KPMG

Employee Benefits Security Administration

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

April 26, 2021

TABLE OF CONTENTS

Section Page

EXECUTIVE SUMMARY i

I. BACKGROUND OF THE TSP AND SYSTEMS ENHANCEMENT AND SOFTWARE CHANGE CONTROLS

A. The Thrift Savings Plan I.1

B. TSP System I.1

C. Systems Enhancement and Software Change Controls Overview I.2

II. OBJECTIVES, SCOPE AND METHODOLOGY

A. Objectives II.1

B. Scope and Methodology II.1

III. FINDINGS AND RECOMMENDATIONS

A. Introduction III.1

B. Findings and Recommendations from Prior Reports III.2

C. 2021 Findings and Recommendations III.21

D. Summary of Open Recommendations III.24

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 Thrift Savings Plan (TSP) systems enhancement and software change controls. Our audit was performed remotely from November 16, 2020 through February 19, 2021. Our scope period for testing was January 1, 2020 through December 31, 2020.

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 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 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.

- Determine whether the Agency implemented certain procedures over system enhancements and software changes that supported its response to the coronavirus pandemic.

- Determine the status of the prior EBSA TSP systems enhancement and software change controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019, and the following prior year recommendations reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls,* dated July 30, 2012:

    - No. 2011-3: Lack of a Vulnerability Management Program, and
    - No. 2011-4: Lack of a Configuration Management Program.

We present two new findings and recommendations related to TSP systems enhancement and software change controls, both 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. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen TSP systems enhancement and software change 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 January 1, 2020 through December 31, 2020, 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. In addition, we conclude that for the period January 1, 2020 through December 31, 2020, the Agency implemented certain procedures over system enhancements and software changes that supported its response to the coronavirus pandemic. However, we noted internal control weaknesses in certain areas of TSP systems enhancement and software change controls within our audit objectives.

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

We also reviewed 14 prior EBSA recommendations related to TSP systems enhancement and software change controls to determine their current status. In addition to the 12 open recommendations reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019, the following prior year recommendations reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated July 30, 2012, were in scope for this performance audit:

- No. 2011-3: Lack of a Vulnerability Management Program, and
- No. 2011-4: Lack of a Configuration Management Program.

Section III.B documents the status of these prior recommendations. In summary, six recommendations have been implemented and closed, one recommendation has been partially implemented but is considered closed, and seven recommendations have been partially implemented and remain open.

The Agency's responses 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.

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 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

April 26, 2021

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) systems enhancement and software change controls at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objectives of this performance audit 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.

- Determine whether the Agency implemented certain procedures over system enhancements and software changes that supported its response to the coronavirus pandemic.

- Determine the status of the prior EBSA TSP systems enhancement and software change controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls,* dated June 7, 2019, and the following prior year recommendations reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls,* dated July 30, 2012:

    - No. 2011-3: Lack of a Vulnerability Management Program, and
    - No. 2011-4: Lack of a Configuration Management Program.

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, 2020 through December 31,

2020. 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 TSP 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 remotely performed the following procedures related to the TSP systems enhancement and software change controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- 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;
- Tested a non-statistical sample 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 non-statistical sample of emergency change requests to determine if those requests were created and updated according to Agency configuration management policy requirements;
- Tested a non-statistical sample of application change requests and system change requests, including emergency change requests, for certain systems that supported the Agency's response to the coronavirus pandemic to determine if those requests were created and updated according to Agency configuration management policy requirements;
- Tested a non-statistical 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; and

- Tested a non-statistical sample of individuals with access to TSP test data to assess the enforcement of access controls and the principle of least privilege.

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 NIST SP 800-53, Rev. 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.