KPMG

Employee Benefits Security Administration

Performance Audit over the Thrift Savings Plan Computer Access and Data Security Controls

June 20, 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 the computer access and data security controls for the Thrift Savings Plan (TSP) recordkeeping system. Our audit was performed remotely from December 6, 2022, through April 14, 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 is 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 audit over TSP computer access and data security controls were to determine whether the Agency and its prime information technology (IT) vendor implemented certain cybersecurity procedures to: (1) limit access to physical and logical assets and facilities to authorized users; and (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

We present three new findings and recommendations related to TSP computer access and data security controls, all of which address fundamental controls. Fundamental control recommendations address significant[1] 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 computer access and data security 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 of June 1, 2022 through January 31, 2023, the Agency and its prime IT vendor implemented cybersecurity procedures to: (1) limit access to physical and logical assets and facilities to authorized users; and (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. However, as indicated above, we noted internal control weaknesses in certain areas of TSP computer access and data security controls within our audit objectives.

We also reviewed 10 prior EBSA recommendations related to TSP computer access and data security controls to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:

- Recommendation No. 2013-04, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated March 26, 2014;
- Recommendation No. 2016-07, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated January 31, 2017;
- Recommendation Nos. 2016-01, 2016-03, and 2016-10, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017;
- Recommendation No. 2017-02, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018;
- Recommendation Nos. 2019-01 and 2019-05, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls,* dated August 22, 2019; and
- Recommendation Nos. 2020-03 and 2020-05, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls*, dated June 4, 2020.

[1] *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, six recommendations have been implemented and closed, one recommendation has been partially implemented/overcome by events and closed, and three recommendations 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

June 20, 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 computer access and data security controls 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 prime information technology (IT) vendor implemented certain cybersecurity procedures to: (1) limit access to physical and logical assets and facilities to authorized users; and (2) manage information and data consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- Determine the status of 10 prior EBSA recommendations related to TSP computer access and data security controls to determine their current status. The following prior year recommendations were determined to be in scope for this performance audit:

    - Recommendation No. 2013-04, reported in *Performance Audit of the Thrift Savings Plan Technical Security Controls*, dated March 26, 2014;
    - Recommendation No. 2016-07, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated January 31, 2017;
    - Recommendation Nos. 2016-01, 2016-03, and 2016-10, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 3, 2017;
    - Recommendation No. 2017-02, reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018;
    - Recommendation Nos. 2019-01 and 2019-05, reported in *Performance Audit of the Thrift Savings Plan Service Continuity Controls*, dated August 22, 2019; and
    - Recommendation Nos. 2020-03 and 2020-05, 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 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 computer access and data 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 computer access and data security controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Inspected applicable contracts and procedures for IT support services;
- Participated in process walkthroughs over computer access and data security activities;
- Inspected applicable contracts and procedures for IT support services;
- Inspected policies that established the requirements for computer access and data security control processes;
- Inspected procedures and plans that documented computer access and data security control processes implemented to comply with established requirements;
- Inspected identification and authentication configuration settings for Converge;
- Tested a non-statistical sample of new users granted access to Converge during the audit scope period to determine whether access requests were documented and approved prior to access being provisioned in accordance with established requirements;
- Tested a non-statistical sample of Converge access reauthorizations and separation of duties reviews to determine whether access was reviewed and reauthorized by appropriate authorizers in accordance with established requirements;

- Tested a non-statistical sample of Converge users who left the program during the audit scope period to determine whether access was removed in a timely manner upon notification of separation in accordance with established requirements;
- Inspected encryption and data loss prevention settings configured to protect Converge data;
- Inspected System and Organization Controls (SOC) reports for Converge cloud service providers and documentation indicating that the reports were reviewed by the Agency's prime IT vendor;
- Inspected evidence that the Converge production environment was maintained separately from pre-production (e.g., development and test) environments.

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 IT vendor's headquarters in [redacted] In Appendix B, we identify the key documentation provided by Agency and prime IT 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.