Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Participant Support Operations

May 4, 2017

TABLE OF CONTENTS

Section Page

Appendices

EXECUTIVE SUMMARY

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

Michael Auerbach
Acting Chief Accountant
U.S. Department of Labor, Employee Benefits Security Administration
Washington, DC

As a part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit of the Thrift Savings Plan (TSP) participant support process. We performed our fieldwork from November 30, 2016 through February 17, 2017, primarily at the Federal Retirement Thrift Investment Board's Staff (Agency) in Washington, DC, and at the two TSP call centers located in Virginia and Maryland. Our scope period for testing was January 1, 2016 through December 31, 2016.

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 engagement are defined in 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 whether 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; (6) enforce physical and logical access controls at the call centers; (7) enforce caller authentication and privacy controls at the call centers; and (8) monitor the call centers' contractors to ensure they are in compliance with the terms of the contracts.

- Test compliance of the TSP participant support process with 5 USC 8439(c) and 5 CFR 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 the Thrift Savings Plan Participant Support Operations,* dated June 15, 2016.

We present six new recommendations, all of which address fundamental controls. Fundamental control recommendations address significant[1] 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, 2016 through December 31, 2016, 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

[1] *Government Auditing Standards* section 6.04 defines significance in the context of a performance audit.

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; (6) enforce physical and logical access controls at the call centers; (7) enforce caller authentication and privacy controls at the call centers; and (8) monitor the call centers' contractors to ensure they are in compliance with the terms of the contracts. As a result of our compliance testing, we did not identify any instances of noncompliance with 5 USC 8439(c) or Agency Regulations. However, as noted above, we noted internal control weaknesses in certain areas of the TSP participant support process.

We also reviewed 22 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, five recommendations have been implemented and closed, three recommendations have not been implemented or have been partially implemented but are considered closed, nine recommendations have been partially implemented and remain open, and five recommendations have not been implemented and remain open.

The Agency's responses to the recommendations, including the Executive Director's formal reply, are included as an appendix within the report (Appendix A). The Agency concurred or partially concurred with all recommendations; the two partial concurrences are discussed below:

Recommendation Number	Auditors' Response
2015-16	Management concurred with the recommendation to update policies and procedures to include review of the Congressional Correspondence Summary but indicated that they do not consider it cost-beneficial to document review of the control log for Congressional inquiries. EBSA will assess the corrective actions implemented by management over Congressional inquiries during the next performance audit covering this subject matter.
2016-02	Management concurred with the recommendation to enhance data sanitization and disposal procedures at the Maryland call center; however, the Agency considers this process to be primarily the responsibility of the call center. As such, management's response did not fully address our recommendation related to Agency monitoring procedures over the call centers' sanitization and

Recommendation Number	Auditors’ Response
	disposal process. Effective monitoring controls are critical to ensuring that processes at the call centers are operating effectively. 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 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

May 4, 2017

I. BACKGROUND OF THE TSP AND PARTICIPANT SUPPORT OPERATIONS

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act of 1986 (FERSA), as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS) and provides a Federal (and, in certain cases, state) income tax deferral on employee contributions and related earnings. The TSP is available to federal and Postal employees, members of Congress and certain Congressional employees, and members of the uniformed services. The TSP began accepting contributions on April 1, 1987, and as of December 31, 2016, had approximately $495 billion in assets and approximately 5 million participants.[2]

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[3]

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:

[2] Source: Minutes of the January 23, 2017 Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

[3] Sources: Virginia Call Center Standard Operating Procedure (SOP), dated December 19, 2016 and Maryland Call Center SOP, dated October 6, 2016.

- Inform all eligible employees/members of TSP options and benefits;
- Maintain adequate supplies of participant TSP election forms (if used by the employer)[4], booklets, and publications to facilitate participation;
- Determine retirement coverage;
- Provide and collect TSP election forms (Form TSP-1 or Form TSP-U-1);
- 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, secure messaging (e-messages), and telephone. The Agency works with the call centers to coordinate information needed to answer participants' inquiries.

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

Once the assigned correspondence agent begins work on the correspondence, he or she is responsible for resolving the inquiry and responding to the participant, either via a phone call or

[4] 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.

letter. The correspondence agency 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.

TSP participants can also submit inquiries via secure messaging through the TSP website. Secure messages, referred to as e-messages, are received at the Maryland call center. The Maryland call center uses the Moxie system to manage and respond to e-messages. When a message is received, Moxie automatically sends a reply to the participant stating that the message has been received and the participant will receive a response within 24 hours. When a new message comes in, it is automatically added into the Moxie inbox and addressed in a first-in, first-out manner. When an e-messaging representative becomes available, he or she is assigned the next available message from the inbox. The representative may put a response on hold if he or she is unable to provide an answer to the inquiry and needs to escalate the request, or has to perform additional research. Putting the message on hold prompts an automated message to the participant stating that the question is under review and a response will be provided shortly.

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. Congressional inquiries are received by the Office of External Affairs (OEA). The OEA Director or staff logs these inquiries in a similar manner as regular correspondence. While most of the correspondence is addressed by the Office of External Affairs, the Office of Participant Operations and Policy or Office of General Counsel may assist with research and resolving issues or drafting the letters, as needed.

During calendar year 2016, the TSP processed approximately 2.3 million TSP participant telephone inquiries, approximately 93,500 written inquiries[5], and approximately 59,000 e-messages[6]. The TSP most frequently processes inquiries regarding withdrawal information.

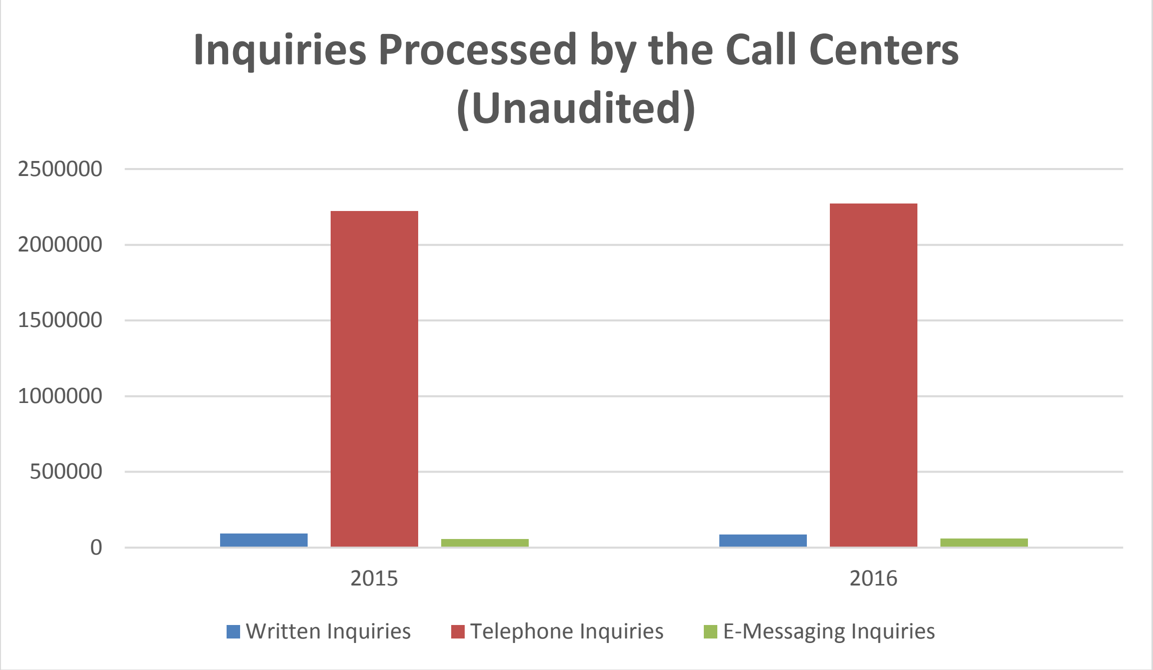
[5] Source: TSP 5003, *Inquiry Status Report*, for December 2016

[6] Source: Thrift Savings Plan *E-Messages Summary* for calendar year 2016

During calendar year 2016, inquiries related to this area accounted for 33 percent of all inquiries processed by the TSP[7].

Exhibit II-1[8] illustrates the number of written, telephone, and e-messaging inquiries processed by the TSP during calendar year 2016. Exhibit II-2 divides the total inquiries processed by the TSP during calendar year 2016 by type of transaction.

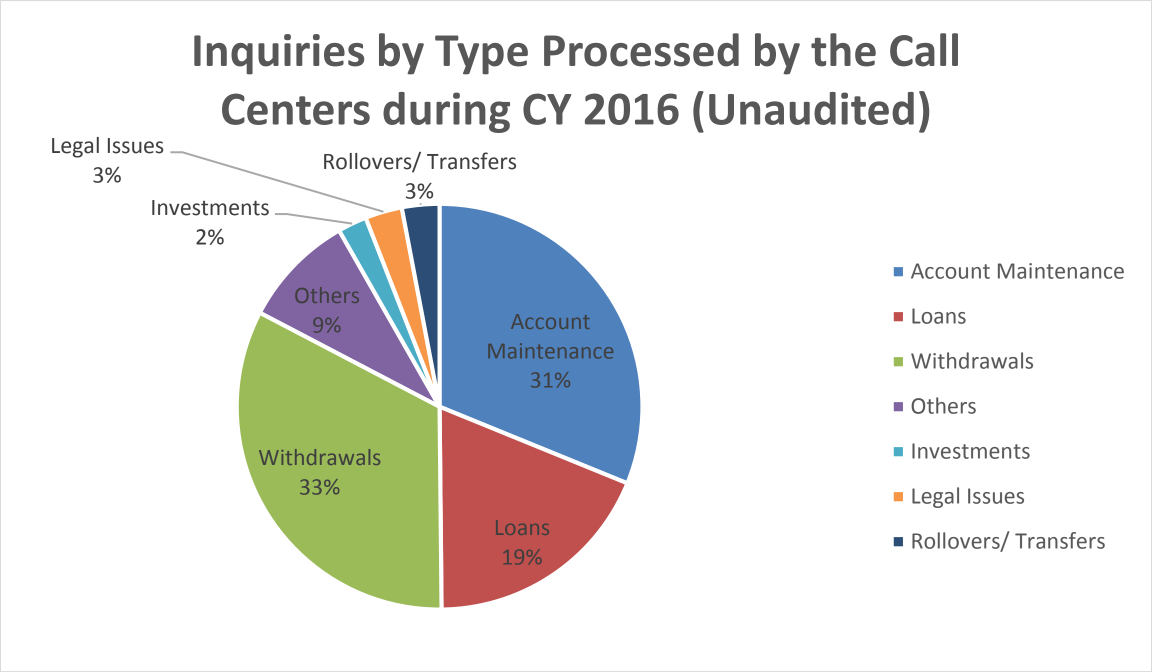
Exhibit II-1



[7] Source: TSP 6011, *Civilian and Uniformed Services Inquiry Report*, for December 2016

[8] Source: TSP 5003, *Inquiry Status Report*, for December 2016 and 2015

Exhibit II-2



2. Participant Statements[9]

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.

[9] Source: *Summary of the Thrift Savings Plan* booklet, version February 2017

C. Description of the TSP Call Centers[10]

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 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, 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[11]), and additional customer service skills training. Selected senior PSRs (e.g., team leads and the helpdesk

[10] Sources: TSP Telephone Service Quality Assurance Program, Virginia Call Center Standard Operating Procedures (SOP), dated December 19, 2016, and Maryland Call Center SOP, dated October 6, 2016.

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

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).

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 a toll-free call arrives 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[12]. 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[13]

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 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.

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

[13] Sources: Agency and call center operating procedures, performance reports, and quality assurance reports.

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 call 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 participants 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.

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 ThriftLine 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 by the call centers. 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 PSRs 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. The tool also contains a bulletin board feature that contains links to common questions and answers or upcoming events and program changes. Additionally, e-messages (messages received, responses, and related notes) are maintained in the Moxie database. 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 Verint 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 our performance audit were to:

- Determine whether 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; (6) enforce physical and logical access controls at the call centers; (7) enforce caller authentication and privacy controls at the call centers; and (8) monitor the call centers' contractors to ensure they are in compliance with the terms of the contracts.

- 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 the Thrift Savings Plan Participant Support Operations*, dated June 15, 2016.

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, 2016 through December 31, 2016. 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[14]. 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 using random attribute sampling to select samples of the following:

- Participant statements, to determine if participants received accurate account information;
- Written inquiries and e-messages, to determine if participant written inquiries and e-messages 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, individuals with physical access to the TSP-dedicated sections of the call centers, and separated individuals, to assess logical and physical access controls at both call centers;
- Call center employees, to assess the enforcement of certain training and Agency on-boarding requirements at both call centers; and
- Calls authenticated and transactions processed by call center representatives, to determine if authentication procedures were performed and to determine if transactions were processed accurately.

[14] 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, 2016 through December 31, 2016.

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, 2016 through December 31, 2016. 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, 2016 through December 31, 2016, 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; (6) enforce physical and logical access controls at the call centers; (7) enforce caller authentication and privacy controls at the call centers; and (8) monitor the call centers' contractors to ensure they are in compliance with the terms of the contracts. As a result of our compliance testing, we did not identify any instances of noncompliance with United States Code Chapter 5, Section 8439(c) or 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 of the TSP participant support process.

We present six new recommendations, presented in Section III.C, related to TSP participant support process, all of which address fundamental controls. Fundamental control recommendations address significant[15] 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

[15] *Government Auditing Standards* section 6.04 defines significance in the context of a performance audit.

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 22 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, five recommendations have been implemented and closed, three recommendations have not been implemented or have been partially implemented but are considered closed, nine recommendations have been partially implemented and remain open, and five recommendations have not been implemented and remain 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 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 2016 performance audit.

a) During 2016 testing, we noted that copies of Versadial recording on DVD/external hard drives, covering the period 2005-2013, remained offsite and unencrypted. Agency management indicated that as a compensating control, the hard drives were locked in a safe deposit box that only a limited number of individuals could access. On December 29, 2016, Agency management signed a one-year risk acceptance, which documented the situation and included compensating controls. However, although the version of Versadial had been updated, an active generic administrator account existed. As a result, this portion of the recommendation remains open.

Disposition:

Recommendation Open.

2009 Participant Support Process 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.**

During our 2016 testing, we noted no exceptions related to privacy training for a selection of 15 users tested at the Maryland call center. However, the Agency did not provide evidence of call center privacy training compliance during 2016 for one of 15 users tested at the Virginia call center.

Disposition: **Recommendation Open.**

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) The Agency has not addressed this portion of the recommendation. However, as a result of changes to the Agency’s operating environment, we revised and reissued this recommendation as 2016 recommendation no. 2016-05. As a result, this portion of the recommendation is closed.

b) During our 2016 testing, the Agency did not provide evidence that access was approved prior to account creation for three of five new network requests selected. As a result, this portion of the recommendation remains open.

Disposition:

Recommendation Open. Also see recommendation no. 2016-05 in Section III.C of this report.

2012 Participant Support 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 2016 performance audit.

b) During 2016 testing, we noted the Maryland call center replaced the Knowledge database previously operating on the unsupported Oracle platform with SharePoint, which was supported by the vendor. However, we noted that the Symposium server at the Maryland call center continued to run on the unsupported Windows 2000. At the Virginia call center, we noted that Symposium continued to run on the unsupported Windows 2003. Although the Agency authorizing official signed one-year risk acceptances for running the unsupported software at the call centers in November 2016, the risk acceptance did not document the mitigating controls that the Agency established to contain the weaknesses identified in the risk acceptance memo (e.g., a corrective action plan or additional vulnerability scans). As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

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: **Implemented.**

During our 2016 testing, we noted that the Agency and call centers had developed and implemented procedures for media protection and sanitization.

Disposition: **Recommendation Closed.**

2015 Participant Support Process Recommendation No. 1:

Title: Control Weaknesses in Administering Logical Access to Agency Systems

Original Recommendation: 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.

Reason for Recommendation: 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).

Status: **Not Implemented.**

Access to Agency systems is requested by the call centers but controlled by the Agency. We performed testing over the Agency's account management program for TSP systems in the 2016 computer access and security controls performance audit, and identified exceptions in the granting, recertification, and timely removal of accounts. Because we reported this issue as an open recommendation in the 2016 computer access and security controls report, we closed this recommendation.

Disposition: **Recommendation Closed.** See *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017, recommendation no. 2007-3, *Logical Access Administration over TSP Systems Should Be Improved*.

2015 Participant Support Process Recommendation No. 2:

Title: Weaknesses in the Call Center Access Recertification Process

Original Recommendation: 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.

Reason for Recommendation: Access recertification weaknesses existed during our scope period at the Virginia and Maryland call centers.

Status: **Partially Implemented.**

a) We tested the recertification of access for Agency-managed systems in the 2016 computer access and security controls performance audit and identified that the control had not been fully implemented. Therefore, it was not included in the scope of this 2016 performance audit.

   Regarding call center-managed systems, we noted that management at the Maryland call center had developed recertification procedures and recertified LAN accounts in accordance with the Agency annual requirement. However, management at the Virginia call center did not develop recertification procedures or perform a recertification of LAN access in 2016. As a result, this portion of the recommendation remains open.

b) During our 2016 fieldwork, Agency management did not provide documented monitoring procedures to ensure call center compliance with Agency recertification requirements. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 3:

Title: Weakness in Restricting Internet Access at the Maryland Call Center

Original Recommendation: 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.

Reason for Recommendation: During our 2015 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.

Status: **Implemented.**

During 2016 testing, we noted that the Agency developed procedures for reviewing internet access at the call centers, the *Call Center Procedure Review of Proxy Server Internet Whitelist*, dated November 17, 2016. We further noted that Maryland call center management performed a quarterly review during the fourth quarter, when the procedures were finalized.

Disposition: **Recommendation Closed.**

2015 Participant Support Process Recommendation No. 4:

Title: Versadial Password Weaknesses at the Virginia Call Center

Original Recommendation: 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.

Reason for Recommendation: Both call centers use the Versadial call recording software. However, the version of Versadial in use during our 2015 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, included minimum password length controls, the Virginia call center had not upgraded its Versadial version because of technical limitations.

Status: **Implemented.**

During our 2016 testing, we observed that the Virginia call center had upgraded its Versadial version to one that requires minimum password length controls.

Disposition: **Recommendation Closed.**

2015 Participant Support Process Recommendation No. 5:

Title: Call Center Physical Access Control Weaknesses

Original Recommendation: 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.

Reason for Recommendation:

During our 2015 audit procedures, we identified certain physical access weaknesses at the Virginia call center server room and Maryland call center data center[16]. 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.

Status:

Not Implemented.

a) We noted that the Maryland call center had documented procedures for the pre-approval of physical access to secured call center areas; however, the Virginia call center had not, and the Agency had not developed, documented or implemented monitoring procedures to enforce the related EISRM policies. As such, this portion of the recommendation remains open.

b) During testing, we noted that the Agency had not developed, documented, or implemented monitoring procedures to ensure that call center management periodically reviews data center and server room access at the Maryland and Virginia call centers. Although the Maryland call center had documented procedures and recertified physical access to the call center, the Virginia call center had not. As such, this portion of the recommendation remains open.

Disposition:

Recommendation Open.

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

2015 Participant Support Process Recommendation No. 6:

Title: Call Center Configuration and Patch Management Weaknesses

Original Recommendation: 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.

Reason for Recommendation: Configuration and patch management vulnerabilities and weaknesses existed at both call centers during our 2015 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.
- 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.
- 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.

Status: **Partially Implemented.**

a) The Agency had not developed, documented, and implemented monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely. Additionally, the Agency did not perform authenticated scans for the call center from August 2016 through December 2016. As a result, this portion of the recommendation remains open.

b) The Agency had not developed, documented, and implemented 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. Additionally, evidence was not provided of call center tracking and remediation of vulnerabilities. As a result, this portion of the recommendation remains open.

c) During our 2016 testing, we noted that the Agency had documented a Responsibilities Matrix, which defined responsibilities for oversight and enforcement of Agency information security requirements to Agency divisions with appropriate knowledge to evaluate performance. As a result, this portion of the recommendation is closed.

d) The Agency did not provide workstation images or Agency-defined baseline configurations to each call center and did not implement periodic monitoring of workstation compliance with USGCB settings. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

2015 Participant Support Process Recommendation No. 7:

Title: Call Center Contract Oversight Weaknesses

Original Recommendation: 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.

Reason for Recommendation:

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;
- 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;
- 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.

Status:

Partially Implemented.

a) The Agency had documented a Responsibilities Matrix, which defined responsible parties for oversight of contract requirements; however, the matrix did not include sufficient detail to determine what individual was responsible for the oversight, what monitoring and review procedures need to be performed, and the frequency of communication of call center monitoring results to the contracting officer’s representative. As a result, this portion of the recommendation remains open.

b) During our 2016 testing, we noted that the Agency was in the process of revising the contracts for re-compete purposes. Management indicated that the revised contracts will support the Agency's review of all contract clauses. We further noted the current call center contracts were modified to replace the former Statement on Standards for Attestation Engagements (SSAE) No. 16 requirement with a requirement for a Service Organization Control Type II engagement for the Maryland call center and a requirement for an agreed upon procedures engagement at the Virginia call center. As a result, this portion of the recommendation is closed.

c) During our 2016 testing, we noted that the Agency updated the call center contracts to modify the documented SSAE No. 16 requirement, which we identified as no longer being applicable during the 2015 participant support performance audit. Although the change was not implemented until December 2016, we saw evidence of coordination with the contracting officer and the vendor beginning in 2015. As a result, this portion of the recommendation is closed.

d) The Agency did not provide documented procedures for the enforcement of contract compliance with required reporting metrics. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 8:

Title: Encryption Weaknesses on Local Versadial Data Storage

Original Recommendation: 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.

Reason for Recommendation: Participant information recorded using the Versadial software located at the Maryland and Virginia call centers was not encrypted, although the data recorded contained sensitive information and personally identifiable information (PII). Backups of this data reside at the primary data center in Vienna and at each call center.

Status: **Not Implemented.**

During our 2016 testing, we noted that the Agency had not yet identified and implemented a solution to encrypt the Versadial data and servers that contain PII at the call centers.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 9:

Title: Encryption Weaknesses on Maryland Call Center Workstations

Original Recommendation: 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.

Reason for Recommendation: 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.

Status: **Not Implemented.**

During our 2016 testing, we noted that the Agency had not yet identified and implemented a solution to encrypt data retained on PSR workstations used for handling participant data.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 10:

Title: Weaknesses in the Virginia Call Center Security Management Program

Original Recommendation: 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.

Reason for Recommendation:

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 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, within the mandated timeframe;
- 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;
- The Agency did not update the Virginia call center POA&Ms 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; 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.

Status:

Partially Implemented.

a) During our scope period, the Agency had not updated the Virginia call center SSP to comply with NIST 800-53 Rev. 4 guidance related to PL-8, *Information Security Architecture Control*, and CM-11, *User Installed Software Control*, as recommended in our 2015 audit report. Further, the Agency did not update the SSP to reflect changes in key personnel, including the Authorizing Official and System Owner. As a result, this portion of the recommendation remains open.

b) During testing, we noted that the Agency did not properly update the Virginia call center SSP to include minimum security controls and associated requirements, as required by NIST for moderate systems. As a result, this portion of the recommendation remains open.

c) The POA&M had been updated during the scope period; however, the Virginia call center had not remediated or accepted the risk associated with an Agency-defined 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. As a result, this portion of the recommendation remains open.

d) The Agency completed a PIA for the Virginia call center, which was signed on March 17, 2016 by the Senior Agency Official for Privacy. As a result, this portion of the recommendation is closed.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 11:

Title: Weaknesses in the Maryland Call Center Security Management Program

Original Recommendation: 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.

Reason for Recommendation: During our 2015 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 Assessment and Authorization (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.

Status: **Partially Implemented.**

a) Maryland call center management finalized the A&A and provided a security risk acceptance, SSP, and authorization letter to the Agency in accordance with contractual requirements. As such, this portion of the recommendation is closed.

b) The Agency did not implement quarterly reviews of the Maryland call center POA&M tracking known weaknesses and vulnerabilities. As such, this portion of the recommendation remains open.

c) The Maryland call center and Agency management completed a PTA in April 2016 in accordance with policy. As such, this portion of the recommendation is closed.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 12:

Title: Rules of Behavior Weakness at the Virginia Call Center

Original Recommendation: 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.

Reason for Recommendation: During our 2015 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.

Status: **Not Implemented.**

The Agency is responsible for obtaining completed ROBs prior to granting call center representatives access to Agency systems. We performed testing over the Agency's account management program for TSP systems within the 2016 computer access and security controls performance audit, and identified exceptions over the completion and tracking of ROBs. As such, we did not perform additional testing within the 2016 participant support performance audit. Because we reported this issue as an open recommendation in the 2016 computer access and security controls report, we closed this participant support recommendation.

Disposition: **Recommendation Closed.** See *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017, recommendation no. 2015-9, *Inconsistent Use of Rules of Behavior (RoB) Requirements*.

2015 Participant Support Process Recommendation No. 13:

Title: Media Sanitization and Disposal Weakness

Original Recommendation: 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.

Reason for Recommendation: Although surplussed hard drives had been sanitized and removed from the Maryland call center, surplussed 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.

Status: **Implemented.**

During our 2016 testing, we noted that the Agency had established a contract with a vendor for media sanitization and disposal for use by the Agency and call center management.

Disposition: **Recommendation Closed**.

2015 Participant Support Process Recommendation No. 14:

Title: Insufficient Documentation Supporting the TSP Website Calculators

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

Reason for Recommendation: 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.

Status: **Partially Implemented.**

During the scope period, we noted that the Agency documented and maintained Microsoft Excel formulas supporting the accuracy of the TSP website calculators. We obtained such formulas and the related reference guides for the web calculators and recalculated all calculators to a sufficient degree of accuracy except for the Retirement Income Calculator. For the Retirement Income Calculator, the formula documented in the reference guide resulted in a "#NUM!" error, and the Excel formulas provided by the Agency did not provide a resolution to demonstrate this calculator's accuracy.

Disposition: **Recommendation Open**.

2015 Participant Support Process Recommendation No. 15:

Title: Congressional Inquiry Documentation Weaknesses

Original Recommendation: 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.

Reason for Recommendation: 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.

Status: **Implemented.**

During our 2016 testing, we received supporting documentation for all 24 Congressional inquiries selected for testing. In addition, we obtained and reviewed the *Congressional Inquiries Policy Document* and the *Congressional Inquiry Procedure Document*, both dated as of December 31, 2016. We noted that the *Congressional Inquiry Procedure Document* included procedures over the documentation, maintenance, and availability of Congressional inquiries and responses, but it excluded inquiries received via telephone. Based on discussions with Agency management, telephone inquiries are infrequent and are usually simple questions about the plan rather than specific participant account questions. For these reasons, the Agency did not include telephone inquiries in its formal inquiry tracking and response procedures. During our audit procedures, we did not identify any Congressional telephone inquiries; as such, we considered the exclusion of such inquiries from the Agency's formal procedures reasonable.

Disposition: **Recommendation Closed.**

2015 Participant Support Process Recommendation No. 16:

Title: Congressional Inquiry Tracking Weaknesses

Original Recommendation: 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.

Reason for Recommendation: 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.

Status: **Not Implemented.**

Although we did not identify deficiencies in the maintenance of the Agency log during our 2016 testing, the Agency log did not contain evidence of management review. We noted that the *Congressional Inquiry Procedure Document*, effective December 31, 2016, describes the procedures to be performed in reviewing, tracking, and responding to congressional inquiries. However, the document does not include management review responsibilities or periodic review procedures to be performed over either the Agency log or the Congressional Correspondence Summary.

Disposition: **Recommendation Open.**

2015 Participant Support Process Recommendation No. 17:

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

Original Recommendation: 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.

<u>Reason for Recommendation:</u> We noted that the Agency had not developed and implemented written policies and procedures related to various aspects of the TSP participant support process.

<u>Status:</u> **Partially Implemented.**

a) We noted that the Agency developed a *Congressional Inquiry Procedure Document*, effective December 31, 2016; however, it does not include management review responsibilities or periodic review procedures to be performed over the Congressional Correspondence Summary. Although this portion of the recommendation was not implemented, it is also addressed in 2015 Participant Support Process Recommendation No. 16, as the Congressional Correspondence Summary is used concurrently with the Agency log. Therefore, this portion of the recommendation is closed.

b) We noted that the Agency developed a *Print Mail Policies and Procedures*, effective September 30, 2016, that, along with the *Requirements Documents* submitted to the statement compilation and printing contractors, describes the procedures related to the generation and distribution of participant account statements. Therefore, this portion of the recommendation is closed.

c) Based on our testing, we noted that the Agency did not implement this recommendation during 2016. No manual review was performed over confirmation notices or reject notices because the Agency relies on the system configuration to accurately generate confirmation and reject notices. We obtained and reviewed the functional design documents that defined the various processing actions that generate either a confirmation or reject notice. Additionally, we did not identify any improperly generated confirmation or reject notices during our 2016 sample testing of 116 notices, and Agency management indicated that they were not made aware of any improperly generated confirmation or reject notices during our scope period. As such, this portion of the recommendation is closed.

d) We noted that the Agency developed *Writer/Editor Team Procedures*, effective September 30, 2016, that documented the procedures for producing and reviewing written TSP communications, and a *Web Calculator Review Desk Procedures* document, effective January 31, 2017, that documented the procedures for reviewing and determining whether updates are needed to the TSP website. Although the *Web Calculator* procedure document was implemented subsequent to our scope period but prior to completion of our fieldwork, this portion of the recommendation is closed.

Disposition: **Recommendation Closed.**

C. 2016 Findings and Recommendations

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

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2016-1: Weaknesses in Call Center Password Requirements

During our scope period, we noted that the Maryland and Virginia call center LANs were not configured to meet the minimum password requirements defined in the Agency's Enterprise Information Security and Risk Management (EISRM) Program Policy and the Baseline Security Requirements (BLSR). Specifically, both call centers required passwords to include only three of the four specified character types (uppercase letters, lowercase letters, numbers, and special characters). Additionally, the Maryland call center LAN was not configured to meet the minimum password history of 24 or the 60 day maximum password age required by the BLSR.

Call centers' management did not fully implement required Agency policies because of a lack of communication of Agency policies and procedures and overreliance on contracted support.

Additionally, Agency oversight was not performed by individuals within appropriate technical roles.

The Agency's Enterprise Information Security and Risk Management (EISRM) Identification and Authentication (IA) Policy, dated June 29, 2012, states:

> (d) Authenticator Management (IA-5 + Enhancements #1, 2, & 3) […]
>
> (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:
>
> - [ ] ! @ # $ % ^ & * ( ) { } < >
>
> Note: Users with elevated privileges (e.g., administrators) SHOULD use passwords with at least 14 characters, although separate system-level enforcement for a subcategory of users is not generally possible.
>
> (D) Enforce password minimum (1 day) and maximum (90 days) lifetime restrictions; and
>
> (E) Prohibit password reuse for a specified number of generations (minimum password history of twenty or more passwords "remembered").

The Agency's *EISRM Baseline Security Requirements (BLSR)* document, effective May 31, 2015, states:

> IA-5 (1) Password-Based Authentication:
>
> 1. The System Administrator SHALL:
>
> 1.2. Enforce minimum password complexity of 12 characters and at least one each of upper-case letters, lower-case letters, numbers, and special characters
>
> 1.4. Enforce password lifetime restrictions of one (1) day minimum and 60 days maximum for user accounts
>
> 1.6. Prohibit password reuse for at least 24 generations

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Authenticator Management, Control IA-5, Control Enhancement (1) states:

> (1) Authenticator Management | Password-Based Authentication
>
> The information system, for password-based authentication:
>
> (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
>
> (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum].

1. **To strengthen password controls, the Agency should enforce Agency requirements for password complexity settings for the Maryland and Virginia call center LANs.**

Weaknesses in password controls increase the risk of unauthorized access to user accounts, which may lead to unauthorized disclosure, modification, or destruction of Agency or participant data.

2016-2: Weakness in Maryland Call Center Media Disposal

During our testing, we were unable to obtain evidence of the disposal of the surplus workstation equipment and memory storage set aside for sanitization and disposal for the Maryland call center. The Agency did not have documentation of the disposal of specific workstation equipment and memory storage because of a lack of coordination between organizational entities and an overreliance on contracted support.

The Agency's *IT Security Electronic Media Destruction or Sanitization Procedure* document, effective January 1, 2015, states:

> 4.3.3 Required Information for Electronic Media Destruction or Sanitization Request (EMDSR)
>
> The EMDSR must be completed in its entirety to include enough information about the media or device to be sanitized to ensure the proper sanitization method is used to protect the FRTIB data.
>
> The EMDSR requires the requester to provide the following information:
>
> - Requester name
> - Requester Department

- System ID
- Media Type
- Part Number (if available)
- Serial Number (if available)

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Media Sanitization, Control MP-6 (1), states:

> The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.
>
> Supplemental Guidance states: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal.

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*, September 2014, states:

> Principle 16.01, page 65: Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
>
> Principle 16.03, page 65: Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring.

2. **The Agency should develop, document, and implement monitoring procedures to ensure that the call centers implement media sanitization and disposal procedures.**

Without tracking the unique hardware sanitized and disposed, the likelihood that media may be lost or misplaced increases, resulting in the risk of inadvertent or deliberate disclosure of Agency systems and participant data.

2016-3: Weakness in Maryland Call Center Physical Access Removal

For 7 of 82 Maryland call center terminations during the scope period, former employees retained physical access to the Agency section of the call center after termination. Call center management indicated that the badges were taken from the individuals and locked up prior to the access being removed to mitigate related risk. However, call center management had not established a backup process for the timely removal of access when the human resources individual responsible for managing call center access is unavailable. Further, the quarterly physical access recertification of accounts was not successful in identifying and removing employees who retained access after termination.

The Agency's EISRM Physical and Environmental Security (PE) Policy, dated June 29, 2012 states:

> Physical Access Authorizations (PE-2)
>
> 1 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.

The Agency's *EISRM BLSR* document, dated May 31, 2015, states:

> PE-2 Physical Access Authorizations:
>
> 1. The System Owner SHALL:
>
> 1.5. Remove individuals from the facility access list when access is no longer required.

NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Physical Access Authorizations, Control PE-2, states:

> Control: The organization:
>
> d. Removes individuals from the facility access list when access is no longer required.

3. **To strengthen Maryland call center physical access controls, the Agency should:**

   a. Update the Maryland call center physical access procedures and implement a process for the timely removal of access when the human resources individual responsible for managing call center access is unavailable.

b. **Update the Maryland call center physical access procedures for periodic recertification and implement a process to ensure that call center personnel do not retain access to the call center after termination.**

Weaknesses in controls for removing physical access permissions to the call center increase the risk that individuals may have inappropriate access to Agency and participant data, which places such data at risk of inadvertent or deliberate disclosure, modification, or destruction.

2016-4: Weaknesses in Virginia Call Center Logical Access Management

Virginia call center management did not provide evidence that logical access to the Virginia call center LAN was removed timely after termination for three of 167 users and after access was no longer required for one user. Additionally, we noted that the process for creating LAN accounts during 2016 included creating accounts prior to the individual signing the Agency non-disclosure agreement (NDA) and ROB, or completing security awareness training, which was not in accordance with Agency policy.

Call center management's logical access procedures did not require the maintenance of documentation to allow the call center to demonstrate timely LAN access removal for terminated users. Additionally, the procedures did not include a process for the removal of access for accounts after access is no longer required, separate from the termination process. Further, call center management did not develop and implement a process to require new employees to sign Agency-required forms and take Agency-required training because of a lack of coordination between organizational entities.

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

(a) Account Management (CM-2 + Enhancements 1, 2, 3, and 4) […]

(1) Information System Owners and/or Information Owners SHALL:

(F) Immediately notify Information System Custodians/Account Managers and Security Administrators whenever:

(iii) A User is terminated, transferred, or placed on administrative leave.

(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:

(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;

  (ii) Expiration of temporary access;

  (iii) Transfer of a user to a position which does not require the same access (i.e., any access) as previously required;

  (iv) Security incident involving the User (e.g., inappropriate usage or unauthorized access).

The Agency's *EISRM BLSR* document, dated May 31, 2015, states:

AC-2 Account Management

3 The System Administrator SHALL:

3.4. Create accounts after validation of signed receipt of Non-Disclosure Agreement (NDA) from contractors, Security, Education, Training, and Awareness (SETA) Certificate, FRTIB Rules of Behavior (RoB), and a favorably adjudicated background investigation commensurate with the level of access required

4 Supervisors, System Administrators, System Owners, Business Owners, Chief Information Security Officer, Information System Security Officers, and COR SHALL:

4.1. Notify account management when:

4.1.1. Accounts are no longer required

4.1.2. Users are terminated or transferred

4.1.3. Individual information system usage or need-to-know changes

PS-4 Personnel Termination

3. The Service Desk SHALL:

3.1. Disable all information system access within 2 hours of notification

3.2. Immediately disable accounts for any individuals identified for termination

3.3. Terminate/revoke any authenticators/credentials associated with the individual.

NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Account Management, Control AC-2, states:

> Control: The organization:
>
> f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
>
> h. Notifies account managers:
>
> 1. When accounts are no longer required;
> 2. When users are terminated or transferred; and
> 3. When individual information system usage or need-to-know changes;

4. **To strengthen Virginia call center logical access controls, the Agency should:**

   a. Ensure the call center has developed, documented, and implemented procedures for the timely removal of access to the call center LAN after a user no longer requires access and for maintenance of related documentation; and

   b. Develop, document, and provide to the call center procedures to require the completion of required Agency agreements, training, and background investigation prior to account creation on the call center LAN.

Weaknesses in controls for removing logical access permissions or granting access without proper training and background investigations increase the risk that individuals may have inappropriate access to Agency and participant data, which places them at risk of inadvertent or deliberate disclosure, modification, or destruction.

<u>2016-5: Weakness in Restricting Internet Access at the Call Centers</u>

During our scope period, the Agency developed procedures for reviewing internet access at the call centers, *Call Center Procedure Review of Proxy Server Internet Whitelist*, dated November 17, 2016. However, we noted the procedures did not establish or enforce a process for Agency review of all allowed websites at the call centers for business need or security concerns. Specifically, we noted that:

- The procedures require the call centers to review and provide the Agency with the whitelist and an explanation of the included websites; however, the whitelist at the Virginia call center was not the complete list of all allowed websites. Call center management restricted internet access by identifying blocked sites, not by denying all websites except those explicitly identified on the whitelist.

- The procedures do not document the process for the Agency to review websites for business need and security concerns and provide approval prior to call center management allowing access to the websites.

Additionally, for the Virginia call center, certain websites not identified on the block list (i.e., list of websites not allowed to be viewed) that were accessible to PSRs, including sites that were identified in previous EBSA audits, were unnecessary for individual PSR job functions and posed potential security risks to PSR workstations and participant data.

Weaknesses existed within Agency procedures because of a lack of understanding of call center processes by Agency management and a lack of coordination between organizational entities.

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; […]

5. To strengthen security controls, the Agency should enhance monitoring procedures for periodically reviewing call center internet whitelists to:

a. Ensure that Maryland and Virginia call center management periodically review all allowed internet sites and restrict all unnecessary sites.

b. Specify a process for Agency review and approval of websites for business need and security concerns and prior to call center management allowing access to the websites.

c. Define responsible Agency individuals to periodically review websites allowed at the call centers and the process for documenting and communicating review results to the contracting officer's representative and call center management.

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

2016-6: Incomplete Maryland Call Center Privacy Impact Assessment

As of December 31, 2016, a PIA had not been completed for the Maryland call center LAN because of a lack of contractor oversight and coordination between appropriate Agency offices.

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 EGovernment 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)

(2) Information System Owners SHALL ensure that additional security controls are designed and implemented to mitigate risks to Personally Identifiable Information determined to exist through the Privacy Impact Assessment (PIA).

NIST SP 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, Appendix J, Privacy Control Catalog, states:

AR-2 Privacy Impact and Risk Assessment

Control: The organization:

a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and
b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Supplemental Guidance: Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. […]

6. **The Agency should:**

a. Complete the PIA for the Maryland call center; and

b. Identify and document the specific locations that house PII for the Maryland call center in a PII inventory that is secured.

Without identifying and documenting the location of PII within each system boundary, Agency management may not be able to apply appropriate security controls to secure the information. This situation could result ultimately in an increased risk of disclosure, modification, or destruction of Agency-maintained sensitive information and PII.

D. Summary of Open Recommendations

<u>2009 RECOMMENDATIONS</u>

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.

<u>2012 RECOMMENDATIONS</u>

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:
   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.

<u>2015 RECOMMENDATIONS</u>

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

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.

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; 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; 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.

*Weaknesses in the Maryland Call Center Security Management Progra*m

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

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 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 Congressional file on a periodic basis.

<u>2016 RECOMMENDATIONS</u>

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in Call Center Password Requirements

1. To strengthen password controls, the Agency should enforce Agency requirements for password complexity settings for the Maryland and Virginia call center LANs.

Weakness in Maryland Call Center Media Disposal

2. The Agency should develop, document, and implement monitoring procedures to ensure that the call centers implement media sanitization and disposal procedures.

Weakness in Maryland Call Center Physical Access Removal

3. To strengthen Maryland call center physical access controls, the Agency should:
   a) Update the Maryland call center physical access procedures and implement a process for the timely removal of access when the human resources individual responsible for managing call center access is unavailable.
   b) Update the Maryland call center physical access procedures for periodic recertification and implement a process to ensure that call center personnel do not retain access to the call center after termination.

Weaknesses in Virginia Call Center Logical Access Management

4. To strengthen Virginia call center logical access controls, the call center should:

a) Ensure that the call center has developed, documented, and implemented procedures for the timely removal of access to the call center LAN after a user no longer requires access and for maintenance of related documentation; and

b) Develop, document, and provide to the call center procedures to require the completion of required Agency agreements, training, and background investigation prior to account creation on the call center LAN.

Weakness in Restricting Internet Access at the Call Centers

5. To strengthen security controls, the Agency should enhance monitoring procedures for periodically reviewing call center internet whitelists to:

   a) Ensure that Maryland and Virginia call center management periodically review all allowed internet sites and restricts all unnecessary sites.

   b) Specify a process for Agency review and approval of websites for business need and security concerns and prior to call center management allowing access to the websites.

   c) Define responsible Agency individuals to periodically review websites allowed at the call centers and the process for documenting and communicating review results to the contracting officer's representative and call center management.

Incomplete Maryland Call Center Privacy Impact Assessment

6. The Agency should:

   a) Complete the PIA for the Maryland call center; and

   b) Identify and document the specific locations that house PII for the Maryland call center in a PII inventory that is secured.

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

THRIFT
SAVINGS
PLAN

May 4, 2017

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

Dear Michael:

This is in response to KPMG's email on April 25, 2017, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan Participant Support Operations, dated May 2017. My comments with respect to this report are enclosed.

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

Very truly yours,

Gregory T. Long

Enclosure

Executive Director's Staff Formal Comments on the
Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan
Participant Support Operations

Prior Year Recommendations to Address Fundamental Controls

2009-4: Call Center Technology Weaknesses Should Be Addressed

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.

2016 Status: Partially Implemented

a. During 2016 testing, we noted that copies of Versadial recording on DVD/external hard drives, covering the period 2005-2013, remained offsite and unencrypted. Agency management indicated that as a compensating control, the hard drives were locked in a safe deposit box that only a limited number of individuals could access. On December 29, 2016, Agency management signed a one-year risk acceptance, which documented the situation and included compensating controls. However, although the version of Versadial had been updated, an active generic administrator account existed. As a result, this portion of the recommendation remains open.

Agency Response:

a. The Agency concurs with the recommendation and considers it closed. The Virginia call center changed the status of the generic administrator account from enabled to disabled after the close of audit fieldwork.

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.

2016 Status: Partially Implemented

During our 2016 testing, we noted no exceptions related to privacy training for a selection of 15 users tested at the Maryland call center. However, the Agency did not provide evidence of call center privacy training compliance during 2016 for one of 15 users tested at the Virginia call center. As a result, this portion of the recommendation remains open.

Agency Response:

The Agency concurs with the recommendation. The Agency will enhance existing procedures to ensure that documentation of evidence is maintained and stored. The Agency will implement the procedures by July 31, 2017.

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

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

b. Develop and implement alternative procedures to maintain documentation supporting the approval of network access for all individuals with such access.

2016 Status: Not Implemented

b. During our 2016 testing, the Agency did not provide evidence that access was approved prior to account creation for three of five new network requests selected. As a result, this portion of the recommendation remains open.

Agency Response:

b. The Agency concurs with the recommendation. The Agency will enhance existing procedures to ensure that documentation of evidence is maintained and stored. The Agency will implement the procedures by November 30, 2017.

2012-4: Weaknesses in Call Center Configuration Management Controls

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.

2016 Status: Partially Implemented

b. During 2016 testing, we noted the Maryland call center replaced the Knowledge database previously operating on the unsupported Oracle platform with SharePoint, which was supported by the vendor. However, we noted that the Symposium server at the Maryland call center continued to run on the unsupported Windows 2000. At the Virginia call center, we noted that Symposium continued to run on the unsupported Windows 2003. Although the Agency authorizing official signed one-year risk acceptances for running the unsupported software at the call centers in November 2016, the risk acceptance did not document the mitigating controls that the Agency established to contain the weaknesses identified in the risk acceptance memo (e.g., a corrective action plan or additional vulnerability scans). As a result, this portion of the recommendation remains open.

Agency Response:

b. The Agency concurs with the recommendation. The Agency will upgrade all TSP supporting systems at the call centers by November 30, 2017.

2015-2: Weaknesses in Call Center Access Recertification Process

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.

2016 Status: Partially Implemented

a. We tested the recertification of access for Agency-managed systems in the 2016 computer access and security controls performance audit and identified that the control had not been fully implemented. Therefore, it was not included in the scope of this 2016 performance audit. Regarding call center-managed systems, we noted that management at the Maryland call center had developed recertification procedures and recertified LAN accounts in accordance with the Agency annual requirement. However, management at the Virginia call center did not develop recertification procedures or perform a recertification of LAN access in 2016. As a result, this portion of the recommendation remains open.

b. During our 2016 fieldwork, Agency management did not provide documented monitoring procedures to ensure call center compliance with Agency recertification requirements. As a result, this portion of the recommendation remains open.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will develop, document and implement recertification procedures as part of the Access Control procedures, for all systems, including systems supporting for the Virginia and Maryland call centers by June 30, 2017.

b. The Agency concurs with the recommendation. The Agency will develop, document, and implement monitoring procedures to ensure Agency and call center compliance with Agency recertification requirements by October 31, 2017.

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.

Status: Not Implemented

a. We noted that the Maryland call center had documented procedures for the pre-approval of physical access to secured call center areas; however, the Virginia call center had not, and the Agency had not developed, documented or implemented monitoring procedures to enforce the related EISRM policies. As such, this portion of the recommendation remains open.

b. During testing, we noted that the Agency had not developed, documented, or implemented monitoring procedures to ensure that call center management periodically reviews data center and server room access at the Maryland and Virginia call centers. Although the Maryland call center had documented procedures and recertified physical access to the call center, the Virginia call center had not. As such, this portion of the recommendation remains open.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will ensure a procedure to manage, control, and document pre-approval of physical access is developed and implemented. The Agency will consider this recommendation closed when the procedure is implemented by August 31, 2017.

b. The Agency concurs with the recommendation. The Agency will ensure a procedure to manage, control, and document periodic recertification of physical access is developed and implemented. The Agency will consider this recommendation closed when the procedure is implemented by August 31, 2017.

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;

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

2016 Status: Partially Implemented

a. The Agency had not developed, documented, and implemented monitoring procedures for the Virginia call center to ensure that vulnerabilities are identified, documented, tracked, and remediated timely. Additionally, the Agency did not perform authenticated scans for the call center from August 2016 through December 2016. As a result, this portion of the recommendation remains open.

b. The Agency had not developed, documented, and implemented 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. Additionally, evidence was not provided of call center tracking and remediation of vulnerabilities. As a result, this portion of the recommendation remains open.

d. The Agency did not provide workstation images or Agency-defined baseline configurations to each call center and did not implement periodic monitoring of workstation compliance with USGCB settings. As a result, this portion of the recommendation remains open.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will develop a corrective action plan by June 30, 2017.

b. The Agency concurs with the recommendation. The Agency will develop a corrective action plan by June 30, 2017.

d. The Agency concurs with the recommendation. The Agency will provide workstation images to the enterprise, to include both call centers and remote sites. These images will leverage the FRTIB-approved baseline configuration settings. In addition, the Agency will document and implement workstation configuration compliance scanning procedures to ensure consistent workstation configuration at all sites. The Agency expects this effort to be completed by December 31, 2017.

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;

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

<u>2016 Status: Partially Implemented</u>

a. The Agency had documented a Responsibilities Matrix, which defined responsible parties for oversight of contract requirements; however, the matrix did not include sufficient detail to determine what individual was responsible for the oversight, what monitoring and review procedures need to be performed, and the frequency of communication of call center monitoring results to the contracting officer's representative. As a result, this portion of the recommendation remains open.

d. The Agency did not provide documented procedures for the enforcement of contract compliance with required reporting metrics. As a result, this portion of the recommendation remains open.

<u>Agency Response:</u>

a. The Agency will further enhance the Responsibilities Matrix to create a more robust methodology for the appropriate oversight and management of contract clauses. This will include details which may include identifying individuals responsible for oversight, what monitoring and review procedures need to be performed, and the frequency of communication of call center monitoring results. The Agency will complete the updated Responsibilities Matrix by December 31, 2017.

d. The Agency concurs with the recommendation. The Agency will modify the current OPOP COR oversight procedures by July 31, 2017.

2015-8: Encryption Weaknesses on Local Versadial Data Storage

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.

<u>2016 Status: Not Implemented</u>

During our 2016 testing, we noted that the Agency had not yet identified and implemented a solution to encrypt the Versadial data and servers that contain PII at the call centers.

<u>Agency Response:</u>

The Agency concurs with the recommendation. The Agency will have a corrective action plan by July 31, 2017.

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.

2016 Status: Not Implemented
During our 2016 testing, we noted that the Agency had not yet identified and implemented a solution to encrypt data retained on PSR workstations used for handling participant data.

Agency Response:

The Agency concurs with the recommendation. The Agency will provide workstation images to the enterprise, to include both call centers and remote sites. These images will leverage the FRTIB-approved baseline configuration settings. In addition, the Agency will document and implement workstation configuration compliance scanning procedures to ensure consistent workstation configuration at all sites. The Agency will complete this effort by December 31, 2017.

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.

2016 Status: Partially Implemented

a. During our scope period, the Agency had not updated the Virginia call center SSP to comply with NIST 800-53 Rev. 4 guidance related to PL-8, *Information Security Architecture Control*, and CM-11, *User Installed Software Control*, as recommended in our 2015 audit report. Further, the Agency did not update the SSP to reflect changes in key personnel, including the Authorizing Official and System Owner. As a result, this portion of the recommendation remains open.

b. During testing, we noted that the Agency did not properly update the Virginia call center SSP to include minimum security controls and associated requirements, as required by NIST for moderate systems. As a result, this portion of the recommendation remains open.

c. The POA&M had been updated during the scope period; however, the Virginia call center had not remediated or accepted the risk associated with an Agency-defined 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. As a result, this portion of the recommendation remains open.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will update the Virginia call center SSP to comply with NIST SP 800-53 Rev 4 by June 30, 2017.

b. The Agency concurs with the recommendation. The Agency will document all minimum system security controls as required by NIST for moderate systems in the Virginia call center SSP by June 30, 2017.

c. The Agency concurs with the recommendation. The Agency will develop a corrective action plan by December 31, 2017.

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:

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;

2016 Status: Partially Implemented

b. The Agency did not implement quarterly reviews of the Maryland call center POA&M tracking known weaknesses and vulnerabilities. As such, this portion of the recommendation remains open.

Agency Response:

b. The Agency concurs with the recommendation. The Agency will develop a corrective action plan by December 31, 2017.

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.

2016 Status: Partially Implemented
During the scope period, we noted that the Agency documented and maintained Microsoft Excel formulas supporting the accuracy of the TSP website calculators. We obtained such formulas and the related reference guides for the web calculators and recalculated all calculators to a sufficient degree of accuracy except for the Retirement Income Calculator. For the Retirement Income Calculator, the formula documented in the reference guide resulted in a "#NUM!" error, and the Excel formulas provided by the Agency did not provide a resolution to demonstrate this calculator's accuracy.

Agency Response:

The Agency concurs with the recommendation. The Agency will develop a corrective action plan by June 30, 2017.

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 Congressional file on a periodic basis.

2016 Status: Not Implemented
Although we did not identify deficiencies in the maintenance of the Agency log during our 2016 testing, the Agency log did not contain evidence of management review. We noted that the *Congressional Inquiry Procedure Document*, effective December 31, 2016, describes the procedures to be performed in reviewing, tracking, and responding to congressional inquiries. However, the document does not include management review responsibilities or periodic review procedures to be performed over either the Agency log or the Congressional Correspondence Summary.

Agency Response:

The Agency partially concurs with the recommendation. The Agency does not believe that the cost of expending staff hours reviewing the log yields a commensurate benefit, as there is no adverse impact to participants in the current state.

However, the Agency has amended its Congressional Inquiry Procedures effective April 30, 2017, to reflect that the Director of OEA will document her review of the Congressional Correspondence Summary (a report tabulating incoming and outgoing letters, as well as the number of days to respond) by initialing and dating the document. This will ensure that Agency behavior which might impact a participant (an undue delay

2016 Participant Support Operations
Appendix A

in Agency response) is monitored and adjusted as needed. The Agency considers this recommendation closed.

2016-1: Weaknesses in Call Center Password Requirements

To strengthen password controls, the Agency should enforce Agency requirements for password complexity settings for the Maryland and Virginia call center LANs.

Agency Response:

The Agency concurs with the recommendation. The Agency will develop a corrective action plan by June 30, 2017.

2016-2: Weakness in Maryland Call Center Media Disposal

The Agency should develop, document, and implement monitoring procedures to ensure that the call centers implement media sanitization and disposal procedures.

Agency Response:

The Agency partially concurs with the recommendation. The Maryland call center has implemented media disposal and sanitization procedures. The Agency will ensure that the Maryland call center enhances these procedures to include more detailed evidence of media sanitization and disposal by July 31, 2017.

2016-3: Weakness in Maryland Call Center Physical Access Removal

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

a. Update the Maryland call center physical access procedures and implement a process for the timely removal of access when the human resources individual responsible for managing call center access is unavailable.

b. Update the Maryland call center physical access procedures for periodic recertification and implement a process to ensure that call center personnel do not retain access to the call center after termination.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will ensure that procedures to manage, control, and document the timely removal of physical access are developed and implemented. The Agency will consider this recommendation closed when the procedure is implemented by August 31, 2017.

b. The Agency concurs with the recommendation. The Agency concurs with the recommendation. The Agency will ensure a procedure to manage, control, and document periodic recertification of physical access are developed and implemented. The Agency will consider this recommendation closed when the procedure is implemented by August 31, 2017.

2016-4: Weaknesses in Virginia Call Center Logical Access Management

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

a. Ensure the call center has developed, documented, and implemented procedures for the timely removal of access to the call center LAN after a user no longer requires access and for maintenance of related documentation; and

b. Develop, document, and provide to the call center procedures to require the completion of required Agency agreements, training, and background investigation prior to account creation on the call center LAN.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will ensure that the Virginia call center has developed, documented, and implemented procedures for the timely removal of access to the call center LAN after a user no longer requires access by July 31, 2017.

b. The Agency concurs with the recommendation. The Agency will ensure that the Virginia call center has developed, documented, and implemented procedures to require the completion of required Agency agreements, training, and background investigation prior to account creation on the call center LAN by July 31, 2017.

2016-5: Weakness in Restricting Internet Access at the Call Centers

To strengthen security controls, the Agency should enhance monitoring procedures for periodically reviewing call center internet whitelists to:

a. Ensure that Maryland and Virginia call center management periodically review all allowed internet sites and restrict all unnecessary sites.

b. Specify a process for Agency review and approval of websites for business need and security concerns and prior to call center management allowing access to the websites.

c. Define responsible Agency individuals to periodically review websites allowed at the call centers and the process for documenting and communicating review results to the contracting officer's representative and call center management.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will enhance its monitoring procedures ensure that the call centers will periodically review all allowed internet sites and restrict all unnecessary sites. The Agency will ensure that the procedures are implemented by July 31, 2017.

b. The Agency concurs with the recommendation. The Agency has already implemented procedures for a periodic review of each call centers' whitelist for security concerns; however, at the time of the audit field work evidence could not be provided that indicated the security review had been completed within the scope period. The Agency will ensure these procedures are updated by November 30, 2017.

c. The Agency concurs with the recommendation. The Agency will enhance its existing procedures to ensure that a process is included for the appropriate communication and documentation of any security concerns pertaining to the call center whitelists. The Agency will ensure these procedures are updated by July 31, 2017. The Agency will close this recommendation by November 30, 2017.

2016-6: Incomplete Maryland Call Center Privacy Impact Assessment

The Agency should:

a. Complete the PIA for the Maryland call center; and

b. Identify and document the specific locations that house PII for the Maryland call center in a PII inventory that is secured.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will complete the Maryland call center PIA by July 31, 2017.

b. The Agency concurs with the recommendation. The Agency will finalize its PII Inventory for each system boundary by June 30, 2017.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

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

- *Summary of Thrift Savings Plan*, dated February 2017
- *Written Inquiry Correspondence Summary Reports* for calendar year 2016
- *Written Inquiry Monthly Quality Assurance Report* for the months of February and May 2016
- Listing of Written Inquiries from PSR during calendar year 2016
- *E-Messages Summary Report* for calendar year 2016
- *E-Messages Mailbox Summary Report* for the months of February and May 2016
- *Monthly Congressional Correspondence Summary Report* for calendar year 2016
- OPSTrack Agency Control Log for Congressional Inquiries for all twelve months of calendar year 2016
- *Congressional Correspondence Policy*, dated December 31, 2016
- *Congressional Correspondence Procedures*, dated December 31, 2016
- *Participant Communications Print/Mail Team Procedures*, dated September 30, 2016
- 2015 Annual Statement Content and Print Approvals
- 2016 First and Third Quarter Statements Content and Print Approvals
- Report No. TSP 6017, *Participating Employees by Department Report*, for calendar year 2016
- Report No. TSP 6019, *Returned Mail Summary Report*, for calendar year 2016
- TSP Form Functional Design Documents
- *Participant Communications – OCE Web Calculator Review Desk Procedures*, dated January 31, 2017
- *Participant Communications – Writer/Editor Team Procedures*, dated September 30, 2016
- TSP Payroll and Personnel Agency Meeting Agendas, June and September 2016
- TSP Web Calculators Microsoft Excel Recalculations
- Minutes of the Meeting of the Board Members, January 2016 through March 2017, posted on www.frtib.gov.
- Active Network, Inc. Contract TIB 2008-C-001
- SERCO Services Inc. Contract TIB 2012-C-007
- *Procedures for Adjusting the Distribution of Toll-Free Calls Between Frostburg and Clintwood*, Revised November 25, 2011
- *Enterprise Information Security Risk Management (EISRM) System Authorization Policy*, dated June 29, 2012
- *EISRM Information Assurance Vulnerability Management Policy*, dated June 26, 2013
- *EISRM Access Control Policy*, dated June 29, 2012

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- *EISRM System and Communications Protection Policy*, dated June 29, 2012
- *EISRM Identification and Authentication Policy*, dated June 29, 2012
- *EISRM Media Protection Policy*, dated June 8, 2012
- *EISRM Program Physical and Environmental Security Policy*, dated June 29, 2012
- *EISRM Contingency Planning Policy*, dated June 29, 2012
- Agency's *Limited Personal Use Policy*, dated August 28, 2012
- *The EISRM: Baseline Security Requirements (BLSR),* effective May, 31, 2015
- *Information Assurance Division Plan of Action and Milestones (POA&M) Procedures*, dated April 30, 2016
- *Call Center Procedure Review of Proxy Server Internet Whitelist*, dated November 17, 2016
- Baselined Agency InfoSec Clauses Ownership, Drivers, and Deliverables responsibilities matrix
- *Office of Technology Services (OTS) IT Security Electronic Media Destruction or Sanitization Procedures*, dated January 1, 2015
- *Information Assurance Division (IAD) IT Security Media Destruction or Sanitation Procedures*, dated July 1, 2014
- Call Verification Chart
- Call Center Quality Assurance Plan, dated December 2010
- Quality Assurance Guidelines, dated April 18, 2011

<u>Virginia Call Center Documents and Reports</u>

- Virginia Call Center *Standard Operating Procedures (SOP)*, dated December 19, 2016
- Virginia Call Center LAN Listing as of January 10, 2017
- Virginia Call Center Active Employee Listing as of January 10, 2017
- Virginia Call Center LAN Listing with Creation Dates
- Virginia Call Center Password Requirement Configurations
- Virginia Call Center Internet Whitelist and Blacklist
- Virginia Call Center Termination Listing
- Virginia Call Center Users with Physical Access Profiles
- Virginia Call Center Active Badges from January 1, 2016 to December 31, 2016
- Virginia Call Center Versadial Administrators
- Virginia Call Center Versadial Password Requirements
- Virginia Call Center Destruction Certificate, dated December 20, 2016
- Virginia Call Center 2016 Monthly Quality Assurance Summaries

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- Virginia Call Center Sophos Safeguard Configuration Settings
- Virginia Call Center Monthly Summary Report – June and September 2016
- Virginia Call Center Call Back Monthly Reports – June 2016 and September 2016
- Virginia Call Center Customer Satisfaction Survey - June and September 2016

Maryland Call Center Documents and Reports

- Maryland Call Center SOP 13.4, *Disposal of Hardware at Frostburg Call Center*
- Maryland Call Center SOP 13.9, *New Hire Events & Background Investigations*
- Maryland Call Center SOP 13.10, *Termination, Transfer and System Access Procedures*
- Maryland Call Center SOP Section 13.12, *FRTIB Password Requirements*
- Maryland Call Center SOP 13.14, *Internet, Website and Network Access*
- Maryland Call Center SOP 13.18, *Active Network Procedures - Physical Access Frostburg, MD Facility*
- Maryland Call Center LAN listing with Creation Dates January 20, 2017
- Maryland Call Center New Employees January 1, 2016 – December 20, 2016
- Maryland Call Center Terminated Employees January 1, 2016 – December 31, 2016
- Maryland Call Center Firewall Rules Restricting Internet Access
- Maryland Call Center 3rd Quarter Whitelist Review
- Maryland Call Center 3rd Quarter LAN Access Review
- Maryland Call Center 4th Quarter LAN Access Review
- Maryland Call Center USB/CD Drive Restriction Configuration Settings
- Maryland Call Center Call Center Physical Access Listings
- Maryland Call Center Physical Access Recertification
- Maryland Call Center Visitor Log for December 20, 2016
- Maryland Call Center Privacy Training Evidence
- Maryland Call Center Software Version Screenshots
- Electronic Sanitization Request Form, dated December 2, 2014
- Active Network Sanitization Document, dated January 20, 2015
- *Maryland Call Center Versadial Procedures*, dated November 4, 2015
- Maryland Call Center Destruction Certificate, dated May 20, 2015
- Maryland Call Center Response and Notification Procedures, dated July 24, 2013
- Maryland Call Center 2016 Monthly Quality Assurance Summaries
- Maryland Call Center Monthly Summary Report – June and September 2016
- Maryland Call Center Password Requirement Configurations