KPMG

Employee Benefits Security Administration

Performance Audit over the Thrift Savings Plan Detection and Monitoring Security Controls

August 23, 2023

TABLE OF CONTENTS

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 detection and monitoring security controls for the Thrift Savings Plan (TSP) information systems. Our audit was performed remotely from February 23, 2023, through May 26, 2023. Our scope period for testing was June 1, 2022, through March 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 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our performance audit over TSP detection and monitoring security controls were to determine whether the Agency and its vendor implemented certain cybersecurity procedures[1] to monitor TSP information systems and assets to identify cybersecurity events and assess the effectiveness of protective measures.

[1] National Institute of Standards and Technology (NIST) and other applicable standards.

We present one new finding and recommendation, which addresses fundamental controls. Fundamental control recommendations address significant[2] 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. This recommendation is intended to strengthen TSP detection and monitoring security controls. The Agency should review and consider this recommendation for timely implementation. Section III.C presents a summary of the current year finding and recommendation, the details of which can be found in Recommendation No. 2023-01: *Weaknesses in Configuration Baseline Controls* of the *Performance Audit Report over the Thrift Savings Plan Information Protection and Processes*, dated August 24, 2023.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period June 1, 2022, through March 31, 2023, the Agency and its vendor implemented certain cybersecurity procedures[1] to monitor TSP information systems and assets to identify cybersecurity events and assess the effectiveness of protective measures. However, as indicated above, we noted an internal control weakness in detection and monitoring security controls within our audit objectives.

We also reviewed five prior EBSA recommendations related to TSP detection and monitoring security controls to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:

- Recommendation No. 2013-01 and 2013-02, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated March 26, 2014;
- Recommendation No. 2020-03, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020;
- Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Participant Website Controls*, dated September 9, 2021; and
- Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Independent Verification & Validation (IV&V) and Penetration Test Remediation Process*, dated September 23, 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, four recommendations were implemented and closed, and one recommendation has been overcome by events and closed.

The Agency's response to this report, including the Executive Director's formal reply, is included as Appendix A. Additionally, we referenced one new finding and recommendation within the *Performance Audit Report over the Thrift Savings Plan Information Protection and Processes* (Appendix A), dated August 24, 2023. See Appendix A of that report for management's response and concurrence to the 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

August 23, 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 detection and monitoring security controls for the Thrift Savings Plan (TSP) information 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 procedures to monitor TSP information systems and assets to identify cybersecurity events and assess the effectiveness of protective measures.

- Determine the status of five prior EBSA recommendations related to TSP detection and monitoring security controls. The following prior year recommendations were determined to be in scope for this performance audit:

    - Recommendation No. 2013-01 and 2013-02, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated March 26, 2014;
    - Recommendation No. 2020-03, reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020;
    - Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Participant Website Controls*, dated September 9, 2021; and
    - Recommendation No. 2021-01, reported in *Performance Audit of the Thrift Savings Plan Independent Verification & Validation (IV&V) and Penetration Test Remediation Process*, dated September 23, 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 March 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 detection and monitoring security controls. 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 detection and monitoring controls 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 detection and monitoring activities;
- Inspected policies that established the requirements for detection and monitoring control processes;
- Inspected software development lifecycle and change management processes with established requirements;
- Inspected procedures that established incident response and vulnerability management to comply with established requirements;
- Inspected baseline configurations supporting the prevention of unauthorized connections, devices and software;
- Inspected automated system alerts to support continuous monitoring, detection, and response capabilities across the Converge program;
- Tested a non-statistical sample of events related to personnel monitoring to determine compliance with information security policies for detecting potential cybersecurity events.
- Tested a non-statistical sample network scans and vulnerability scans to determine compliance with internal information security policies regarding overall system architecture on a consistent basis;
- Tested a non-statistical sample of continuous monitoring reports to determine how the cloud service providers (CSP) monitor the security controls and posture on a consistent basis; and
- Inspected evidence of penetration reports and remediation of findings conducted to identify weakness within Converge.

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.