



Employee Benefits Security Administration

**Performance Audit over the
Thrift Savings Plan**

Risk Management and Vendor Management

May 11, 2022

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP, RISK MANAGEMENT, AND VENDOR MANAGEMENT	
A. The Thrift Savings Plan	I.1
B. TSP System.....	I.1
C. Certain Other New Vendors and Service Providers	I.2
D. Risk Management and Vendor Management.....	I.3
II. OBJECTIVE, SCOPE AND METHODOLOGY	
A. Objective	II.1
B. Scope and Methodology	II.1
III. FINDINGS AND RECOMMENDATIONS	
A. Introduction.....	III.1
 <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 over the Thrift Savings Plan (TSP) risk management and vendor management controls. Our audit was performed remotely from December 15, 2021 through March 11, 2022, in coordination with personnel primarily from the Federal Retirement Thrift Investment Board's Staff (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2021 through December 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' (AICPA) *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 (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our audit over TSP risk management and vendor management controls were to determine whether the Agency implemented certain procedures to (1) assess risks related to the new vendors and service providers in accordance with applicable NIST guidance; (2) properly categorize, authorize, and monitor the new vendors and service providers systems in accordance with applicable NIST guidance; and (3) assess new vendors and service providers against key

contractual and service level agreement requirements related to information technology (IT) security.

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, 2021 through December 31, 2021, the Agency implemented certain procedures to (1) assess risks related to the new vendors and service providers in accordance with applicable NIST guidance; (2) properly categorize, authorize, and monitor the new vendors and service providers systems in accordance with applicable NIST guidance; and (3) assess new vendors and service providers against key contractual and service level agreement requirements related to IT security.

No prior findings or recommendations were within the scope of this audit, and the current engagement produced no new findings or recommendations. The Agency's response to this report, including the Executive Director's formal reply, is included as Appendix A.

This performance audit did not constitute an audit of the TSP's financial statements or an attestation engagement as defined by *Government Auditing Standards* and the AICPA standards for attestation engagements. 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

May 11, 2022

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 over the Thrift Savings Plan (TSP) risk management and vendor management at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency).

The objectives of this performance audit were to determine whether the Agency implemented certain procedures to (1) assess risks related to the new vendors and service providers in accordance with applicable National Institute of Standards and Technology (NIST) guidance; (2) properly categorize, authorize, and monitor the new vendors and service providers systems in accordance with applicable NIST guidance; and (3) assess new vendors and service providers against key contractual and service level agreement requirements related to information technology security.

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, 2021 through December 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 risk management and vendor management. During the planning phase, we inquired of Agency management and reviewed Board meeting minutes to identify and select new Agency vendors and service providers. We designed test procedures to evaluate whether the Agency designed and implemented procedures for assessing risk to vendors and for categorizing, authorizing, and monitoring systems. We also designed procedures to evaluate Agency contract oversight and assessment of key contractual requirements for certain vendors. 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 TSP risk management and vendor management to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected documentation provided by the Agency and in-scope vendors and service providers;
- Inspected applicable contracts and procedures related to the new TSP recordkeeping system, services provided by the Department of Justice, and services provided by the Department of the Interior's Interior Business Center;
- Inspected Agency policies that established the requirements for risk management and vendor management; and
- Inspected Agency risk management and system authorization documentation.

Our testing considered controls in areas such as risk management, supply chain risk management, information security planning, categorization, authorization, control assessment, plans of actions and milestones, information security continuous monitoring, configuration management, and vulnerability management. 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 and the in-scope vendors and service providers 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 NIST Special Publication 800-53, Revision 5, *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.**