



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Insider Threat Controls

July 23, 2020

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND INSIDER THREAT CONTROLS	
A. The Thrift Savings Plan	I.1
B. Insider Threat Controls Program	I.1
II. OBJECTIVES, SCOPE AND METHODOLOGY	
A. Objectives	II.1
B. Scope and Methodology	II.1
III. FINDINGS AND RECOMMENDATIONS	
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Reports.....	III.2
C. Summary of Open Recommendations	III.4
 <u>Appendices</u>	
A. Agency's Response.....	A.1
B. Key Documentation and Reports Reviewed.....	B.1

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) insider threat controls. Our fieldwork was performed remotely from March 23, 2020 through May 15, 2020, in coordination with personnel primarily from the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was May 1, 2019 through April 30, 2020.

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 objectives. Criteria used for this audit is 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 objectives of our audit over the TSP insider threat controls were to:

- Determine whether the Agency implemented certain controls to prevent, monitor, and detect insider threats to TSP systems and data by Agency personnel and contractors; and
- Perform limited social engineering procedures to test for the existence of insider threat controls.

However, based on Agency management’s security concerns, we were not granted access to Agency facilities for purposes of performing the limited social engineering procedures. As such, we were not able to meet the second audit objective listed above. This situation was discussed promptly with EBSA, and EBSA directed us to complete the audit with the first audit objective only.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objective. We conclude that for the period May 1, 2019 through April 30, 2020, the Agency did not implement certain controls to prevent, monitor, and detect insider threats to TSP systems and data by Agency personnel and contractors. We noted that previously-identified internal control weaknesses continued to exist in all areas of TSP insider threat controls within our audit objective.

We also reviewed two prior EBSA recommendations related to TSP insider threat controls, both of which address fundamental controls, to determine their current status. Fundamental control recommendations address significant¹ 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. Section III.B documents the status of these prior recommendations. In summary, one recommendation has been partially implemented and remains open, and one recommendation has not been implemented and remains open. The Agency’s response to these recommendations is included as an appendix within the report (Appendix A). The Agency concurred with both recommendations. Based on the status of these prior EBSA recommendations and the implementation status of the TSP insider threat program, the current engagement produced no new recommendations.

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

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

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

July 23, 2020

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) insider threat controls at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objectives of this performance audit were to:

- Determine whether the Agency implemented certain controls to prevent, monitor, and detect insider threats to TSP systems and data by Agency personnel and contractors; and
- Perform limited social engineering procedures to test for the existence of insider threat controls.

However, based on Agency management's security concerns, we were not granted access to Agency facilities for purposes of performing the limited social engineering procedures. As such, we were not able to meet the second audit objective listed above. This situation was discussed promptly with EBSA, and EBSA directed us to complete the audit with the first audit objective only.

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 May 1, 2019 through April 30, 2020. 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 the TSP insider threat program. 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 to achieve our audit objectives:

- Conducted interviews; and
- Collected and inspected auditee-provided documentation and evidence.

We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, D.C. In Appendix B, we identify the key documentation provided by Agency personnel that we reviewed during our performance audit.

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.**