



## **Employee Benefits Security Administration**

### **Performance Audit over the Thrift Savings Plan Vendor Risk Management**

**June 14, 2023**

## TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
<b>EXECUTIVE SUMMARY .....</b>	<b>i</b>
<b>I. BACKGROUND OF THE TSP AND VENDOR RISK MANAGEMENT .....</b>	<b>I.1</b>
A. The Thrift Savings Plan .....	I.1
B. TSP System.....	I.1
C. Converge Vendor Oversight .....	I.2
D. Certain Other New Vendors and Service Providers .....	I.2
E. Risk Management Framework.....	I.3
<b>II. OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>II.1</b>
A. Objectives .....	II.1
B. Scope and Methodology .....	II.1
<b>III. FINDINGS AND RECOMMENDATIONS .....</b>	<b>III.1</b>
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Reports.....	III.2
C. 2023 Findings and Recommendations .....	III.8
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 Thrift Savings Plan (TSP) vendor risk management controls. Our audit was performed remotely from December 6, 2022, through March 2, 2023, in coordination with personnel primarily from the Federal Retirement Thrift Investment Board's Staff (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2022, through December 31, 2022.

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 is 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 TSP vendor risk management controls were to determine whether the Agency implemented certain procedures to (1) assess service providers against key contractual and service level agreement requirements related to information technology security; (2) establish, document, and implement security management controls for the new recordkeeping system; and (3) establish, document, and implement privacy controls to protect TSP data by third-party

vendors. The audit also determined the research and benchmarking performed by the Agency when establishing service level requirements and key performance metrics for the Converge<sup>1</sup> contract.

We present three new findings and recommendations, all of which address fundamental controls. Fundamental control recommendations address significant<sup>2</sup> 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 vendor risk management 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, 2022, through December 31, 2022, the Agency implemented certain procedures to (1) assess service providers against key contractual and service level agreement requirements related to information technology security; (2) establish, document, and implement security management controls for the new recordkeeping system; and (3) establish, document, and implement privacy controls to protect TSP data by third-party vendors. However, as indicated above, we noted internal control weaknesses in certain areas of TSP vendor risk management. We also determined that although the Agency did not benchmark or establish metrics on its own for service level requirements and key performance indicators prior to the Converge acquisition process, the acquisition strategy established a requirement for the interested bidders to build these metrics into their delivery strategy, which was assessed during the source selection process.

We also reviewed four prior EBSA recommendations related to TSP risk management and vendor risk management controls to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:

- Recommendation No. 2017-05 reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018; and

---

<sup>1</sup> TSP Recordkeeping Systems (TSP system or Converge) are a collection of applications that value accounts daily, process and record loans and withdrawals, record contributions, and process interfund transfer requests for TSP participants and beneficiaries. In November 2020, the Agency contracted with a vendor to provide recordkeeping services for the TSP under a recordkeeping services acquisition contract (i.e., the Converge contract).

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

- Recommendation Nos. 2020-01, 2020-02, and 2020-06, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated June 4, 2020.

Section III.B documents the status of these prior recommendations. In summary, three were implemented and/or overcome by events and closed, and one recommendation was not implemented but closed.

The Agency's response to the recommendations is 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

June 14, 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 Thrift Savings Plan (TSP) vendor risk management controls at the Federal Retirement Thrift Investment Board's (Board) Staff (Agency).

The objectives of this performance audit were to:

- Determine whether the Agency implemented certain procedures to (1) assess service providers against key contractual and service level agreement requirements related to information technology security; (2) establish, document, and implement security management controls for the new recordkeeping system; and (3) establish, document, and implement privacy controls to protect TSP data by third-party vendors.
- Determine the research and benchmarking performed by the Agency when establishing service level requirements and key performance metrics for the Converge contract.
- Determine the status of four prior EBSA recommendations related to TSP risk management and vendor risk management controls to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:
  - Recommendation No. 2017-05 reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018; and
  - Recommendation Nos. 2020-01, 2020-02, and 2020-06, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated June 4, 2020.

### **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, 2022, through December 31, 2022. 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 vendor risk management. During the planning phase, we inquired of Agency management and reviewed Board meeting minutes to identify and select Agency vendors and service providers. We designed test procedures to (1) evaluate whether the Agency implemented procedures to assess service providers against key contractual and service level agreement requirements; (2) evaluate security management controls for the new recordkeeping system to include if the Agency established, documented, and implemented privacy controls to protect TSP data by third-party vendors; and (3) determine the research and benchmarking performed by the Agency when determining service level requirements and key performance metrics for the Converge contract. Arranging for 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 vendor risk management to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected documentation provided by the Agency and in-scope vendors and service providers;
- Inspected applicable contracts and procedures related to the new TSP recordkeeping system and services provided by the Department of Justice (DOJ);
- Inspected Agency policies that established the requirements for vendor risk management;
- Inspected benchmarking documentation related to the new TSP recordkeeping system;
- Inspected Agency privacy program documentation; and
- Inspected Agency risk management and system authorization documentation.

Our testing considered controls in areas such as risk management, program management, security assessment and authorization, plans of actions and milestones, continuous monitoring, benchmarking, privacy program plan, and personally identifiable information management. We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, D.C. In Appendix B, we identify the key documentation

provided by Agency and the in-scope vendors and service providers 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 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.**