



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Information Protection Processes and Procedures

June 4, 2025

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
I. BACKGROUND OF THE TSP AND INFORMATION PROTECTION PROCESSES AND PROCEDURES.....	I.1
A. The Thrift Savings Plan	I.1
B. TSP System.....	I.1
C. Information Protection Processes and Procedures Overview	I.2
II. OBJECTIVES, SCOPE, AND METHODOLOGY.....	II.1
A. Objectives	II.1
B. Scope and Methodology	II.1
III. FINDINGS AND RECOMMENDATIONS	III.1
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Reports.....	III.2
 <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.

Acting 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 information protection processes and procedures for the Thrift Savings Plan (TSP) recordkeeping system. Our fieldwork was performed remotely from November 15, 2024, through March 21, 2025, in coordination with personnel primarily from the Federal Retirement Thrift Investment Board Staff's (Agency) headquarters in Washington, D.C., including their vendor support personnel. Our scope period for testing was March 1, 2024, through February 28, 2025.

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 are defined in the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

The objectives of our audit over TSP information protection processes and procedures were to determine whether the Agency and its vendor implemented certain procedures to: (1) maintain and manage the protection of information systems and assets through configuration management, backup and recovery, and personnel security; (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information (i.e., data security and encryption of data at rest and in transit); and (3) evaluate vendor contractual compliance with its data and privacy protection contractual provisions.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period March 1, 2024, through February 28, 2025, the Agency and its vendor implemented certain procedures to (1) maintain and manage the protection of information systems and assets through configuration management, backup and recovery, and personnel security; (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information (i.e., data security and encryption of data at rest and in transit); and (3) evaluate vendor contractual compliance with its data and privacy protection contractual provisions.

The current engagement produced no new findings or recommendations.

We also reviewed three prior EBSA recommendations related to TSP information protection processes and procedures to determine their current status. Section III.B documents the status of these prior recommendations. In summary, all three recommendations have been implemented and closed.

The Agency's formal response to the draft report is included as an appendix within this report (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

June 4, 2025

II. OBJECTIVES, SCOPE, AND METHODOLOGY

A. Objectives

The U.S. Department of Labor Employee Benefits Security Administration (EBSA) engaged KPMG LLP to conduct a performance audit over the Thrift Savings Plan (TSP) information protection processes and procedures.

The objectives of this performance audit were to determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) and its vendor implemented certain procedures to: (1) maintain and manage the protection of information systems and assets through configuration management, backup and recovery, and personnel security; (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information (i.e., data security and encryption of data at rest and in transit); and (3) evaluate vendor contractual compliance with its data and privacy protection contractual provisions.

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 March 1, 2024, through February 28, 2025. We performed the audit in four phases: (1) planning, (2) arranging for engagement with the Agency, (3) testing and interviewing, and (4) report writing.

During the planning phase, team members developed a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with TSP information protection processes and procedures. 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 walkthroughs, and designed and performed tests of information technology controls. Our performance audit procedures related to TSP information protection processes and procedures covered the period of March 1, 2024, through February 28, 2025, and included the following procedures to achieve our audit objectives:

- Inspected applicable contracts and procedures for information technology support services;
- Inspected policies that established the requirements for information protection control processes;
- Inspected procedures and plans that documented information protection control processes implemented to comply with established requirements;
- Inspected baseline configuration settings for the Converge system;
- Inspected procedures that documented software development lifecycle and change management processes to comply with established requirements;
- Inspected information backup configuration settings;
- Inspected recovery policies and procedures implemented and tested recovery processes by inspecting the results of the most recent recovery plan exercise and the updates and lessons learned that were documented as a result of the test;
- Tested a sample of Converge new employees/contractors during the audit scope period to determine whether proper screening was conducted and documented prior to those individuals beginning work on the Converge system in accordance with established requirements;
- Tested a sample of configuration changes during the audit scope period to determine whether configuration change policies and procedures were followed in accordance with established requirements; and
- Tested a sample of dates for backups that occurred during the audit scope period to determine whether each backup job ran successfully and for those that did not, whether the job was investigated and the subsequent backup was successfully run.

We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, DC and its vendor's headquarters in Arlington, VA. Appendix B lists the key documentation and reports we reviewed during our performance audit. Because we used non-statistically determined sample sizes in our procedures, our results are applicable to the sample items 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 National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for 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.**