



Employee Benefits Security Administration

**Performance Audit over the
Thrift Savings Plan
Information Protection Processes and Procedures**

August 24, 2023

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND INFORMATION PROTECTION PROCESSES AND PROCEDURES CONTROLS.....	I.1
A. The Thrift Savings Plan	I.1
B. TSP System	I.1
C. Information Protection Processes 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. Introduction	III.1
B. Findings and Recommendations from Prior Reports	III.2
C. 2023 Findings and Recommendations	III.6
D. Summary of Open Recommendations	III.12
 <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 information protection processes and procedures for the Thrift Savings Plan (TSP) recordkeeping system. Our audit was performed remotely from December 6, 2022, through May 26, 2023. Our scope period for testing was June 1, 2022, through January 31, 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 (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Information Systems and Organizations*.

The objectives of our performance audit over TSP information protection processes and procedures were to determine whether the Agency and its vendor implemented certain cybersecurity procedures¹ to (1) maintain and manage the protection of information systems and assets through configuration management, backup and recovery, media sanitization, personnel

¹ NIST Cybersecurity Framework version 1.1 and other applicable standards.

security, and vulnerability management controls; and (2) evaluate vendor's contractual compliance with its data and privacy protection contractual provisions.

We present three new findings and recommendations related to TSP information protection processes and procedures, all of which address fundamental controls. Fundamental control recommendations address significant² 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 TSP information protection processes and procedures. 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 of June 1, 2022, through January 31, 2023, the Agency and its prime IT vendor implemented cybersecurity procedures to maintain and manage the protection of information systems and assets through configuration management, backup and recovery, media sanitization, personnel security, and vulnerability management controls; and evaluate vendor's contractual compliance with its data and privacy protection contractual provisions. However, as indicated above, we noted internal control weaknesses in certain areas of TSP information protection processes and procedures controls within our audit objectives.

We also reviewed five prior EBSA recommendations related to TSP information protection processes and procedures to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:

- Recommendation No. 2013-1 reported in *Performance Audit of the Thrift Savings Plan System Enhancements and Software Change Controls*, dated November 27, 2013;
- Recommendation Nos. 2015-1c and 2015-3 reported in *Performance Audit of the Thrift Savings Plan System Enhancement and Software Change Controls*, dated June 17, 2016;
- Recommendation No. 2019-4b reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019; and
- Recommendation No. 2021-2 reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated April 26, 2021.

² *Government Auditing Standards* section 8.15 defines significance in the context of a performance audit.

Section III.B documents the status of these prior recommendations. In summary, three recommendations have been implemented and closed, and two recommendations have not been implemented but have been overcome by events and closed.

The Agency's responses to the recommendations 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, 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

August 24, 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 information protection processes and procedures for the Thrift Savings Plan (TSP) recordkeeping system 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 implemented certain cybersecurity procedures¹ to (1) maintain and manage the protection of information systems and assets through configuration management, backup and recovery, media sanitization, personnel security, and vulnerability management controls; and (2) evaluate vendor's contractual compliance with its data and privacy protection contractual provisions.

- Determine the status of five prior EBSA recommendations related to TSP information protection processes and procedures to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:
 - Recommendation No. 2013-1 reported in *Performance Audit of the Thrift Savings Plan System Enhancements and Software Change Controls*, dated November 27, 2013;
 - Recommendation Nos. 2015-1c and 2015-3 reported in *Performance Audit of the Thrift Savings Plan System Enhancement and Software Change Controls*, dated June 17, 2016;
 - Recommendation No. 2019-4b reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated June 7, 2019; and
 - Recommendation No. 2021-2 reported in *Performance Audit of the Thrift Savings Plan Systems Enhancement and Software Change Controls*, dated April 26, 2021.

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 January 31, 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 information protection processes and procedures. 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 TSP information protection processes and procedures to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Inspected applicable contracts and procedures for information technology support services;
- Participated in process walkthroughs over information protection activities;
- Inspected policies that established the requirements for information protection control processes;
- Inspected procedures and plans that documented information protection control processes implemented to comply with established requirements;
- Inspected baseline configuration settings for the Converge system;
- Inspected software development lifecycle and change management processes with established requirements;
- Inspected information backup configuration settings;
- Inspected processes for the destruction of data based on established requirements;
- Inspected and tested response and recovery policies and procedures implemented and testing of response and recovery processes;
- Tested a non-statistical sample of Converge new employees/contractors during the audit scope period to determine whether proper screening was conducted prior to those individuals beginning work on the Converge system in accordance with established requirements;
- Tested a non-statistical sample of terminated/departed Converge program employees and contractors during the audit scope period to determine whether deprovisioning procedures were appropriately completed in accordance with established requirements;

- Tested a non-statistical sample of Converge system vulnerability scans and patches to determine whether vulnerability management processes were followed in accordance with established requirements; and
- Inspected evidence to determine whether the Agency's prime vendor was in compliance with provisions of the Converge contract related to information protection processes and procedures.

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]. Appendix B lists the key documentation and reports provided by Agency and prime vendor 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 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.**