KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Access and Data Security Controls

May 14, 2025

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

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 access and data security controls for the Thrift Savings Plan (TSP) recordkeeping system (TSP system or Converge). Our fieldwork was performed remotely from November 15, 2024, through March 7, 2025, in coordination with personnel from the Federal Retirement Thrift Investment Board's Staff (Agency) and its vendor. 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 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 audit over Converge access and data security controls were to determine whether the Agency and its vendor implemented certain procedures to: (1) authenticate users for Converge and its subsystems; (2) limit logical access to Converge and its subsystems to approved users and services; and (3) restrict and manage access to the identity and access management solution.

We present one new finding and two related recommendations, which address a fundamental control. 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. These recommendations are intended to strengthen Converge access and data security controls. The Agency should review and consider these recommendations for timely implementation. Section III.C presents the details that support the current year finding 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 March 1, 2024, through February 28, 2025, the Agency and its vendor implemented certain procedures to (1) authenticate users for Converge and its subsystems; (2) limit logical access to Converge and its subsystems to approved users and services; and (3) restrict and manage access to the identity and access management solution. However, as indicated above, we noted internal control weaknesses in certain areas of Converge access and data security controls within our audit objectives.

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

The Agency's response 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. Additionally, in the response, the Agency identified certain completed remediation action and indicated that management had provided us with evidence of action taken. As remediation was completed subsequent to the end of the scope period, we did not perform procedures over the evidence provided and therefore did not adjust the finding or recommendation language.

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

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

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 14, 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 access and data security controls for the Thrift Savings Plan (TSP) recordkeeping system (TSP system or Converge).

The objectives of our audit over Converge access and data security controls were to determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) and its vendor implemented certain procedures to: (1) authenticate users for Converge and its subsystems; (2) limit logical access to Converge and its subsystems to approved users and services; and (3) restrict and manage access to the identity and access management solution.

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 Converge access and data security 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 information technology (IT) controls. Our performance audit procedures included using random attribute sampling to select samples from the following populations related to Converge access and data security controls for the period March 1, 2024, through February 28, 2025, which we used to determine if Converge access and data security controls operated effectively during the period:

- New administrative accounts created during the period March 1, 2024, through February 28, 2025;
- New service accounts created during the period March 1, 2024, through February 28, 2025;

- New temporary accounts created during the period March 1, 2024, through February 28, 2025;
- Accounts deprovisioned during the period March 1, 2024, through February 28, 2025;
- Accounts reviewed and reauthorized during the period March 1, 2024, through February 28, 2025;
- Individuals newly assigned as [redacted] or authorized delegates (i.e., individuals with the responsibility to authorize and reauthorize system access) during the period March 1, 2024, through February 28, 2025; and
- Changes to the [redacted] during the period March 1, 2024, through February 28, 2025.

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*, and 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.