KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls

June 7, 2019

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) systems enhancement and software change controls. Our fieldwork was performed from November 20, 2019 through March 8, 2019, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2018 through December 31, 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 at the Agency over the TSP systems enhancement and software change controls were to:

- Determine whether the Agency implemented certain procedures to: (1) control the development, alteration, and configuration of TSP software applications and supporting infrastructure; (2) authorize, test, approve, and implement changes to existing software applications and supporting infrastructure; and (3) control the processes for creating, storing, and accessing TSP production data used to test application changes.

(A&A) process. However, management did not provide the risk assessment and categorization of sensitive data on non-production environments, and the A&A documentation did not specify that it included non—production environments for all in-scope systems. As such, we did not revise the status of this recommendation.

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.

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 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

June 7, 2019

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) systems enhancement and software change controls.

The objectives of our performance audit were to:

- Determine whether the Agency implemented certain procedures to: (1) control the development, alteration, and configuration of TSP software applications; (2) authorize, test, approve, and implement changes to existing software applications; and (3) control the processes for creating, storing, and accessing TSP production data used to test application changes.

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls,* dated June 17, 2016.

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, 2018 through December 31, 2018. 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 systems enhancement and software change 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 to achieve our audit objectives:

- Conducted interviews;
- Participated in process walk-throughs for configuration management program activities, IT asset configuration and identification, system enhancement and change control activities, and separation of duties;
- Inspected applicable contracts and procedures for information technology support services;
- Inspected policies that established the requirements for a standardized systems enhancement and change control process;
- Inspected the manuals that documented systems enhancement and change control process and procedures;
- Collected and inspected auditee-provided documentation and evidence;
- Tested a [redacted] of application change requests and system change requests for certain systems to determine if those requests were created and updated according to Agency configuration management policy requirements;
- Tested a [redacted] of emergency change requests to determine if those requests were created and updated according to Agency configuration management policy requirements; and
- Tested a [redacted] sample of new hires and separated individuals with access to TSP source code repositories to assess the enforcement of access controls and separation of duties.

We conducted these test procedures primarily at Agency headquarters [redacted] and at the Agency's contractor's location in [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.

Criteria used for this engagement are defined in 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 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.