



Employee Benefits Security Administration

**Performance Audit over the
Thrift Savings Plan
Status of Certain Prior Year Findings**

September 15, 2023

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND PRIOR YEAR TSP RECOMMENDATIONS.....	I.1
A. The Thrift Savings Plan	I.1
B. TSP System.....	I.1
C. Prior Year TSP Audit Recommendations.....	I.2
II. OBJECTIVES, SCOPE, AND METHODOLOGY	II.1
A. Objectives	II.1
B. Scope and Methodology	II.3
III. FINDINGS AND RECOMMENDATIONS	III.1
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Reports.....	III.6
C. 2023 Findings and Recommendations	III.68
D. Summary of Open Recommendations	III.72
E. Summary of Recommendations Closed in This Report.....	III.73
 <u>Appendices</u>	
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 over the status of certain prior year findings for the Thrift Savings Plan (TSP). Our audit was performed remotely from February 8, 2023, through June 9, 2023. Our scope period for testing was June 1, 2022, through June 9, 2023.

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 audit over the status of certain prior year findings for the TSP were to:

- Determine and validate whether recommendations that the Federal Retirement Thrift Investment Board's Staff (Agency) views as effectively resolved have been resolved; and

- Conduct procedures over certain prior year recommendations to determine whether each recommendation has been closed, partially closed, or remains open (or may have been potentially overtaken by events).

We reviewed the following 65 prior EBSA recommendations related to the TSP that the Agency identified as closed to determine their current status:

- Recommendation No. 2010-01, reported in *Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings*, dated July 30, 2010;
- Recommendation No. 2013-03, reported in *Performance Audit of the Thrift Savings Plan System Enhancements and Software Change Controls*, dated November 27, 2013;
- Recommendation Nos. 2019-02a and b and 2019-03, reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019;
- Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated April 26, 2021;
- Recommendation Nos. 2015-03 and 2015-07b, reported in *Performance Audit of the Thrift Savings Plan IT Operations Controls*, dated July 13, 2016;
- Recommendation Nos. 2019-05, 2019-06a, and 2019-07, reported in *Performance Audit of the Thrift Savings Plan IT Operations Controls*, dated August 30, 2019;
- Recommendation No. 2007-03c, reported in *Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System*, dated March 30, 2007;
- Recommendation No. 2011-01b, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated July 30, 2012;
- Recommendation No. 2013-01, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated August 16, 2013;
- Recommendation Nos. 2015-01, 2015-02, 2015-04, 2015-05a, and 2015-10, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated July 17, 2015;
- Recommendation Nos. 2016-02a, c, and d; 2016-04a, b, and e; 2016-08; and 2016-09, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017;
- Recommendation No. 2017-03, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018;
- Recommendation No. 2013-03a, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated March 26, 2014;

- Recommendation Nos. 2013-01f and h, 2013-02a and b, 2013-03, 2013-04, 2013-06b, and 2013-08a and b, reported in *Performance Audit of Thrift Savings Plan Service Continuity Controls*, dated March 26, 2014;
- Recommendation Nos. 2016-02 and 2016-05b, c, and d, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated January 31, 2017;
- Recommendation Nos. 2019-02, 2019-03 2019-04, 2019-06, and 2019-07, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated August 22, 2019;
- Recommendation No. 2021-02, reported in *Performance Audit of the Thrift Savings Plan Participant Website Controls*, dated September 9, 2021;
- Recommendation Nos. 2014-01; 2014-02a, b, and d; 2014-03; 2014-05; and 2014-06, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration Management*, dated April 15, 2015;
- Recommendation Nos. 2016-01; 2016-02; 2016-03b; 2016-04; 2016-05; 2016-06a and b; 2016-07a, c, and d; 2016-08; 2016-09c; 2016-10 b and c; 2016-13; 2016-14a. b. and c; 2016-16; and 2016-17, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls*, dated May 8, 2017;
- Recommendation Nos. 2018-01 and 2018-02, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls*, dated December 7, 2018;
- Recommendation Nos. 2016-01, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Audit Recommendations*, dated April 26, 2017;
- Recommendation Nos. 2019-01b and 2019-02a, reported in *Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations*, dated September 6, 2019;
- Recommendation No. 2020-02, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020; and
- Recommendation Nos. 2018-01 and 2018-02, reported in *Performance Audit of Certain General Information Technology Controls at Thrift Savings Plan Remote Contractor Sites*, dated October 4, 2018.

We present three new findings and recommendations related to the Agency’s processes for enforcing or extending deadlines for the remediation of prior year findings, establishing business continuity planning standards, and tracking media for destruction and sanitization, all of which address fundamental controls. Fundamental control recommendations address significant¹

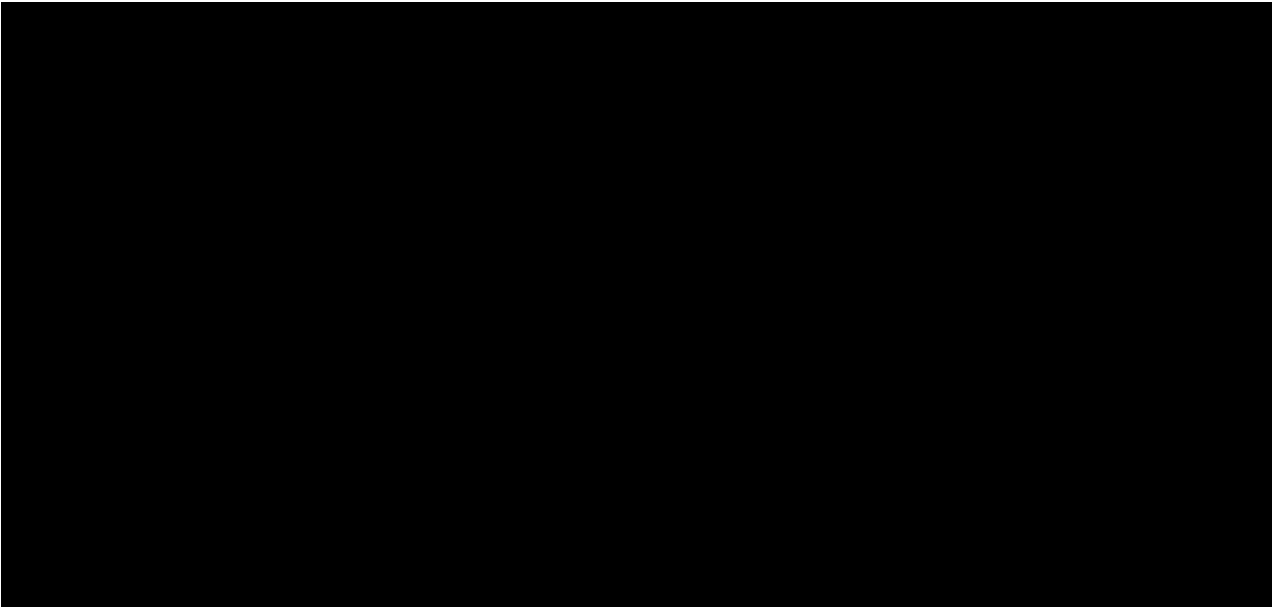
¹ *Government Auditing Standards* section 8.15 defines significance in the context of a performance audit.

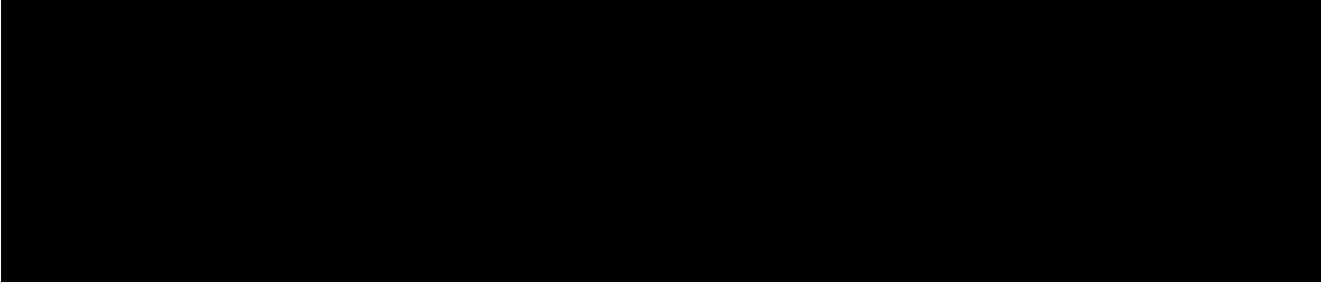
procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. All recommendations are intended to strengthen the Agency's processes for managing risk related to information technology (IT) systems and programs. 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. As of June 9, 2023, we determined the status of the above EBSA recommendations that the Agency identified as closed. As indicated above, we also noted internal control weaknesses in certain areas of the Agency's processes for managing risk related to IT systems and programs.

Section III.B documents the status of these 65 prior recommendations. In summary, 11 recommendations were implemented and closed, 1 recommendation was partially implemented and closed, 3 recommendations were not implemented but closed, and 50 recommendations were overcome by events and closed.

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, except the following recommendation:





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

September 15, 2023

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 over the status of certain prior year findings for the Thrift Savings Plan (TSP) at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency).

The objectives of this performance audit were to:

- Determine and validate whether recommendations that the Agency views as effectively resolved have been resolved; and
- Conduct procedures over certain prior year recommendations to determine whether each recommendation has been closed, partially closed, or remains open (or may have been potentially overtaken by events).

We reviewed the following 65 prior EBSA recommendations related to the TSP that the Agency identified as closed to determine their current status:

- Recommendation No. 2010-01, reported in *Performance Audit on Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings*, dated July 30, 2010;
- Recommendation No. 2013-03, reported in *Performance Audit of the Thrift Savings Plan System Enhancements and Software Change Controls*, dated November 27, 2013;
- Recommendation Nos. 2019-02a and b and 2019-03, reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019;
- Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated April 26, 2021;
- Recommendation Nos. 2015-03 and 2015-07b, reported in *Performance Audit of the Thrift Savings Plan IT Operations Controls*, dated July 13, 2016;
- Recommendation Nos. 2019-05, 2019-06a, and 2019-07, reported in *Performance Audit of the Thrift Savings Plan IT Operations Controls*, dated August 30, 2019;
- Recommendation No. 2007-03c, reported in *Review of the Computer Access and Technical Security Controls over the Thrift Savings Plan System*, dated March 30, 2007;

- Recommendation No.2011-01b, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated July 30, 2012;
- Recommendation No. 2013-01, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated August 16, 2013;
- Recommendation Nos. 2015-01, 2015-02, 2015-04, 2015-05a, and 2015-10, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated July 17, 2015;
- Recommendation Nos. 2016-02a, c, and d; 2016-04a, b, and e; 2016-08; and 2016-09, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017;
- Recommendation No. 2017-03, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018;
- Recommendation No. 2013-03a, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated Marcy 26, 2014;
- Recommendation Nos. 2013-01f and h, 2013-02a and b, 2013-03, 2013-04, 2013-06b, and 2013-08a and b, reported in *Performance Audit of Thrift Savings Plan Service Continuity Controls*, dated March 26, 2014;
- Recommendation Nos. 2016-02 and 2016-05b, c, and d, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated January 31, 2017;
- Recommendation Nos. 2019-02, 2019-03 2019-04, 2019-06, and 2019-07, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated August 22, 2019;
- Recommendation No. 2021-02, reported in *Performance Audit of the Thrift Savings Plan Participant Website Controls*, dated September 9, 2021;
- Recommendation Nos. 2014-01; 2014-02a, b, and d; 2014-03; 2014-05; and 2014-06, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration Management*, dated April 15, 2015;
- Recommendation Nos. 2016-01; 2016-02; 2016-03b; 2016-04; 2016-05; 2016-06a and b; 2016-07a, c, and d; 2016-08; 2016-09c; 2016-10b and c; 2016-13; 2016-14a, b, and c; 2016-16; and 2016-17, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls*, dated May 8, 2017;
- Recommendation Nos. 2018-01 and 2018-02, reported in *Performance Audit of the Thrift Savings Plan Mainframe Configuration and Security Controls*, dated December 7, 2018;
- Recommendation Nos. 2016-01, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Audit Recommendations*, dated April 26, 2017;

- Recommendation Nos. 2019-01b and 2019-02a, reported in *Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations*, dated September 6, 2019;
- Recommendation No. 2020-02, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020; and
- Recommendation Nos. 2018-01 and 2018-02, reported in *Performance Audit of Certain General Information Technology Controls at Thrift Savings Plan Remote Contractor Sites*, dated October 4, 2018.

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 June 1, 2022, through June 9, 2023. 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 recommendations and Agency remediation efforts. 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 certain prior year TSP findings to achieve our audit objectives:

- Conducted interviews;
- Inspected closure packages for Agency closed findings;
- Inspected Agency policies over project management requirements, including documentation retention requirements;
- Inspected Agency procedures over annual physical audits of Agency assets, the tracking and documenting media scheduled for destruction or sanitization, and Corrective Action Plans (CAP);
- Inspected Agency policies and procedures for key control areas of the TSP recordkeeping systems (TSP system or Converge);

- Inspected relevant sections of the Converge contract and the Converge System Security Plan (SSP);
- Inspected the Information System Contingency Plan and Security Assessment Report for the Converge system;
- Inspected Agency policies and procedures over the risk acceptance process for system vulnerabilities and related monitoring procedures;
- Inspected Agency procedures over tracking completion of annual privacy awareness training for federal employees;
- Inspected the Agency's annual privacy awareness training for federal employees;
- Inspected Agency documentation related to business continuity standards;
- Inspected Agency procedures over the risk assessment process prior to entering into an Interconnection Security Agreement (ISA);
- Inspected Agency non-concur justification memo template for audit recommendations;
- Inspected Agency policies and procedures over the monitoring and updating of Plan of Actions and Milestones (POA&Ms);
- Inspected Agency policies over the retention of system security documentation;
- Inspected Agency deauthorization and decommissioning memorandums for systems and system boundaries that were decommissioned subsequent to the Converge implementation;
- Tested a non-statistical sample of risk acceptances to determine whether management implemented monitoring procedures to enforce risk acceptance procedures, including the review and update of system documentation as applicable in accordance with established requirements;
- Tested a non-statistical sample of ISAs to determine whether the Agency performed a risk assessment prior to entering into the agreement in accordance with established requirements;
- Tested a non-statistical sample of CAPs with scheduled closure deadlines to determine whether the Agency enforced established procedures related to closure package time schedules and documentation of approvals for deadline extensions; and
- Inspected a non-statistical sample of POA&Ms to determine whether monitoring procedures were performed in accordance with established requirements.

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.

We conducted these test procedures remotely in coordination with personnel from the Agency's headquarters in Washington, D.C. and the prime vendor's headquarters in [REDACTED] In

Appendix B, we identify the key documentation provided by Agency and prime vendor personnel that we reviewed during our performance audit.

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.**