KPMG

Employee Benefits Security Administration

Performance Audit over the Thrift Savings Plan Pre-Implementation Vendor Cybersecurity Management

May 9, 2022

TABLE OF CONTENTS

Section Page

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) pre-implementation vendor cybersecurity management. Our audit was performed remotely from December 15, 2021 through March 4, 2022, 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 as of December 8, 2021.

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 Special Publication 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objective of our audit over the TSP pre-implementation vendor cybersecurity management was to determine whether the Agency has implemented certain procedures to determine if the new recordkeeping service provider developed certain cybersecurity and data protection procedures over TSP and participant account data in accordance with applicable Federal and contractual requirements.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objective. We conclude that as of December 8, 2021, the Agency implemented certain procedures to determine if the new recordkeeping service provider developed certain cybersecurity and data protection procedures over TSP and participant account data in accordance with applicable Federal and contractual requirements.

No prior findings or recommendations were within the scope of this audit, and the current engagement produced no new findings or recommendations. The Agency's response to this report, including the Executive Director's formal reply, is included as Appendix A.

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

May 9, 2022

II. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objective

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) pre-implementation vendor cybersecurity management at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objective of this performance audit was to determine whether the Agency has implemented certain procedures to determine if the new recordkeeping service provider developed certain cybersecurity and data protection procedures over TSP and participant account data in accordance with applicable Federal and contractual requirements.

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 as of December 8, 2021. 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 cybersecurity management. During the planning phase, we designed test procedures to evaluate whether the Agency determined if the TSP managed service provider established cybersecurity processes in accordance with applicable requirements. Our testing included the review of cybersecurity documentation developed by the TSP managed service provider for the new recordkeeping system. 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 vendor cybersecurity management to achieve our audit objective:

- Conducted interviews;

- Collected and inspected documentation provided by the Agency and TSP managed service provider;
- Inspected applicable contracts and procedures for information technology support services;
- Inspected Agency policies that established the requirements for vendor cybersecurity management; and
- Inspected TSP managed service provider policies, procedures, and plans that established processes for compliance with Agency-defined and external cybersecurity requirements.

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 TSP managed service provider personnel that we reviewed during our performance audit. Because the new recordkeeping system is in the pre-implementation phase, we did not evaluate the implementation or operating effectiveness of new recordkeeping system controls as part of our test procedures.

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 (NIST) Special Publication (SP) 800-53, Revision (Rev.) 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. In order to prioritize the NIST SP 800-53 Rev. 5 requirements related to cybersecurity when designing our test procedures, we aligned our testing to the NIST Cybersecurity Framework (CSF) using a mapping from SP 800-53 Rev. 5 to the CSF created and distributed by NIST on January 22, 2021. Our test procedures spanned the following CSF categories in the cybersecurity function areas of Identify, Protect, Detect, Respond, and Recover, and focused on the SP 800-53 Rev. 5 requirements mapped to each category:

- Identify: Asset Management; Governance; Risk Management Strategy; Supply Chain Risk Management
- Protect: Identity Management, Authentication[9], and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Protective Technology
- Detect: Anomalies and Events; Security Continuous Monitoring; Detection Processes
- Respond: Response Planning; Communications; Analysis; Mitigation
- Recover: Recovery Planning

[9] We assessed authentication procedures related to internal Converge systems and not external-facing participant/beneficiary systems.

We inspected documentation provided by the Agency and the TSP managed service provider to evaluate whether processes had been designed to meet NIST 800-53 Rev. 5 requirements in the areas noted above.

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.