KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Computer Access and Technical Security Controls

June 4, 2020

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 of the Thrift Savings Plan (TSP) computer access and technical security controls. Our fieldwork was performed from December 2, 2019 through March 20, 2020, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. and at an Agency's contractor's location in Virginia. Our scope period for testing was January 1, 2019 through December 31, 2019.

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' *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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our audit over the TSP computer access and security controls were to:

- Determine whether (1) security management controls had been established, documented, and implemented for in-scope TSP systems[1]; (2) physical and logical access controls had been

[1] In-scope systems for this performance audit included: Participant Services Representative (PSR), Agency Payroll Interface (API) Online, Court Order Document Imaging System (CODIS), Death Document Imaging System (DeDIS), Cash Management System (CaMS), SunGard Omni Suite (Omni Plus, Omni Security, Omni Pay, Omni Admin Web),

established, documented, and enforced for in-scope TSP systems; and (3) privacy controls had been established, documented, and enforced to protect TSP data.

- Determine the status of the prior EBSA TSP computer access and security controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018.

We present six new findings and recommendations related to TSP computer access and security controls, all of which address 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. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen TSP computer access and 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 January 1, 2019 through December 31, 2019, (1) security management controls were not consistently established, documented, and implemented for in-scope TSP systems; (2) physical and logical access controls were not consistently established, documented, and enforced for in-scope TSP systems; and (3) privacy controls were established and documented, but not consistently enforced to protect TSP data. As indicated above, we noted internal control weaknesses in all areas of TSP computer access and security controls within our audit objectives.

We also reviewed 27 prior EBSA recommendations related to TSP computer access and security controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, five recommendations have been implemented and closed, three recommendations have been partially implemented but are considered closed, one recommendation has not been implemented but is considered closed, 15 recommendations have been partially implemented and remain open, and three recommendations have not been implemented and remain open.

SunGard EXP AG, Genesys, FRTIB Domain, SANDD Domain, applicable Windows servers, applicable Oracle databases, applicable DB2 databases, and applicable Microsoft Structured Query Language (MS SQL) databases.

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

The Agency's responses to the recommendations, including the Executive Director's formal reply, are included as an appendix within the report (Appendix A). The Agency concurred with all recommendations and indicated within its response where management performed corrective actions after the audit scope period and now considers certain recommendations to be closed. We did not validate the implementation of corrective actions taken after the audit scope period.

This performance audit did not constitute an audit of the TSP's financial statements in accordance with *Government Auditing Standards.* 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 4, 2020

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 of the Thrift Savings Plan (TSP) computer access and security controls at the Federal Retirement Thrift Investment Board's Staff (Agency).

The objectives of this performance audit were to:

- Determine whether (1) security management controls had been established, documented, and implemented for in-scope TSP systems[1]; (2) physical and logical access controls had been established, documented, and enforced for in-scope TSP systems; and (3) privacy controls had been established, documented, and enforced to protect TSP data.

- Determine the status of the prior EBSA TSP computer access and security controls open recommendations reported in *Performance Audit of the Thrift Savings Plan Computer Access and Security Controls*, dated May 15, 2018.

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, 2019 through December 31, 2019. 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 security. 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 the TSP computer access and security controls to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence[19];
- Participated in process walk-throughs for physical and logical access and data monitoring activities, security and risk management activities, and TSP sensitive information activities;
- Inspected applicable contracts and procedures for information technology support services;
- Inspected system documentation for evidence of implementation and ongoing monitoring;
- Inspected system identity and access management settings and privileged access for compliance with Agency requirements;
- Inspected a non-statistical sample of active users for evidence of a successful suitability investigation, completed privacy training, and completed security awareness training;
- Inspected a non-statistical sample of security incidents for evidence of timely reporting to the United States Computer Emergency Readiness Team (US-CERT);
- Inspected a non-statistical sample of new user accounts for evidence of approval and signed rules of behavior forms prior to account creation;
- Inspected the population of terminated employees and contractors for evidence of removal from selected systems and applications upon termination;
- Inspected a non-statistical sample of annual reviews and recertifications of system access; and
- Inspected a non-statistical sample of individuals with physical access to the primary and backup data centers for evidence of approval and removal upon termination.

We conducted these test procedures primarily at Agency headquarters in Washington, D.C. and at the Agency's contractor's location in Virginia. In Appendix B, we identify the key documentation provided by Agency 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 the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *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.

[19] We obtained and utilized certain user listings subsequent to the scope period. The Agency represented that such listings were functionally and technically the same as those in place as of December 31, 2019.

This report contains Sensitive Information and will not be posted.