Employee Benefits Security Administration

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

December 7, 2018

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 Benefit 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) mainframe configuration and security controls. Our fieldwork was performed from February 1, 2018 through August 17, 2018, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was March 1, 2017 through February 28, 2018, and additionally included testing following the Agency's data center outage on March 2, 2018.

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 *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 the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our audit over the TSP mainframe configuration and security controls were to:

- Determine whether the Agency established, documented and implemented certain controls to (1) monitor and configure the operating system and hardware; (2) administer access and segregation of duties for the mainframe; and (3) detect unauthorized data mining.

- Determine the status of the prior EBSA TSP mainframe configuration and security controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls,* dated May 8, 2017.

We present two new findings and recommendations related to TSP mainframe configuration and security controls, one of which address fundamental controls and the other that addresses other 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. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen the TSP mainframe configuration and security 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 March 1, 2017 through February 28, 2018, the Agency (1) did not establish, document, and implement certain controls to monitor and configure the operating system and hardware; (2) did not establish, document, and implement certain controls to administer segregation of duties for the mainframe, or detect unauthorized data mining; and (3) did establish, document and implement certain controls for administering access to the mainframe. As a result, we noted internal control weaknesses in certain areas of TSP mainframe configuration and security controls within our audit objectives.

We also reviewed 24 prior EBSA recommendations related to the TSP mainframe configuration to determine their current status. Section III.B documents the status of these prior recommendations. In summary, two recommendations were implemented and closed, 10 recommendations were partially implemented and remain open, and 12 recommendations were not implemented and remain open.

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

---

1 *Government Auditing Standards* section 6.04 defines significance in the context of a performance audit.

[redacted]

[redacted]

[redacted]

This performance audit did not constitute an audit of the TSP's financial statements in accordance with *Government Auditing Standards.* 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.

This report contains detailed information about mainframe weaknesses, the misuse of which could cause potential damage if made publicly available. As such, in accordance with *Government Auditing Standards*, this report is considered a limited use report and is intended solely for the information and use of the U.S. Department of Labor Employee Benefit 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

December 7, 2018

II. OBJECTIVE, 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) mainframe configuration.

The objectives of our audit over the TSP mainframe configuration and security controls were to:

- Determine whether the Agency established, documented and implemented controls to (1) monitor and configure the operating system and hardware; (2) administer access and segregation of duties for the mainframe; and (3) detect unauthorized data mining; and

- Determine the status of the prior ESA TSP mainframe configuration and security controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls,* dated May 8, 2017.

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 July 1, 2015 through June 30, 2016. 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 to develop a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with the TSP mainframe configuration. 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 the TSP mainframe configuration and security controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Participated in process walk-throughs for access and configuration management, data exfiltration monitoring and protection, and services security management;
- Inspected applicable contracts and procedures for IT support services;
- Inspected applicable mainframe configuration settings and privileged access;
- Inspected a [redacted] sample of new mainframe user accounts for evidence of approval;
- Inspected a [redacted] sample of terminated employees for evidence of removal from the mainframe; and
- Inspected a [redacted] sample of mainframe change requests for evidence of approval and testing.

We conducted these test procedures primarily at Agency headquarters [redacted] and at the Agency's contractor's location [redacted]. In Appendix B, we identify the key documentation provided by Agency personnel that 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.

Testing procedures were based on the objectives and control areas for information security and access controls in the Government Accountability Office's *Federal Information System Controls Audit Manual*. In addition, the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, was used to evaluate the status of the Agency's control environment.

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.