AG users selected for test procedures retained access to SunGard EXP AG after 180 days of inactivity;
- Sixty-five of 155 LAN users, all system accounts, retained access to the local LAN after 180 days of inactivity;
- One of five SunGard users selected for test procedures retained access to SunGard EXP AG after termination; and
- One individual that transferred roles as a PSR agent to a Help Desk Support role in November 2014 maintained unnecessary administrative access to PSR as of June 29, 2015.

These conditions existed because the Agency did not enforce existing processes and procedures and did not properly coordinate with the Service Desk for removal of access and notification from the call centers of terminated or transferred employees.

The Agency's Enterprise Information Security and Risk Management (EISRM) *Access Control (AC) Policy*, dated June 26, 2012, states:

> (a) Account Management (CM-2 + Enhancements 1, 2, 3, and 4)
>
> Each Information System Owner, in cooperation with, and subject to the approval of, the Information Owners having information contained or processed within each Information System, SHALL assign Information System Custodians to be responsible for the daily administration of all Information System access, including creating, activating, modifying, disabling, and removing accounts. Additionally, […]
>
> (2) Information System Custodians/Account Managers and Security Administrators SHALL follow designated procedures for creating, activating, modifying, disabling, and removing user accounts and authentication credentials, including, but not limited to: […]
>
> (C) Reviewing account access privileges for appropriateness based on type of account and current requirements, including reviewing: […]
>
> (iii) All in-active accounts after 90 days of inactivity to determine whether each should be disabled; all inactive account which cannot be justified for continued access MUST be disabled after 180 days of inactivity. […]
>
> (F) Disabling accounts and removing all access immediately upon notification by the Information System Owner, Information Owner, FRTIB Security personnel,

FRTIB Personnel Office, or Contractor Management (regarding the contractor's own employees or a subcontractor's employees) of the following conditions:

(i) Termination or suspension (i.e., when placed on administrative leave) of a User; […]

(3) Users SHALL:

(A) Be authorized by the Information Owner and Information System Owner prior to accessing a particular information resource. […]

NIST Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Access Control (AC), Control AC-2 states:

Control: The organization: […]

a. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;

b. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined personnel or conditions*] […]

1. The Agency should enforce the existing EISRM policies that require:

a. Users to obtain appropriate Agency and call center management approval prior to obtaining system access;

b. Disabling of user accounts that exceed Agency-established periods of inactivity; and

c. Timely removal of user access to Agency systems when employees and contractors are terminated or transfer job functions.

The lack of disabling terminated, transferred, or inactive accounts and the administering of access to Agency systems without appropriate approvals increase the risk that individuals may have unnecessary or inappropriate access to Agency systems and data, which places Agency systems at risk of inadvertent or deliberate disclosure, modification, or destruction.

Weaknesses in the Call Center Access Recertification Process

Access recertification weaknesses existed during our scope period at the Virginia and Maryland call centers. Specifically, we noted the following:

- While evidence of a recertification of user access was provided by the Agency for Agency-managed systems, the documentation did not specify for which application(s) the recertification was completed, the individuals covered by the review, the levels of access evaluated, the timing of review, and the performer of the recertification; and
- A recertification of user access to the Virginia and Maryland call center networks, managed by the call centers, was not performed in accordance with Agency policy.
- Access to the PSR application, the application used to process participant transactions by call center representatives, was not restricted based on job function. At the Maryland call center, 1 of 15 call center representatives from our sample maintained excessive access to the PSR application, including the IDENTADH and XSPR roles (i.e., roles with supervisor-level access). At the Virginia call center, 1 of 15 call center representatives from our sample maintained excessive access to the PSR application, including the CSPR role (i.e., role with supervisor-level access).

Agency and call center management did not comply with Agency requirements to perform and adequately document a recertification of Agency and call center-managed systems because of the lack of sufficient management oversight to comply with Agency requirements. Additionally, the Agency and call centers did not develop, document, and implement recertification procedures for systems that support the Virginia and Maryland call centers, including Agency-managed systems and call center-managed systems.

The Agency's EISRM *Access Control (AC) Policy*, dated June 26, 2012, states:

> (2) Information System Custodians/Account Managers and Security Administrators SHALL follow designated procedures for creating, activating, modifying, disabling, and removing user accounts and authentication credentials, including, but not limited to: […]
>
> (C) Reviewing account access privileges for appropriateness based on type of account and current requirements, including reviewing:
>
> (i) All active permanent accounts for appropriateness of assigned access rights no less than annually […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Access Control (AC), Control AC-2 states:

> Control: The organization: […]
>
> j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*]; […]

The Agency's *EISRM Access Control (AC) Policy,* dated June 26, 2012, states:

> (e) Least Privilege (AC-6)
>
> (1) Information System Owners, in cooperation with Information Owners and the Information System Security Manager/CISO, SHALL ensure that Information Systems enforce the most restrictive set of rights/privileges or access needed by users (or processes acting on behalf of users) for the performance of specified tasks.
>
> (2) Information System Owners SHALL employ the concept of least privilege when assigning rights related to specific duties and Information System access (as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals) in accordance with:
>
> (A) Job descriptions,
>
> (B) Risk assessments,
>
> (C) Audit findings, and
>
> (D) IA Best Practices.
>
> (3) The "Least Privilege" principle includes, but is not limited to, the following:
>
> (A) User rights/privileges,
>
> (B) Physical access,
>
> (C) Logical access […]

2. The Agency should:

a. Develop, document, and implement recertification procedures for systems that support the Virginia and Maryland call centers, including Agency-managed systems and call center-managed systems; and

b. Develop, document, and implement monitoring procedures to ensure Agency and call center compliance with Agency recertification requirements.

The lack of a periodic review of access permissions increases the risk that individuals may have unnecessary or inappropriate access to Agency and call center systems and data, which places Agency and call center systems and data at risk of inadvertent or deliberate disclosure, modification, or destruction.

Weakness in Restricting Internet Access at the Maryland Call Center

During our scope period, we noted that at the Maryland call center, the internet whitelist, which governs which websites PSRs may access, had not been reviewed to restrict access and remove unnecessary sites. This condition existed because procedures were not developed or documented for reviewing the internet whitelist periodically for appropriateness.

The Agency's EISRM *System and Communications Protection (SC) Policy*, dated June 29, 2012, states:

> 6. POLICIES & CONTROLS:
>
> (e) BOUNDARY PROTECTION (SC-7 + Enhancement #1, #2, #3, #4, #5, & #7)
>
> (1) Information System Owners under the supervision and guidance of the Chief Technology Officer (CTO) and the Chief Information Security Officer, SHALL ensure that Information Systems are protected from external and internal network based attacks by:
>
> (A) Allowing connections to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged and configured in accordance with FRTIB security architecture policies and standards, including:
>
> (iv) Establishing a traffic flow policy for each managed interface [Enhancement #4b]; and
>
> - Documenting each exception to the traffic flow policy with a waiver (signed by the Authorizing Official) supporting mission/business need and duration of that need [Enhancement #4d] as well as compensating controls;
> - Reviewing exceptions to the traffic flow policy annually [Enhancement #4e]; and
> - Removing traffic flow policy exceptions that are no longer supported by an explicit mission/business need [Enhancement #4f]. […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, System and Communications Protection (SC), Control SC-7 states:

> Control: The information system:
>
> a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; […]

3. To strengthen security controls, the Agency should develop, document, and implement monitoring procedures to ensure that Maryland call center management periodically reviews the internet whitelist and removes all unnecessary internet sites.

Inappropriate internet access for PSRs poses potential security risks to Agency systems and data and increases the risk of inadvertent or deliberate unauthorized disclosure, modification, or destruction of Agency systems and participant data.

Versadial Password Weaknesses at the Virginia Call Center

Both call centers use the Versadial call recording software. However, the version of Versadial in use during our scope period at the Virginia call center did not meet the minimum password character length settings as required by Agency policy. Although newer versions of Versadial, including the version used by the Maryland call center, include minimum password length controls, the Virginia call center had not upgraded its Versadial version because of technical limitations. Some Agency management officials were not aware that different Versadial versions were in use at each call center.

The Agency's EISRM *Identification and Authentication (IA) Policy*, dated June 26, 2012, states:

> (d) AUTHENTICATOR MANAGEMENT (IA-5 + Enhancements #1, 2, & 3)
>
> (1) Information System Owners, in cooperation with Information System administrators, Security Engineers, and Information System Security Officers (ISSOs) and with the review and approval of the Information System Security Manager (i.e., the CISO or a designated representative thereof, acting as the Certification Agent), SHALL manage Information System authenticators (e.g., passwords and tokens) by: […]

(I) Requiring users to take, and having devices implement, specific measures to safeguard authenticators, e.g., using strong passwords [as described in (2)(C) below]:

(2) For password-based authentication, Information System Architects, Developers, Administrators, and Engineers, in cooperation with Information System Security Officers (ISSOs), SHALL ensure that Information Systems: […]

(C) Require Users (employees and contractors) to employ "strong" passwords. Strong passwords require the use of at least twelve (12) characters with at least one character from each of the following categories:

(i) Upper case letters,

(ii) Lower case letters,

(iii) Numbers, and

(iv) Special characters, including, but not limited to any of the following:

☐ [ ] ! @ # $ % ^ & * ( ) { } < > […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Identification and Authentication (IA), Control IA-5 states:

Control: The organization manages information system authenticators by:

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators […]

4. To address password weaknesses at the Virginia call center, the Agency should require that Virginia call center management upgrade Versadial to a version that includes minimum password length controls, or document the acceptance of this risk and compensating controls in appropriate security documentation.

Call center technology is a critical component in supporting participants, and protecting participant information is an integral part of providing this support. Weak passwords increase the risks associated with unauthorized access and disclosure of participant information.

Call Center Physical Access Control Weaknesses

During our audit procedures, we identified certain physical access weaknesses at the Virginia call center server room and Maryland call center data center[12]. Specifically, we noted the following:

- Of five individuals in our sample with access to the Virginia call center server room, one was not appropriately authorized; and
- Physical access for all users to the Maryland call center and the call center's data center and the Virginia call center server room were not recertified annually.

This condition existed because of a lack of oversight by call center and Agency management.

The Agency's EISRM *Physical and Environmental (PE) Policy*, dated June 26, 2012, states:

(a) PHYSICAL ACCESS AUTHORIZATIONS (PE-2) […]

(2) FRTIB Facilities Managers SHALL:

(A) Annually review and approve the access list and authorization credentials.

(B) Promptly remove from the access list personnel no longer requiring access to facilities where Information Systems reside. […]

(b) PHYSICAL ACCESS CONTROL (PE-3)

(1) FRTIB Facilities Managers SHALL:

(A) Control all physical access points (including designated entry/exit points) to the facilities where FRTIB Information Systems reside, (except for those areas within the facility officially designated as publicly accessible);

(B) Verify individual access authorizations before granting access to the facility […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Physical and Environmental Protection (PE), Control PE-2 states:

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

[12] The Maryland call center, as a Contractor owned/Contractor operated facility, hosts its own data center. The facility supports multiple clients, including FRTIB. The Maryland call center data center is entirely separate from and managed differently from the FRTIB production data center in Virginia.

c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and
d. Removes individuals from the facility access list when access is no longer required.

5. To strengthen call center physical access controls, the Agency should:

a. Develop, document, and implement monitoring procedures to enforce EISRM policies that require pre-approval for physical access to secured areas of the call center facility; and

b. Develop, document, and implement monitoring procedures to ensure that call center management periodically reviews data center and server room access at the Maryland and Virginia call centers, respectively.

Weaknesses in controls for authorizing and periodically reviewing data center physical access permissions increase the risk that individuals may have inappropriate access to Agency systems and data, which places them at risk of inadvertent or deliberate disclosure, modification, or destruction.

Call Center Configuration and Patch Management Weaknesses

Configuration and patch management vulnerabilities and weaknesses existed at both call centers during our scope period. Agency management did not ensure that the necessary security updates or patches were applied or were applied timely to Agency systems, or that call center workstations complied with Agency-required settings. Specifically, we noted the following:

- The Agency and call center management did not ensure timely remediation of Virginia call center vulnerabilities in accordance with Agency policy. We noted that high, medium, and low configuration and patch management weaknesses remained on servers and workstations supporting the Virginia call center beyond Agency-established timelines for required remediation.
- The Agency and call center management did not document or track vulnerabilities using a Plan of Action and Milestone (POA&M), or ensure timely remediation of Maryland call center vulnerabilities in accordance with Agency policy. We noted that high, medium, and low configuration and patch management weaknesses remained on servers and workstations supporting the Maryland call center beyond Agency-established timelines for required remediation.

- The Agency did not provide workstation images or Agency-defined baseline configurations to each call center, or monitor whether workstations at each call center complied with United States Government Configuration Baseline (USGCB) settings.

These conditions occurred because the Agency had not defined procedures, nor clearly delineated responsibilities in the contract, for oversight and enforcement of Agency security requirements, including developing and monitoring of Agency-defined USGCB settings on all call center workstations. Additionally, the Maryland call center Assessment and Authorization (A&A) process was ongoing during our fieldwork; however, call center management did not plan to actively remediate known vulnerabilities until the completion of the A&A process, which could take several months.

The Agency's EISRM *System and Information Integrity (SI) Policy*, dated June 26, 2012, states:

(a) FLAW REMEDIATION (SI-2 + Enhancements #1 & #2) […]

(2) The Chief Information Security Officer (CISO) with the cooperation of Information System Owners SHALL ensure that that designated Security Personnel employ automated vulnerability assessment tools [Enhancement #2] on a monthly basis (at minimum) in order to detect software and hardware flaws and: […]

(3) Information System Owners SHALL ensure that any vulnerabilities discovered through the scanning process and/or reported to them by the CISO [or a designated representative thereof], an internal audit, or external auditors are:

(A) Placed in the appropriate Information System Plan of Action and Milestones (POA&M) document; and

(B) Remediated within the specified period based upon the System Security Categorization and CVSS impact scores, as follows:[…]

(ii) Information Systems with a MODERATE FIPS 199 Security Categorization:

- High impact vulnerability: mitigation =< 20 days;
- Moderate impact vulnerability: mitigation =< 30 days;
- Low impact vulnerability: mitigation =< 60 days; […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Configuration Management (CM), Control CM-6 states:

Control: The organization:

a. Establishes and documents 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 any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Risk Assessment (RA), Control RA-5 states:

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, System and Information Integrity (SI), Control SI-2 states:

Control: The organization:

a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

The Agency's EISRM *Configuration Management (CM) Policy*, dated June 29, 2012, states:

(a) BASELINE CONFIGURATION (CM-2 + Enhancements "1, 3, [4] or 5, 6)

(1) The Authorizing Official [i.e., the Chief Technology Officer or a designated representative thereof] SHALL ensure that a baseline configuration is established and maintained for all Information Systems throughout the System Development Life Cycle (SDLC) and SHALL ensure that the baseline configuration documentation includes:

(A) A well-defined and detailed set of design specifications to which the Information System is built;

(B) Information about the components of an Information System, including but not limited to:

(i) Standard Hardware, including firmware revisions for all devices (e.g., Mainframe, servers, workstations, notebook computers, routers, and switches),

(ii) Standard Operating Systems, including versions and patch levels,

(iii) Standard software loaded on all computing devices, including versions and patch levels […]

6. The Agency should:

a. Develop, document, and implement monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely and in accordance with Agency policy;

b. Develop, document, and implement monitoring procedures for the Maryland call center to ensure that call center management documents and tracks

vulnerabilities and to ensure that vulnerabilities are identified and remediated timely and in accordance with Agency policy;

c. **Define procedures and modify call center contract language, as necessary, to clearly delineate responsibilities for oversight and enforcement of Agency information security requirements at non-Agency facilities specific to vulnerability management; and**

d. **Provide workstation images or Agency-defined baseline configurations to each call center and periodically monitor workstation compliance with USGCB settings.**

Because security updates or patches are released to mitigate the risk of vulnerabilities affecting operating systems or applications, the untimely application of security updates or patches increases the risk of potential compromise of the confidentiality, integrity, and availability of data residing on the information system. Without timely remediation of vulnerabilities in the Agency and call center information technology (IT) environments, an increased risk exists that systems and network flaws in their IT environments could expose sensitive participant information and Agency systems and applications to attacks, unauthorized modification, or data compromise. Additionally, failure to comply with the USGCB settings requirements increases the risk of an unauthorized user gaining access Agency systems and participant data.

Call Center Contract Oversight Weaknesses

We determined that certain contracting oversight weaknesses existed for the Maryland and Virginia call centers. Specifically, we noted that Agency management did not:

- Formalize responsibilities across various Agency offices and centrally track and communicate contractor compliance with Section H – *Information and Information System Security/Privacy Requirements for IT Contracts* (Section H) of the Agency's call center contracts;
- Review or modify call center contracts to ensure clear delineation of responsibilities, where applicable, for Agency and contractor-managed sites;
- Modify call center contracts timely after the Agency determined that portions of Section H of the contracts did not apply or were no longer relevant, in particular sections that referred to a material breach of the contract related to the lack of a Statements on Standards for Attestation Engagements No. 16 examination and report;

- Monitor the Maryland call center monthly to ensure contract compliance with the blocked call metric included in the contract; and
- Monitor the Virginia call center to ensure contract compliance with the outbound call metric included in the contract.

Agency management did not formalize contract compliance reporting channels, methods and timelines with contracting officials across appropriate Agency offices because of a lack of contract oversight requirements. Additionally, in an attempt to address weaknesses in the prior contracts with both call centers, Agency management included standardized security clauses in each call center contract without fully evaluating their relevance and impact to each call center, and the contracting officer was not informed of subsequent requirement changes in order to make modifications to the contract.

Office of Management and Budget Circular No. A-123, *Management's Responsibility for Internal Control*, dated December 21, 2004, states:

> Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. […] Management should identify internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, management should take into account relevant interactions within the organization as well as with outside organizations. […] Identified risks should then be analyzed for their potential effect or impact on the agency. […] It is management's responsibility to develop and maintain effective internal control.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Standards) states:

> Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

7. The Agency should complete the following activities related to call center contract oversight and management:

a. **Formalize and document call center contract oversight management procedures and responsible parties to ensure each appropriate Agency office understands its contract oversight roles and responsibilities;**
b. **Review and modify each call center contract, as needed, to ensure that all call center contract clauses are relevant, specific, and applicable to each call center environment and clearly delineate responsibilities for Agency and contractor-managed sites;**
c. **Ensure timely coordination with the contracting officer for any subsequent changes to the call center contracts; and**
d. **Develop, document, and implement procedures to enforce contract compliance with required reporting metrics.**

The Agency's reliance upon contractors for mission critical activities such as call center services makes effective management and oversight of call center contracts critical. Without proper oversight of call center contracts, the Agency is at increased risk of poor contractor performance, miscommunication, and mission critical failures.

Encryption Weaknesses on Local Versadial Data Storage

Participant information recorded using the Versadial software located at the Maryland and Virginia call centers is not encrypted, although the data recorded contains sensitive information and PII. Backups of this data reside at the primary data center in Vienna and at each call center.

Because of competing priorities and limited resources, Agency management had not evaluated, purchased, installed, or implemented a product or solution to encrypt Versadial recorded information at the call centers.

The Agency's EISRM *System and Communication Protection (SC),* dated June 26, 2012, states:

(k) PROTECTION OF INFORMATION AT REST (SC-28)

(1) Unless Information Systems are otherwise protected by alternative physical measures, Information System Owners, under the supervision and guidance of the Chief Technology Officer (CTO) and the Chief Information Security Officer, SHALL ensure that Information Systems employ cryptographic mechanisms to prevent unauthorized disclosure and modification of information "at rest" [Enhancement #1], including but not limited to protecting: […]

(B) The Confidentiality and Integrity of information/data as it resides on secondary storage, including, but not limited to:
(i) Proprietary,
(ii) Business Confidential,
(iii) Classified, and/or
(iv) Personal information and Personally Identifiable Information (PII).

NIST 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, System and Communications Protection (SC), Control SC-28 states:

Control: The information system protects the [Selection (one or more): confidentiality; integrity] of [*Assignment: organization-defined information at rest*].

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION
The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].

8. The Agency should identify and implement a solution to encrypt the Versadial data and servers that contain PII and are physically located at each call center.

Without proper encryption and safekeeping of recorded participant calls at each call center, participant data, including PII, is at risk of inadvertent or deliberate disclosure.

Encryption Weaknesses on Maryland Call Center Workstations

We determined that data on workstations at the Maryland call center were not encrypted, as required by Agency policy and contract, and may contain sensitive participant information. Because of a lack of Agency oversight and enforcement, call center management had not installed and implemented a product or solution to encrypt these workstations.

The Agency's EISRM *System and Communication Protection (SC)*, dated June 26, 2012, states:

(k) PROTECTION OF INFORMATION AT REST (SC-28)
(1) Unless Information Systems are otherwise protected by alternative physical measures, Information System Owners, under the supervision and guidance of the

Chief Technology Officer (CTO) and the Chief Information Security Officer, SHALL ensure that Information Systems employ cryptographic mechanisms to prevent unauthorized disclosure and modification of information "at rest" [Enhancement #1], including but not limited to protecting: […]

(B) The Confidentiality and Integrity of information/data as it resides on secondary storage, including, but not limited to:
  (i) Proprietary,
  (ii) Business Confidential,
  (iii) Classified, and/or
  (iv) Personal information and Personally Identifiable Information (PII).

NIST 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, System and Communications Protection (SC), Control SC-28 states:

Control: The information system protects the [Selection (one or more): confidentiality; integrity] of [*Assignment: organization-defined information at rest*].

Control Enhancements:

(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION
The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined information*] on [*Assignment: organization-defined information system components*].

9. The Agency should work with Maryland call center management to identify and implement a solution to encrypt data retained on PSR workstations used for handling participant data.

Lack of proper encryption and safekeeping of call center data stored on PSR workstations increases the risk of inadvertent or deliberate disclosure, modification, or destruction of participant data.

Weaknesses in the Virginia Call Center Security Management Program

During our audit procedures, we identified certain weaknesses in the security management program at the Virginia call center. Specifically, we noted the following:

- The Virginia call center System Security Plan (SSP) was not updated to fully comply with NIST SP 800-53, Rev. 4, within the mandated timeframe. Specifically, we noted that the provided SSP, approved on September 24, 2014, had not been fully updated to include NIST SP 800-53, Rev. 4 guidance related to PL-8, *Information Security Architecture Control*, and CM-11, *User Installed Software Control*;
- The Agency did not properly document minimum security controls and associated requirements within the Virginia call center SSP, as required by NIST for moderate systems. Specifically, we noted that the provided SSP, approved on September 24, 2014, did not specify how the controls were implemented, relevant scoping guidance, if the controls were common controls, and the responsible party for implementation;
- The Agency did not update the Virginia call center Plan of Actions and Milestones (POA&M) quarterly as required by Agency policy;
- As of July 21, 2015, the Virginia call center had not remediated or accepted the risk associated with an Agency-defined Authority to Operate (ATO) requirement from November 2014. The ATO required that the Agency and call center address the lack of an automated fire suppression capability at the Virginia call center within 60 days of authorization; and
- Although a Privacy Threshold Assessment (PTA) determined PII was stored at the Virginia call center, as of July 2015, the Agency had not completed a Privacy Impact Assessment (PIA) for this call center.

These conditions existed because of the lack of Agency management oversight of the Virginia call center contract's security requirements. Additionally, for 14 of 15 months of our scope period, the Agency operated without approved POA&M monitoring procedures because of lack of enforcement of Agency policies requiring continuous monitoring activities.

NIST Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, states:

> 8. Implementations.
>
> […] Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended.
>
> 9. Effective Date.

This standard is effective immediately. Federal agencies must be in compliance with this standard not later than one year from its effective date.

NIST 800-18, Rev. 1, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, dated February 2006, states:

3.14 Minimum Security Controls

Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented;

3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

The Agency's EISRM *Security Planning (PL) Policy,* dated June 29, 2012, states:

(a) SYSTEM SECURITY PLAN (PL-2 + Enhancement #1) […]

(H) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions and compensating controls (if applicable); […]

The Agency's EISRM *Program Management (PM) Policy,* dated June 29, 2012, states:

(d) PLAN OF ACTION AND MILESTONES PROCESS (PM-4) […]

(1) The Chief Information Security Officer (CISO), in cooperation with the Chief Technology Officer (as Authorizing Official) and all Information System Owners, SHALL establish a Plan of Action and Milestones (POA&M) process (as per NIST SP 800-37) in order to:

(D) Ensure that Plans of Action and Milestones (POA&Ms) documents are maintained for:

(i) Individual Information Systems […]

(B) Document the individual and collective actions taken to mitigate risks […]

(2) The POA&M process SHALL include a template for tracking individual POA&M items and/or control development as well as all mitigations collectively throughout the System Development Life Cycle, by including: […]

(E) Current Status of the POA&M item; and

(F) Dates of POA&M item completion:
(i) Scheduled; and
(ii) Actual.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Assessment and Authorization (CA), Control CA-5 states:

a. Develops a plan of action and milestones for the information system to document the organizations planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

The Agency's EISRM *System Authorization (CA) Policy*, dated June 29, 2012, states:

(e) SECURITY AUTHORIZATION (CA-6)
Before allowing the Information System to commence initial operations, then every three years thereafter or whenever the Information System configuration is significantly altered through upgrading, reconfiguring, or replacing components, the Authorizing Official [i.e., either the Chief Technology Officer or a designated representative thereof, as defined in (e)(1) above] SHALL:
(A) Review the Authorization "Package" (as per NIST 800-37) including:
(i) The current (i.e., up-to-date) System Security Plan (see PL-2)
(ii) Initial Security Assessment Report (SAR) and (for continuing Authorization or renewal) Annual Assessment Reports; and
(iii)The current (i.e., up –to-date) Plan of Action & Milestones Document.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Assessment and Authorization (CA), Control CA-6 states:

Control: The organization: […]

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations […]

The Agency's EISRM *Security Planning (PL) Policy*, dated June 29, 2012 states:

(d) PRIVACY IMPACT ASSESSMENT (PL-5)

(1) Unless waived by the Executive Director, in accordance with privacy provisions of the E-Government Act of 2002, the Authorizing Official (i.e., the CTO or a designated representative thereof) SHALL ensure that:

(A) System Owners (or designated representatives thereof, e.g., Information System Security Officers) conduct:

(i) A Privacy Threshold Analysis (PTA) on all Information Systems to determine if those systems contain Personally Identifiable Information (PII); and

(ii) if that determination is positive, a Privacy Impact Assessment on Information Systems determined (through the PTA, above) to contain Personally Identifiable Information (PII) […]

10. To strengthen the security management program at the Virginia call center, the Agency should:

a. Update the Virginia call center SSP to comply with NIST SP 800-53, Rev. 4;

b. Document all minimum system security controls as required by NIST for moderate systems in the Virginia call center SSP;

c. Enforce monitoring activities required of security personnel, including quarterly review and update of the POA&M and assessment of compliance with ATO requirements for the Virginia call center; and

d. Complete a PIA for the Virginia call center.

By not reviewing and updating the SSP and POA&Ms and not complying with ATO and PIA requirements, Agency management may not be aware of the security risks posed by the system. Without such awareness, an increased risk exists of inadvertent or deliberate disclosure, modification, or destruction of Agency systems or participant data.

Weaknesses in the Maryland Call Center Security Management Program

During our audit procedures, we identified certain weaknesses in the security management program at the Maryland call center. Specifically, we noted the following:

- During our scope period, the Agency had not performed an A&A review, including an ATO, at the Maryland call center as required by the contract;

- The Agency did not track known weaknesses or vulnerabilities at the Maryland call center as required by Agency policy; and
- Within our scope period, a PTA had not been performed for the Maryland call center.

These conditions occurred because of a lack of Maryland call center contract oversight by the Agency related to contractor security requirements. Additionally, for 14 of 15 months of our scope period, the Agency operated without approved POA&M monitoring procedures because of a lack of enforcement of Agency policies requiring continuous monitoring activities.

The Agency's EISRM *System Authorization (CA) Policy,* dated June 29, 2012, states:

> (e) SECURITY AUTHORIZATION (CA-6)
>
> Before allowing the Information System to commence initial operations, then every three years thereafter or whenever the Information System configuration is significantly altered through upgrading, reconfiguring, or replacing components, the Authorizing Official [i.e., either the Chief Technology Officer or a designated representative thereof, as defined in (e)(1) above] SHALL:
>
> (A) Review the Authorization "Package" (as per NIST 800-37) including:
>
> (i) The current (i.e., up-to-date) System Security Plan (see PL-2)
>
> (ii) Initial Security Assessment Report (SAR) and (for continuing Authorization or renewal) Annual Assessment Reports; and
>
> (iii)The current (i.e., up –to-date) Plan of Action & Milestones Document.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Assessment and Authorization (CA-6) states:

> Control: The organization: […]
>
> b. Ensures that the authorizing official authorizes the information system for processing before commencing operations […]

The Agency's EISRM *Program Management (PM) Policy,* dated June 29, 2012, states:

> (d) PLAN OF ACTION AND MILESTONES PROCESS (PM-4) […]
>
> (1) The Chief Information Security Officer (CISO), in cooperation with the Chief Technology Officer (as Authorizing Official) and all Information System Owners, SHALL establish a Plan of Action and Milestones (POA&M) process (as per NIST SP 800-37) in order to:

(A) Ensure that Plans of Action and Milestones (POA&Ms) documents are maintained for: […]

(i) Individual Information Systems […]

(B) Document the individual and collective actions taken to mitigate risks […]

(2) The POA&M process SHALL include a template for tracking individual POA&M items and/or control development as well as all mitigations collectively throughout the System Development Life Cycle, by including: […]

(E) Current Status of the POA&M item; and

(F) Dates of POA&M item completion:

(i) Scheduled; and

(ii) Actual.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Security Assessment and Authorization (CA), Control CA-5 states:

a. [The organization:] Develops a plan of action and milestones for the information system to document the organizations planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

The Agency's EISRM *Security Planning (PL) Policy*, dated June 29, 2012 states:

(d) PRIVACY IMPACT ASSESSMENT (PL-5)

(1) Unless waived by the Executive Director, in accordance with privacy provisions of the E-Government Act of 2002, the Authorizing Official (i.e., the CTO or a designated representative thereof) SHALL ensure that:

(A) System Owners (or designated representatives thereof, e.g., Information System Security Officers) conduct:

(i) A Privacy Threshold Analysis (PTA) on all Information Systems to determine if those systems contain Personally Identifiable Information (PII) […]

11. To strengthen the security management program at the Maryland call center, the Agency should:

a. Ensure the contractor finalizes the A&A and ATO for the Maryland call center;

b. Enforce monitoring activities required of security personnel, including development and quarterly review of a Maryland call center POA&M for known weaknesses and vulnerabilities; and

c. Ensure the contractor performs a PTA for the Maryland call center.

By not completing the assessment and authorization process or a PTA for the Maryland call center, Agency management may not be aware of the security risks posed by the system, which places Agency systems at risk of inadvertent or deliberate disclosure, modification, or destruction of participant data.

Rules of Behavior Weakness at the Virginia Call Center

During our audit procedures, we noted that the Virginia call center's Rules of Behavior (ROBs) were not signed timely by all five Virginia call center PSRs selected for testing. Per Agency policy and contract requirements, PSRs are required to sign ROBs prior to obtaining access to Agency systems. Although the selected PSRs signed the ROBs, the signatures were not obtained until after our request for this documentation.

This condition occurred because of the lack of call center contract oversight by the Agency related to ROB compliance. Additionally, the Agency did not communicate the ROB requirement timely to the call centers.

The Agency's EISRM *Security Planning (PL) Policy*, dated June 29, 2012, states:

(c) RULES OF BEHAVIOR (PL-4)

(3) Information System Owners SHALL ensure that:

(A) BEFORE Users are granted access to an Information System the Rules of Behavior (RoB) are readily available to all users of that Information System and that,

(i) Information System Users have:

- Read the Rules of Behavior, and signed an "Acknowledgement and Acceptance" form agreeing to abide by the Rules of Behavior, and

- Submitted the signed form to the System Owner or a designated representative thereof. […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Planning (PL), Control PL-4 states:

Control: The organization:

a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior [*Assignment: organization-defined frequency*]; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

12. The Agency should develop, document, and implement monitoring procedures to ensure that individuals at the Virginia call center sign ROBs prior to obtaining access to Agency systems and that signed ROBs are properly maintained.

Granting system access to individuals prior to obtaining a signed ROB presents the possibility of inappropriate individuals obtaining access to Agency systems and data. These situations put Agency systems and data at risk of inadvertent or deliberate disclosure, modification, or destruction.

Media Sanitization and Disposal Weakness

Although surplused hard drives had been sanitized and removed from the Maryland call center, surplused workstation equipment and memory storage set aside for sanitization and disposal as requested on July 1, 2014 by the Maryland call center had not been disposed properly as of June 2015. The Agency uses ad hoc Government Services Administration bulk purchase agreements to select media and sanitization contractors; however, no regular procedures or schedule had been developed by the Agency for each call center because of a lack of call center oversight and technology asset management.

The Agency's EISRM *Media Protection (MP) Policy*, dated June 29, 2012, states:

> […] (e) MEDIA SANITIZATION AND DISPOSAL (MP-6)
>
> Before any Agency owned or management computing equipment is transferred, donated, "surplused," or otherwise disposed of, storage media associated with the equipment must be sanitized as described below. […]
>
> (1) Information System Owner Officers SHALL document in individual System Security Plans (SSPs), System-specific Rules of Behavior (RoB), and/or operational security (Op-Sec) procedures:
>
> (A) The system-specific media requiring Sanitization prior to disposal, and
>
> (B) The specific procedures required to sanitize and dispose of Information Systems media. […]

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Media Protection (MP), Control MP-6 states:

> Control: The organization:
>
> a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
>
> b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

13. To strengthen media sanitization procedures, the Agency should establish a contract for both call centers for the proper disposal of workstations and memory storage, including items previously identified for disposal.

Without timely contract procurement for media sanitization and disposal, the likelihood that media may become lost or misplaced increases the risk of inadvertent or deliberate disclosure of Agency systems and participant data.

RECOMMENDATIONS TO ADDRESS OTHER CONTROLS

Insufficient Documentation Supporting the TSP Website Calculators

We noted that the Agency did not have available documentation to support that the formulas used for TSP calculators on the TSP website were accurate. During our review of the configuration settings for the TSP calculators provided through the TSP website, we requested a copy of the formulas used on the website to perform the calculations. The Agency provided a formula for the Estimate Loan Payments calculator and reference guides for each of the following calculators:

- How Much Will My Savings Grow?
- Paycheck Estimator
- Retirement Income Calculator
- TSP Monthly Payment Calculator

Using the loan payment formula and the reference guides provided by the Agency, which were written in the perl language[13], we were unable to recalculate the results from the calculators on the TSP website in Microsoft Excel based on user inputs we selected. For the Retirement Income Calculator and the TSP Monthly Payment Calculator, the formula documented in the reference guide resulted in a "#NUM!" error. Test results of the other TSP website calculators noted above indicated differences between the TSP website results and our test results ranging from 9% to 96%, and in one case, no results were provided. The Agency informed us that because the reference guides were written in the perl language, they did not translate to Microsoft Excel for recalculation purposes. The Agency subsequently performed recalculations in Microsoft Excel; however, these recalculations were performed in response to our audit request and were not previously performed and documented.

The Agency's Microsoft Excel recalculations were not readily available as management deemed such documentation unnecessary because the calculations have not materially changed since the calculators were made public. The Agency indicated that the calculations would be revalidated at the time any material changes were made.

[13] Perl is a scripting language developed in the Linux environment initially designed to support data extraction and reporting capabilities for larger applications such as structured query language (SQL) and Microsoft Excel, among many others. Similar to Java, perl also supports websites by providing data extraction and reporting capabilities not available in native web language.

The GAO Standards states:

> Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

14. The Agency should maintain documentation to support that formulas used for the TSP calculators on the TSP website are accurate.

By not properly maintaining documentation to support formulas used for the TSP calculators on the TSP website, the Agency is unable to timely support the accuracy of those calculators should questions arise.

Congressional Inquiry Documentation Weaknesses

Supporting documentation was not provided for certain Congressional inquiries selected for testing. Specifically, we noted the following missing documentation in our sample:

- Two of 73 Congressional inquiries did not have documentation evidencing the detailed nature of the inquiry or sufficient support that such inquiries were received by telephone; and
- Two of 73 Congressional inquiries did not have responses to the inquiry.

The Agency did not have documented procedures requiring that all Congressional inquiries and responses be properly documented, maintained, and available for review upon request.

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* (Standards) states:

> Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

15. The Agency should update procedures over the Congressional inquiry process to include detailed procedures for documenting, maintaining, and having available all Congressional inquiries and responses, including inquiries received by telephone.

By not properly maintaining documentation related to Congressional inquiries and responses, the Agency is unable to accurately support that responses adequately address the Congressional inquiry and are provided to the Congressional party in a timely manner.

Congressional Inquiry Tracking Weaknesses

The Agency log, a tool used to track Congressional inquiries, was not accurately and timely updated to maintain its reliability. Specifically, we noted the following for a sample of Congressional inquiries in our scope period:

- Two of 26 inquiries did not have accurate dates in the Agency log;
- Three of 73 inquiries did not have an accurate inquiry nature documented in the Agency log;
- One of 73 inquiries was not accurately and timely updated in the Agency log at the time of receipt or closure; and
- Three of 73 inquiries did not have an accurate social security number/ account number for the participant account to which the inquiry was referring documented in the Agency log.

This condition exists because of the lack of Agency management review over the Agency log and the Congressional file, which includes the actual Congressional inquiry and related correspondence.

The GAO Standards states:

> Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.

16. The Agency should update policies and procedures over the Congressional inquiry process to include detailed procedures for reviewing the Agency log and Congressional file on a periodic basis.

The lack of a periodic review of the Agency log and Congressional file increases the risk that Congressional inquiries will not be tracked properly and answered in a timely and accurate manner.

Weaknesses in the Documentation of the Agency's Policies and Procedures

We noted that the Agency had not developed and implemented written policies and procedures related to:

- The review of the Monthly Congressional Correspondence Summary, including the required steps to be taken when further investigation is deemed necessary;
- The generation and distribution of participant account statements;
- The generation, distribution, and correction of improperly-generated rejection and confirmation notices;
- The process for identifying a need to update the information provided on the TSP website (e.g., booklets, leaflets, and frequently asked questions); and
- The process for updating the information provided on the TSP website (e.g., booklets, leaflets, and frequently asked questions).

Because the Agency's staff size is not large and the turnover rate is fairly low, management had determined that formalizing such policies and procedures in an official written document was not the most efficient use of their resources.

The GAO Standards states:

> Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

17. The Agency should:

a. Update policies and procedures over the Congressional inquiry process to include detailed procedures for performing the review of the Monthly Congressional Correspondence Summary;

b. Develop, document, and implement policies and procedures for the generation and distribution of quarterly and annual participant account statements;

c. Develop, document, and implement policies and procedures for the generation, distribution, and correction of improperly-generated rejection and confirmation notices; and

d. Develop, document, and implement policies and procedures for identifying needs to update the information provided on the TSP website timely.

Without sufficiently documented policies and procedures in place, the Agency may not be able to execute existing processes or properly train new employees in the event that current employees suddenly vacate their positions. Additionally, the Agency may not provide Congress and participants with appropriate and timely information.

D. Summary of Open Recommendations

2009 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Call Center Technology Weaknesses Should Be Addressed

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.

Information Privacy Requirements Should Be Enforced at the Call Centers

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

2012 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Additional Logical Access Control Weaknesses at the Call Centers

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.

Weaknesses in Call Center Configuration Management Controls

4. To strengthen configuration management controls at the call centers, the Agency should:
   b. Upgrade its TSP supporting systems at the call centers to vendor-supported software versions.

Weaknesses in Call Center Controls for Media Handling and Disposal

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

2015 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Control Weaknesses in Administering Logical Access to Agency Systems

1. The Agency should enforce the existing EISRM policies that require:
   a. Users to obtain appropriate Agency and call center management approval prior to obtaining system access;
   b. Disabling of user accounts that exceed Agency-established periods of inactivity; and
   c. Timely removal of user access to Agency systems when employees and contractors are terminated or transfer job functions.

Weaknesses in the Call Center Access Recertification Process

2. The Agency should:

a. Develop, document, and implement recertification procedures for systems that support the Virginia and Maryland call centers, including Agency-managed systems and call center-managed systems; and
b. Develop, document, and implement monitoring procedures to ensure Agency and call center compliance with Agency recertification requirements.

Weakness in Restricting Internet Access at the Maryland Call Center

3. To strengthen security controls, the Agency should develop, document, and implement monitoring procedures to ensure that Maryland call center management periodically reviews the internet whitelist and removes all unnecessary internet sites.

Versadial Password Weaknesses at the Virginia Call Center

4. To address password weaknesses at the Virginia call center, the Agency should require that Virginia call center management upgrade Versadial to a version that includes minimum password length controls, or document the acceptance of this risk and compensating controls in appropriate security documentation.

Call Center Physical Access Control Weaknesses

5. To strengthen call center physical access controls, the Agency should:
   a. Develop, document, and implement monitoring procedures to enforce EISRM policies that require pre-approval for physical access to secured areas of the call center facility; and
   b. Develop, document, and implement monitoring procedures to ensure that call center management periodically reviews data center and server room access at the Maryland and Virginia call centers, respectively.

Call Center Configuration and Patch Management Weaknesses

6. The Agency should:
   a. Develop, document, and implement monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely and in accordance with Agency policy;
   b. Develop, document, and implement monitoring procedures for the Maryland call center to ensure that call center management documents and tracks vulnerabilities

and to ensure that vulnerabilities are identified and remediated timely and in accordance with Agency policy;

c. Define procedures and modify call center contract language, as necessary, to clearly delineate responsibilities for oversight and enforcement of Agency information security requirements at non-Agency facilities specific to vulnerability management; and

d. Provide workstation images or Agency-defined baseline configurations to each call center and periodically monitor workstation compliance with USGCB settings.

Call Center Contract Oversight Weaknesses

7. The Agency should complete the following activities related to call center contract oversight and management:

   a. Formalize and document call center contract oversight management procedures and responsible parties to ensure each appropriate Agency office understands its contract oversight roles and responsibilities;

   b. Review and modify each call center contract, as needed, to ensure that all call center contract clauses are relevant, specific, and applicable to each call center environment and clearly delineate responsibilities for Agency and contractor-managed sites;

   c. Ensure timely coordination with the contracting officer for any subsequent changes to the call center contracts; and

   d. Develop, document, and implement procedures to enforce contract compliance with required reporting metrics.

Encryption Weaknesses on Local Versadial Data Storage

8. The Agency should identify and implement a solution to encrypt the Versadial data and servers that contain PII and are physically located at each call center.

Encryption Weaknesses on Maryland Call Center Workstations

9. The Agency should work with Maryland call center management to identify and implement a solution to encrypt data retained on PSR workstations used for handling participant data.

Weaknesses in the Virginia Call Center Security Management Program

10. To strengthen the security management program at the Virginia call center, the Agency should:
    a. Update the Virginia call center SSP to comply with NIST SP 800-53, Rev. 4;
    b. Document all minimum system security controls as required by NIST for moderate systems in the Virginia call center SSP;
    c. Enforce monitoring activities required of security personnel, including quarterly review and update of the POA&M and assessment of compliance with ATO limitations for the Virginia call center; and
    d. Complete a PIA for the Virginia call center.

Weaknesses in the Maryland Call Center Security Management Program

11. To strengthen the security management program at the Maryland call center, the Agency should:
    a. Ensure the contractor finalizes the A&A and ATO for the Maryland call center;
    b. Enforce monitoring activities required of security personnel, including development and quarterly review of a Maryland call center POA&M for known weaknesses and vulnerabilities; and
    c. Ensure the contractor performs a PTA for the Maryland call center.

Rules of Behavior Weakness at the Virginia Call Center

12. The Agency should develop, document, and implement monitoring procedures to ensure that individuals at the Virginia call center sign ROBs prior to obtaining access to Agency systems and that signed ROBs are properly maintained.

Media Sanitization and Disposal Weakness

13. To strengthen media sanitization procedures, the Agency should establish a contract for both call centers for the proper disposal of workstations and memory storage, including items previously identified for disposal.

RECOMMENDATIONS TO ADDRESS OTHER CONTROLS

Insufficient Documentation Supporting the TSP Website Calculators

14. The Agency should maintain documentation to support that formulas used for the TSP calculators on the TSP website are accurate.

Congressional Inquiry Documentation Weaknesses

15. The Agency should update procedures over the Congressional inquiry process to include detailed procedures for documenting, maintaining, and having available all Congressional inquiries and responses, including inquiries received by telephone.

Congressional Inquiry Tracking Weaknesses

16. The Agency should update policies and procedures over the Congressional inquiry process to include detailed procedures for reviewing the Agency log and the Congressional file on a periodic basis.

Weaknesses in the Documentation of the Agency's Policies and Procedures

17. The Agency should
    a. Update policies and procedures over the Congressional inquiry process to include detailed procedures for performing the review of the Monthly Congressional Correspondence Summary;
    b. Develop, document, and implement policies and procedures for the generation and distribution of quarterly and annual participant account statements;
    c. Develop, document, and implement policies and procedures for the generation, distribution, and correction of improperly-generated rejection and confirmation notices; and
    d. Develop, document, and implement policies and procedures for identifying needs to update the information provided on the TSP website timely.

AGENCY'S RESPONSE

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

June 15, 2016

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 May 16, 2016, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan Participant Support Operations, dated May 2016. 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,

for Ravindra Deo
Gregory T. Long

Enclosure

2009 RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2009 – 4 Call Center Technology Weaknesses Should Be Addressed:

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 unique user IDs and passwords for individuals performing administrative duties over Versadial are established.

Response:

a) The Agency concurs with this recommendation. The Agency also concurs with the noted condition that the 2005-2013 Versadial recordings on DVD/external hard drives remain offsite and unencrypted. As a compensating control the Agency has followed EISRM policy to ensure that the recordings are "protected by alternative physical measures" specifically that they are stored in the Wells Fargo safety deposit box. Thus, the risk of loss in the Agency's opinion currently low. The Agency will be implementing a plan to transfer and store the data which will include data encryption. This project should be completed by November 30, 2016.

2009 – 7 Information Privacy Requirements Should Be Enforced at the Call Centers:

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

Response:

While the Agency concurs with the original recommendation, it does not concur with the noted condition which results in the status of the recommendation remaining open. The two identified Maryland-call center individuals were hired (10/14/14 & 2/9/15) which was after the date of annual training (6/30/14). While new hires receive privacy act training during the first couple of days on the job, the Agency had no requirement for new hires to sign a certificate of completion verifying that this occurred. Thus, the Agency properly enforced the call center requirements for maintaining adequate evidence of privacy training in effect at the time. The two Maryland employees completed the 2015 annual training and signed the certificate of completion prior to the Agency deadline of 7/31/2015). The Agency considers this recommendation closed.

Effective for new hires after July 31, 2015, we have strengthened this process and the Agency now requires Privacy Act training be completed within 60 days and that a certificate of completion be signed and provided to the COR. Further, beginning February 2016, the Privacy Act training is accessible and completed using the Agency's Enterprise Learning Management System (ELMS) to monitor compliance for this training.

2012 RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2012 – 1 Additional Logical Access Control Weaknesses at the Call Centers:

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:

a) The Agency concurs with this recommendation. In response to the 2015 finding, the six (6) websites reported on the whitelist were removed. The Agency will develop, document, and implement monitoring procedures to ensure that call center management periodically reviews the internet whitelist and removes all unnecessary internet sites. This task will be completed by August 1, 2016.

b) The Agency concurs with this recommendation. The Agency will develop and implement alternative procedures to maintain documentation support the approval of network access for all individuals with such access. This task will be complete by November 30, 2016.

2012 – 4 Weaknesses in Call Center Configuration Management Controls:

4. To strengthen configuration management controls at the call centers, the Agency should:
   b. Upgrade its TSP supporting systems at the call centers to vendor-supported software versions.

Response:

b) The Agency concurs with this recommendation. The Agency concurs that it needs to upgrade its TSP supporting systems at the call centers to vendor-supported software versions. The Agency is developing a plan to review and potentially replace/upgrade unsupported components of our telecommunications infrastructure. The Agency expects to have a completed plan by August 1, 2016.

2012 - 8 Weaknesses in Call Center Controls for Media Handling and Disposal:

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

Response:

The Agency concurs with this recommendation. The Agency is in the process of awarding a multi-year/multi-site asset disposal contract. The call center sites are included in this contract. The Agency believes that this contract in addition to the noted Agency level policy and procedures which were developed and implemented are sufficient to address this recommendation. This will be in place by November 30, 2016.

2015 RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2015-1 - Control Weaknesses in Administering PSR Logical Access to Agency Systems

1. The Agency should enforce the existing EISRM policies that require:

- **a. Users to obtain appropriate Agency and call center management approval prior to obtaining system access;**
- **b. Disabling of user accounts that exceed Agency-established periods of inactivity; and**
- **c. Timely removal of user access to Agency systems when employees and contractors are terminated or transfer job functions.**

Response:

a. The Agency concurs with this recommendation. The Agency will enforce existing EISRM policies that require users to obtain appropriate Agency and call center management approval prior to obtaining system access. The Agency will develop and implement processes and procedures to ensure this issue is remediated by September 30, 2016.

b. The Agency concurs with this recommendation. The Agency will enforce existing EISRM policies that require the disabling of user accounts that exceed Agency-established periods of inactivity. The Agency will develop and implement processes and procedures to ensure this issue is remediated by September 30, 2016.

c. The Agency concurs with this recommendation. The Agency will enforce existing EISRM policies that require the timely removal of user access to Agency systems when employees and contractors are terminated or transfer job functions. The Agency will develop and implement processes and procedures to ensure this issue is remediated by September 30, 2016.

2015 – 2 Weaknesses in the Call Center Access Recertification Process

2. The Agency should:

a. Develop, document, and implement recertification procedures for systems that support the Virginia and Maryland call centers, including Agency-managed systems and call center-managed systems; and

b. Develop, document, and implement monitoring procedures to ensure Agency and call center compliance with Agency recertification requirements.

Response:

a. The Agency concurs with this recommendation. To remediate the issue the Agency will enhance, document, and implement recertification procedures for system that support the Virginia and Maryland call centers, including Agency-managed systems and call center-managed systems. The Agency will complete this task by August 1, 2016.

b. The Agency concurs with this recommendation. To remediate the issue the Agency will develop, document, and implement monitoring procedures to ensure Agency and call center compliance with Agency recertification requirements. The Agency will complete this task by August 1, 2016.

2015 – 3 Weakness in Restricting Internet Access at the Maryland Call Center

To strengthen security controls, the Agency should develop, document, and implement monitoring procedures to ensure that call center management periodically reviews the internet whitelist and removes all unnecessary internet sites.

Response:

The Agency concurs with this recommendation. The Agency will develop, document, and implement monitoring procedures to ensure that call center management periodically reviews the internet whitelist and removes all unnecessary internet sites. This task will be completed by August 1, 2016.

2015 – 4 Versadial Password Weaknesses at the Virginia Call Center

To address password weaknesses at the Virginia call center, the Agency should require that Virginia call center management upgrade Versadial to a version that includes minimum password length controls, or document the acceptance of this risk and compensating controls in appropriate security documentation; and

Response:

The Agency concurs with the recommendation and now considers it to be closed. Since the audit field work the Agency has confirmed that Versadial has been upgraded to now include the requisite password parameters as of September 9, 2015 at the Virginia call center. Versadial now requires unique ID and password parameters of 12 characters or more, and change every 30 days.

2015 – 5 Call Center Physical Access Control Weaknesses

To strengthen call center physical access controls, the Agency should:

a. **Develop, document, and implement monitoring procedures to enforce EISRM policies that require pre-approval for physical access to secured areas of the call center facility; and**

b. **Develop, document, and implement monitoring procedures to ensure that call center management periodically reviews data center and server room access at the Maryland and Virginia call centers, respectively.**

Response:

a. The Agency concurs with the recommendation. The Agency will ensure the development, documentation, and implementation of monitoring procedures to ensure that EISRM policies requiring physical access approval prior to obtaining access to secure areas of the facility are enforced. Physical access to the respective data center and server rooms currently requires electronic identification cards coded for access. The Agency expects to have these procedures in place by August 1, 2016.

b. The Agency concurs with the recommendation. The Agency will develop, document, and implement monitoring procedures to ensure that call center management periodically reviews respective data center and server room access at the call centers. The Agency expects to have these procedures in place by August 1, 2016.

2015 – 6 Call Center Configuration and Patch Management Weaknesses

The Agency should:

a. **Develop, document, and implement monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely and in accordance with Agency policy;**

b. **Develop, document, and implement monitoring procedures for the Maryland call center to ensure that call center management documents and tracks vulnerabilities and to ensure that vulnerabilities are identified and remediated timely and in accordance with Agency policy;**

c. **Define procedures and modify call center contract language, as necessary, to clearly delineate responsibilities for oversight and enforcement of Agency information security requirements at non-Agency facilities specific to vulnerability management;**

d. **Provide workstation images or Agency-defined baseline configurations to each call center and periodically monitor workstation compliance with USGCB settings.**

Response:

a. The Agency concurs with this recommendation. The Agency currently performs vulnerability scans on servers at the Virginia call center and has an active POA&M list to remediate identified vulnerabilities. The Agency will develop, document, and implement monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely and in accordance with Agency policy. The Agency will complete this task by September 30, 2016.

b. The Agency concurs with this recommendation. The Agency currently performs vulnerability scans on servers at the Maryland call center and has an active POAM list to remediate identified vulnerabilities. The Agency will develop, document, and implement monitoring procedures for the Maryland call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely and in accordance with Agency policy. The Agency will complete this task upon completion of the Maryland call center A&A and ATO no later than August 1, 2016.

c. The Agency concurs with this recommendation. The Agency will establish contract reviews between the Program Office Deputy and COR and make sure the COR understands the contract, deliverables, and terms/conditions. The COR will establish a line of communications with all Agency contract clause owners. The COR will have a contract deliverable matrix added to the contact to assure both contractor and COR understand the required deliverables on the contract. The Agency will complete this task by October 31, 2016.

d. The Agency concurs with this recommendation. The Agency will deliver a plan to develop an FRTIB workstation standard compliant with USGCB settings by August 31, 2016.

2015 - 7 Call Center Contract Oversight Weaknesses

The Agency should complete the following activities related to call center contract oversight and management:

- **a. Formalize and document call center contract oversight management procedures and responsible parties to ensure each appropriate Agency office understands its contract oversight roles and responsibilities;**
- **b. Review and modify each call center contract, as needed, to ensure that all call center contract clauses are relevant, specific, and applicable to each call center environment and clearly delineate responsibilities for Agency and contractor-managed sites;**
- **c. Ensure timely coordination with the contracting officer for any subsequent changes to the call center contracts; and**
- **d. Develop, document, and implement procedures to enforce contract compliance with required reporting metrics.**

Response:

a. The Agency concurs with this recommendation. The Agency has documented contract oversight procedures which will be strengthened in response to this recommendation. The Agency currently follows the Procurement Policy, Guidelines, and Procedures Manual (Directive 12A) and the Contracting Policy, which define and explain COR duties and responsibilities. COs, CORs, and their supervisors sign COR nomination and designation forms to ensure CORs are properly trained and certified prior to performing COR duties. OPOP, OTS, and OCFO will create a matrix of day-to-day roles and responsibilities for the Call Center contracts by October 31, 2016. The Agency is currently creating Contracting Procedures that explain Agency COR duties and responsibilities in greater detail than the current Directive and Policy. The Agency will complete this task by December 31, 2016.

b. The Agency concurs with the recommendation. The call center CORs and Agency clause owners will review the contracts to confirm that all call center clauses are relevant and applicable to each call center environment. The CO will sign a memorandum stating that they, the COR, and the clause owners have reviewed the call center clauses and they are relevant and applicable to each call center environment. If it is determined that clauses are not relevant

or applicable, the COR will work with the CO to modify the contracts. The Agency will complete this task by October 31, 2016.

c. The Agency concurs with this recommendation. The Agency has documented contract oversight procedures which will be strengthened in response to this recommendation. The Agency currently follows the Procurement Policy, Guidelines, and Procedures Manual (Directive 12A) and the Contracting Policy, which define and explain COR duties and responsibilities. COs, CORs, and their supervisors sign COR nomination and designation forms to ensure CORs are properly trained and certified prior to performing COR duties. OPOP, OTS, and OCFO will create a matrix of day-to-day roles and responsibilities for the Call Center contracts by October 31, 2016. The Agency is currently creating Contracting Procedures that explain Agency COR duties and responsibilities in greater detail than the current Directive and Policy. The Agency will complete this task by December 31, 2016.

d. The Agency concurs with the recommendation. The COR will clarify which metrics are relevant, and will work with the CO on modifying the contracts, as needed. The Agency will complete this task by October 31, 2016.

2015 - 8 Encryption Weaknesses on Local Versadial Data Storage

The Agency should identify and implement a solution to encrypt the Versadial data and servers, including PII, physically located at each call center.

Response:

The Agency concurs with the recommendation. Although the Agency has looked at ways in which we can secure the current Versadial solution, the Agency has not determined a way to encrypt the data in the current Versadial. In planning a new acquisition (ExPRESS), the Agency will address the need to encrypt the Versadial data and servers. In the meantime, we will initiate a study to determine if there are intermediate steps that the Agency can take prior to ExPRESS to achieve the encryption standard cited in the finding and recommendation. The Agency will complete this study by August 31, 2016.

As a compensating control the Agency has followed EISRM policy to ensure that the recordings are "protected by alternative physical measures" specifically that they are located within secure facilities which require physical access credentials.

2015 - 9 Encryption Weaknesses on Maryland Call Center Workstations

The Agency should work with Maryland call center management to identify and implement a solution to encrypt data retained on PSR workstations used for handling participant data.

Response:

The Agency concurs with the recommendation. The Agency has already begun to work with the Maryland call center management to identify and implement a solution (e.g. BitLocker) to encrypt data retained on PSR workstations used for handling participant data. The Agency will complete this action by August 1, 2016.

2015 - 10 Weaknesses in the Virginia Call Center Security Management Program

To strengthen the security management program at the Virginia call center, the Agency should:

- **a. Update the Virginia call center SSP to comply with NIST SP 800-53, Rev. 4;**
- **b. Document all minimum system security controls as required by NIST for moderate systems in the Virginia call center SSP;**
- **c. Enforce monitoring activities required of security personnel, including quarterly review and update of the POA&M and assessment of compliance with ATO requirements for the Virginia call center; and**
- **d. Complete a PIA for the Virginia call center.**

Response:

a. The Agency does not concur with the recommendation. The Agency created the Virginia call center SSP which complies with NIST SP 800-53, Rev. 4 as of November 24, 2014.

b. The Agency does not concur with the recommendation. The Agency has documented all minimum system security controls as required by NIST for moderate systems in the Virginia call center SSP. This is documented in the Virginia call center SSP as of November 24, 2014.

c. The Agency concurs with the recommendation. The Agency concurs that the documentation of these reviews was not captured in the POA&M document itself. However, email artifacts detailing monthly vulnerability reports were sent to the Virginia Call Center as well as POA&M review requests. This activity began shortly after the Virginia call center received its ATO (11/20/2014). The Agency will enforce monitoring activities required of security personnel, including quarterly review and update of the POA&M and assessment of compliance with ATO requirements for the Virginia call center by September 30, 2016.

d. The Agency considers this recommendation closed, as the Senior Agency Official for Privacy (SAOP) signed the PIA for the Clintwood Call Center on March 17, 2016.

2015 - 11 Weaknesses in the Maryland Call Center Security Management Program

To strengthen the security management program at the Maryland call center, the Agency should:

a. Ensure the contractor finalizes the A&A and ATO for the Maryland call center;

b. Enforce monitoring activities required of security personnel, including development and quarterly review of a Maryland call center POA&M for known weaknesses and vulnerabilities; and

c. Ensure the contractor performs a PTA for the Maryland call center.

Response:

a. The Agency concurs with the recommendation. The Agency will ensure that Maryland call center management finalizes the A&A and ATO by August 1, 2016.

b. The Agency concurs with the recommendation. The Agency will enforce monitoring activities required of security personnel including development and quarterly review of a Maryland call center POA&M for known weaknesses and vulnerabilities. The Agency will implement this monitoring activity by January 31, 2017.

c. The Agency concurs with the recommendation. The Agency will ensure that Maryland call center management finalizes the PTA by August 1, 2016.

2015 - 12 Rules of Behavior Weakness at the Virginia Call Center

The Agency should develop, document, and implement monitoring procedures to ensure that individuals at the Virginia call center sign ROBs prior to obtaining access to Agency systems and that signed ROBs are properly maintained.

Response:

The Agency concurs with the recommendation and now considers it to be closed. Since the audit field work occurred, the Agency has developed, documented, and implemented monitoring procedures to ensure that individuals at the Virginia call center sign ROBs prior to obtaining access to Agency systems and that signed ROBs are properly maintained. This corrective action was implemented as of July 2015.

2015 – 13 Media Sanitization and Disposal

To strengthen media sanitization procedures, the Agency should establish a contract for both call centers for the proper disposal of workstations and memory storage, including items previously identified for disposal.

Response:

The Agency concurs with the recommendation. The Agency is in the process of awarding a multi-year/multi-site asset disposal contract. The call center sites are included in this contract. This will be in place by November 30, 2016.

RECOMMENDATIONS TO ADDRESS OTHER CONTROLS

2015 – 14 Insufficient Documentation Supporting the TSP Website Calculators

The Agency should maintain documentation to support that formulas used for the TSP calculators on the TSP website are accurate.

Response:

The Agency concurs with this recommendation. The Agency will maintain documentation consisting of the formulas used to verify the accuracy of TSP calculators on the TSP website, and document any additional formulas by October 31, 2016.

2015 – 15 Congressional Inquiry Documentation Weaknesses

The Agency should update procedures over the Congressional inquiry process to include detailed procedures for documenting, maintaining, and having available all Congressional inquiries and responses, including inquiries received by phone.

Response:

The Agency does not concur with the finding (condition described) but does concur with the recommendation. The Agency provided information regarding the cases noted above. In all cases, the method of inquiry was noted in the file; similarly, in all cases, responses were in the file. However, as to the need for a policy and procedures, OEA issued a Congressional Correspondence policy on November 12, 2014 and a Congressional Correspondence procedure on May 30, 2015.

2015 – 16 Congressional Inquiry Tracking Weaknesses

The Agency should update policies and procedures over the Congressional inquiry process to include detailed procedures for reviewing the Agency log and the Congressional file on a periodic basis.

Response:

The Agency concurs with the finding but does not concur with the recommendation. While there were errors in the documentation, the errors did not impact the Agency staff's ability to track these cases or locate them in Agency records. In addition, none of the errors caused any impact to the level of service provided to Congressional offices on behalf of TSP participants, all of whom received timely responses from OEA.

2015 – 17 Weaknesses in the Documentation of the Agency's Policies and Procedures

The Agency should:

- **a. Update policies and procedures over the Congressional inquiry process to include detailed procedures for performing the review of the Monthly Congressional Correspondence Summary;**
- **b. Develop, document, and implement policies and procedures for the generation and distribution of quarterly and annual participant account statements;**
- **c. Develop, document, and implement policies and procedures for the generation, distribution, and correction of improperly-generated rejection and confirmation notices;**
- **d. Develop, document, and implement policies and procedures for identifying needs to update the information provided on the TSP website timely; and**

Response:

a. The Agency concurs with this recommendation. The Office of External Affairs issued a Congressional Correspondence policy on November 12, 2014 and a Congressional Correspondence procedure on May 30, 2015. The Agency considers this finding to be closed.

b. The Agency concurs with this recommendation. The Agency is currently working with a contracted consultant to assist in the documentation of its participant statement procedures. The Agency will have these procedures in place by October 31, 2016.

c. The Agency concurs with this recommendation. The Agency is currently working with a contracted consultant to assist in the documentation of its notices procedures. The Agency will have these procedures in place by October 31, 2016.

d. The Agency concurs with this recommendation. The Agency is currently working with a contracted consultant to assist in the documentation of its website content update procedures. The Agency will have these procedures in place by October 31, 2016.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

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

- Written Inquiry Quality Control Reports for the months of January 2014, October 2014, and February 2015
- Report of all Congressional Inquiries for the time period of January 1, 2014 through March 31, 2015
- *Summary of Thrift Savings Plan* dated May 2012
- *TSP In Service Withdrawals* dated May 2012
- TSP Payroll and Personnel Agency Representative meeting agendas for the quarters dated March 2014, September 2014, and March 2015
- Report No. TSP 6009, *Master Participant Notices Generated Summary Report*, for the period of January 1, 2014 through December 31, 2014
- Report No. TSP 6009, *Master Participant Notices Generated Summary Report*, for the period of January 1, 2015 through March 31, 2015
- Report No. TSP 6017, *Participating Employees by Department*, for calendar year 2014
- Report No. TSP 6019, *Returned Mail Summary Report*, for calendar year 2014
- Software Change Request (SCR) No. 001298, Statements – Accommodate new retirement codes mandated by OPM
- SCR No. 001330, 2014 Q2 Participant Support Enhancements
- SCR No. 001331, 2014 Q2 Participant Support Enhancements
- SCR No. 001453, Report of Suppressed Annual and Quarterly Statements Due to Bad Address
- SCR No. 001781, 2014 Q4 Participant Statement Enhancement
- SCR No. 001782, 2014 Q4 Participant Statement Enhancement
- SCR No. 001783, 2014 Annual Participant Statement Enhancements
- SCR No. 001784, 2014 Annual Participant Statement Enhancements
- The Enterprise Information Security and Risk Management (EISRM) Program Personnel Security Policy, dated June 26, 2012
- EISRM Identification and Authentication Policy, dated June 29, 2012
- EISRM Media Protection Policy, dated June 8, 2012
- EISRM Limited Personal Use Policy, dated August 8, 2012
- EISRM System and Communications Protection Policy, dated June 29, 2012
- EISRM Access Control Policy, dated June 29, 2012

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- Draft Identity and Access Management SOP, dated February 25, 2014
- PSR User Listing for both call centers, dated June 29, 2015
- SunGard EXP AG User Listing for both call centers, dated June 29, 2015
- PSR Security Matrix, dated March 7, 2014
- Access Recertification Spreadsheet, dated July 16, 2014
- PSR Group Descriptions, dated February 10, 2015
- Information Assurance Division (IAD) IT Security Media Destruction or Sanitation Procedures, dated July 1, 2014
- AT&T Call Load Distribution Procedures, dated November 11, 2011
- 2014 Call Distribution Change Log for the period January 1, 2014 – December 31, 2014
- 2015 Call Distribution Change Log for the period January 1, 2015 – March 31, 2015
- Call Center Quality Assurance Plan, dated December 2010
- Minutes of the April 20, 2015, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov

Virginia Call Center Documents and Reports

- Virginia Call Center-TIB-2007-C-002 P00011
- Virginia Call Center Employee Listing, for the period January 1, 2014 – March 31, 2015
- Virginia Call Center Standard Operating Procedures (SOP), dated August 22, 2014
- Virginia Call Center Internet Blacklist, dated May 28, 2015
- Virginia Call Center Internet Whitelist, dated May 28, 2015
- Virginia Call Center Call Center LAN Settings, dated June 29, 2015
- Virginia Call Center Sophos Encryption Settings, dated June 10, 2015
- LAN User Listing for Virginia Call Center, dated June 29, 2015
- Virginia Call Center Organization Chart, dated June 29, 2015
- Virginia Call Center LAN Access Approvals, dated October 21, 2015
- Virginia Call Center Logical Access Approval Email, dated December 5, 2014
- Virginia Call Center Server Room Access Listing, dated June 23, 2015
- Virginia Call Center Clean Desk Policy, dated June 27, 2014
- Virginia Call Center Versadial Backup Script, dated November 5, 2013
- Virginia Call Center Quality Reports for March 2014, November 2014, and January 2015

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

Maryland Call Center Documents and Reports

- Maryland Call Center Employee Listing, for the period January 1, 2014 – March 31, 2015
- Maryland Call Center-TIB-2008-C-001 P00010
- Maryland Call Center New Hire Procedures & BI, dated August 6, 2013
- Maryland Call Center Termination & Transfer Procedures, dated March 12, 2015
- Maryland Call Center Workstation Group Policy Object, dated May 19, 2015
- Maryland Call Center Internet Blacklist, dated May 19, 2015
- Maryland Call Center Internet Whitelist, dated May 19, 2015
- LAN User Listing for Maryland Call Center, dated June 29, 2015
- Call Center Backup Configuration Settings, dated September 1, 2015
- Maryland Call Center Organization Chart, dated June 15, 2015
- Maryland Call Center SOP Section 13 Security, dated March 12, 2012
- Maryland Call Center Data Center Access Double Door Listing, dated May 19, 2015
- Maryland Call Center Data Center Access Single Door Listing, dated May 19, 2015
- Maryland Call Center Data Center March 2015 Access Review, dated May 19, 2015
- Electronic Sanitization Request Form, dated July 1, 2014
- Maryland Call Center HDD Destruction Certificate, dated May 21, 2015
- Maryland Call Center Call Center Versadial Backup Settings, dated August 6, 2015
- Maryland Call Center Training Procedures, Section 10. New Hire Orientation Procedure
- Maryland Call Center Quality Reports for March 2014, November 2014, and January 2015