KPMG

Employee Benefits Security Administration

Performance Audit of the
Thrift Savings Plan
Vendor Risk Management and Oversight Controls

July 25, 2025

TABLE OF CONTENTS

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 related to vendor risk management and oversight controls for the Thrift Savings Plan (TSP). Our fieldwork was performed remotely from January 16, 2025, through April 15, 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 January 1, 2024, through December 31, 2024.

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 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 objectives of our performance audit over vendor risk management and Agency oversight controls were to:

- Determine whether the Agency implemented certain procedures to assess the Converge vendor against key contractual and service level agreement requirements related to information technology security, to include a review of the continuous monitoring policies and procedures

related to the multiple Federal Risk and Authorization Management Program (FedRAMP) services; and

- Determine whether the Agency and its Converge vendor implemented certain procedures to: (1) assess and monitor the implementation of security controls for Converge and its subsystems; (2) authorize Converge and its subsystems; and (3) establish, document, and implement privacy controls to protect TSP data by third-party vendors.

We present three new findings and related recommendations, one of which addresses fundamental controls. Fundamental control findings and 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 findings and recommendations address procedures or processes that are less significant than fundamental controls. These recommendations are intended to strengthen the TSP vendor risk management process. The Agency should review and consider these recommendations for timely implementation. Section III.C includes 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, 2024, through December 31, 2024:

1. The Agency implemented certain procedures to assess the Converge vendor against key contractual and service level agreement requirements related to information technology security.
2. No specific key contractual or service level agreement requirements were in place for continuous monitoring policies and procedures as they relate to the multiple FedRAMP services; as such, Agency procedures for monitoring such requirements were not necessary.
3. The Agency and its Converge vendor implemented certain procedures to: (1) assess and monitor the implementation of security controls for Converge and its subsystems; (2) authorize Converge and its subsystems; and (3) establish, document, and implement privacy controls to protect TSP data by third-party vendors.

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

However, as indicated above, we noted internal control weaknesses in certain areas of TSP vendor risk management within our audit objectives.

We also reviewed three prior EBSA recommendations related to vendor risk management controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, two recommendations have been implemented and closed, and one recommendation has been partially implemented and remains open.

The Agency's response to the recommendations, including the Executive Director's formal reply, is included as an appendix within the report (Appendix A). The Agency concurred with all recommendations, except for the following:

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

July 25, 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 related to vendor risk management and oversight controls for the Thrift Savings Plan (TSP) at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objectives for this performance audit were to:

- Determine whether the Agency implemented certain procedures to assess the Converge vendor against key contractual and service level agreement requirements related to information technology security, to include a review of the continuous monitoring policies and procedures related to the multiple Federal Risk and Authorization Management Program (FedRAMP) services; and

- Determine whether the Agency and its Converge vendor implemented certain procedures to: (1) assess and monitor the implementation of security controls for Converge and its subsystems; (2) authorize Converge and its subsystems; and (3) establish, document, and implement privacy controls to protect TSP data by third-party vendors.

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, 2024, through December 31, 2024. 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 processes and personnel involved with vendor risk management and oversight controls. 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 controls. Our performance audit procedures included using random attribute sampling to select samples from the following populations related to TSP vendor risk management and oversight controls for the period of January 1, 2024, through December 31, 2024, which we used to determine if such controls operated effectively during the period:

- Contractual Deliverables, Service Level Agreements, and Key Performance Indicators documented during the period of January 1, 2024, through December 31, 2024;
- Security Control Assessments documented during the period of January 1, 2024, through December 31, 2024;
- Plans of Action and Milestones documented during the period of January 1, 2024, through December 31, 2024;
- System Authorizations documented during the period of January 1, 2024, through December 31, 2024; and
- [redacted] documented during the period of January 1, 2024, through December 31, 2024.

We conducted these test procedures remotely in coordination with personnel 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.