KPMG

Employee Benefits Security Administration

Performance Audit over the Thrift Savings Plan Mainframe Security and Configuration Controls

August 20, 2024

TABLE OF CONTENTS

Section Page

EXECUTIVE SUMMARY i

I. BACKGROUND OF THE TSP AND MAINFRAME SECURITY AND CONFIGURATIONS I.1

A. The Thrift Savings Plan I.1

B. TSP System I.1

C. Mainframe Security and Configuration Controls 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. Introductions III.1

B. 2024 Findings III.1

C. Other Results III.3

Appendices

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 of the security and configuration controls for the Thrift Savings Plan (TSP) mainframe. Our audit was performed remotely from January 22, 2024, through May 24, 2024, in coordination with personnel primarily from the Federal Retirement Thrift Investment Board's Staff (Agency) headquarters in Washington, D.C, including their vendor support personnel. Our scope period for testing was April 1, 2023, through March 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 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 performance audit over the TSP mainframe configuration and security controls were to determine whether the Agency and its vendor established, documented, and implemented certain controls related to: (1) monitoring and configuring the mainframe operating system; (2) access administration and separation of duties for the mainframe; and (3) mainframe boundary protection.

We present one new finding without a recommendation, which addresses a fundamental control. Fundamental controls 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. Section III.B presents the details that support the current year finding.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period April 1, 2023, to March 31, 2024, the Agency and its vendor established, documented, and implemented certain controls related to: (1) monitoring and configuring the mainframe operating system; (2) access administration and separation of duties for the mainframe; and (3) mainframe boundary protection. However, as indicated above, we noted an internal control weakness in certain areas of TSP mainframe security and configuration controls within our audit objectives.

The Agency's response to the report is included as an appendix within the 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

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

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 20, 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 security and configuration controls for the Thrift Savings Plan (TSP) mainframe at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objectives of this performance audit were to determine whether the Agency and its vendor established, documented, and implemented controls related to: (1) monitoring and configuring the mainframe operating system; (2) access administration and separation of duties for the mainframe; and (3) mainframe boundary protection.

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 April 1, 2023, through March 31, 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.

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 the TSP mainframe. Arranging for 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 mainframe security and configuration controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Inspected policies and procedures that established requirements related to mainframe security and configuration controls, including but not limited to batch and interface jobs, access controls, and segregations of duties;

- Tested a non-statistical sample of failed batch jobs to determine whether job failures were monitored and resolved;
- Tested a non-statistical sample of changes made to the configurations or functionality of mainframe batch jobs to determine whether changes to jobs were approved; and
- Tested a non-statistical sample of new or modified users, terminated users, and user access reviews to determine whether access to the mainframe was approved, reviewed, and removed timely after termination.

We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, D.C. 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 sampling procedures, our results are applicable to the samples 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 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.