KPMG

Employee Benefits Security Administration

Performance Audit over the Thrift Savings Plan Mobile Device Security and Governance Controls

August 27, 2024

TABLE OF CONTENTS

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) mobile device security and governance controls. Our audit was performed remotely from February 1, 2024, through June 17, 2024, 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 May 1, 2023, through April 30, 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 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 5, *Security and Privacy Controls for Information Systems and Organizations*.

The objectives of our audit over TSP mobile device security and governance controls were to:

- Determine whether the Agency and its TSP recordkeeping systems (Converge) vendor (1) developed a mobile device security and governance program for Agency-managed mobile

devices; (2) established controls for tracking and monitoring Agency-managed mobile devices; (3) established controls for configuring, updating, and removing mobile devices from the Agency's network; (4) developed a mobile device security and governance program for Converge-issued mobile devices; and (5) established controls for configuring, updating, and removing mobile devices from the Converge network.

We present four new findings and recommendations related to TSP mobile device security and governance controls, all of which address fundamental controls. Fundamental control 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. All recommendations are intended to strengthen TSP mobile device security and governance controls. The Agency should review and consider these recommendations for timely implementation. Section III.C presents 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 May 1, 2023, through April 30, 2024, the Agency (1) developed a mobile device security and governance program for Agency-managed mobile devices; (2) established certain controls for tracking and monitoring Agency-managed mobile devices; and (3) established certain controls for configuring, updating, and removing mobile devices from the Agency's network. However, we noted internal control weaknesses in certain areas of TSP mobile device security and governance controls within our audit objectives.

In addition to above audit objectives, we determined that for the period May 1, 2023, through April 30, 2024, the Agency's Converge vendor did not (1) develop a mobile device security and governance program for Converge-issued mobile devices; or (2) establish controls for configuring, updating, and removing mobile devices from the Converge network because such programs and controls were not necessary. We determined that personnel from the Converge vendor were not provided mobile devices with access to mobile applications related to Converge during our scope period.

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

We also reviewed 11 prior EBSA recommendations related to the TSP mobile device security and governance controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, eight recommendations were implemented and closed, two recommendations have been partially implemented and remain open, and one recommendation has not been implemented and remains open.

The Agency's responses to the recommendations are included as an appendix within the report (Appendix A). The Agency concurred with all recommendations, except for the following recommendation:

[redacted]

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

August 27, 2024

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) mobile device security and governance controls.

The objectives of this performance audit were to:

- Determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) and its TSP recordkeeping systems (Converge) vendor (1) developed a mobile device security and governance program for Agency-managed mobile devices; (2) established controls for tracking and monitoring Agency-managed mobile devices; (3) established controls for configuring, updating, and removing mobile devices from the Agency's network; (4) developed a mobile device security and governance program for Converge-issued mobile devices; and (5) established controls for configuring, updating, and removing mobile devices from the Converge network.

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, 2023, through April 30, 2024. 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.

During the planning phase, team members developed a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with the TSP mobile device security and governance controls. 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 mobile device security and governance controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Participated in process walk-throughs for mobile device administration activities and mobile device security and governance monitoring activities;
- Inspected applicable procedures for information technology support services;
- Inspected system documentation for evidence of implementation and ongoing monitoring of mobile devices;
- Inspected the population of mobile device users for evidence of baseline configuration actions, removal activities, and administrative monitoring;
- Inspected the population of mobile device administrators for evidence of least privilege access;
- Inspected a non-statistical sample of terminated employees and contractors for evidence of removal from the Mobile Device Management tool;
- Inspected a non-statistical sample of new mobile device requests for evidence of appropriate approval; and
- Inspected a non-statistical sample of monthly vulnerability reports for evidence of scanning and remediation activities performed over the Mobile Device Management tool.

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 [redacted]. 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.