KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Participant Website Controls

September 9, 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

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

As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit of the Thrift Savings Plan (TSP) participant website controls. Our audit was performed remotely from March 25, 2021 through July 23, 2021. Our scope period for testing was April 1, 2020 through March 31, 2021.

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 Special Publication 800-53, Revision 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 website controls were to:

- Determine whether the Agency implemented certain procedures to (1) secure participant communications and transactions via the Web through password and user identification configurations settings, system edits check regarding certain indicative data updates, and transaction types, and (2) manage website configurations changes.

- Determine whether the Agency implemented certain procedures over participant website changes that occurred during the coronavirus pandemic.

- Assess the status of all open prior year recommendations in this area.

We present two new findings and recommendations related to TSP participant website controls, both 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. The recommendations are intended to strengthen TSP participant website controls. 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 April 1, 2020 through March 31, 2021, the Agency implemented certain procedures to (1) secure participant communications and transactions via the Web through password and user identification configuration settings, system edits check regarding certain indicative data updates, and transaction types, and (2) manage website configuration changes. In addition, we concluded that for the period April 1, 2020 through March 31, 2021, the Agency implemented certain content changes to the Participant Website that supported its response to the coronavirus pandemic. However, we noted internal control weaknesses in certain TSP Participant Website controls.

We also reviewed six prior U.S. Department of Labor Employee Benefits Security Administration (EBSA) recommendations related to TSP Participant Website controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, three recommendations have been implemented and closed, two recommendations have been partially implemented and closed, and one recommendation was not implemented but was closed.

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

---

[1] *Government Auditing Standards* section 8.15 defines significance in the context of a performance audit.

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

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

KPMG LLP

September 9, 2021

II. OBJECTIVES, SCOPE AND METHODOLOGY

A. Objectives

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 website controls.

The objectives of this performance audit were to:

- Determine whether the Agency implemented certain procedures to (1) secure participant communications and transactions via the Web through password and user identification configurations settings, system edits check regarding certain indicative data updates, and transaction types, and (2) manage website configurations changes.

- Determine whether the Agency implemented certain procedures over participant website changes that occurred during the coronavirus pandemic.

- Assess the status of all open prior year recommendations in this area.

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 April 1, 2020 through March 31, 2021. 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 in developing a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with TSP IT operations management. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we performed the following procedures related to the TSP participant website controls to achieve our audit objectives:

- Conducted interviews;
- Participated in process walk-throughs for daily monitoring of the TSP accounts and My Account website;
- Reviewed changes on the TSP.gov and My Account websites to determine if they were approved by management prior to migration into production;
- Inspected documentation on access to modify the TSP.gov website for evidence of approval and appropriateness;
- Inspected evidence of daily validation controls over participant data loaded to the MyAccount website;
- Participated in process walk-throughs for the My Account web application scans;
- Inspected evidence on network traffic for the My Account website; and
- Collected and inspected evidence on the TSP.gov website cryptographic session reviews.

We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, D.C. and the Agency's contractor's location in Virginia. In Appendix B, we identify the key documentation provided by Agency personnel that we reviewed during our performance audit. Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the samples we tested and were not extrapolated to the population.

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 Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

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.

This report contains Sensitive Information and will not be posted.