



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Participant Website Controls

June 27, 2019

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND PARTICIPANT WEBSITE	
A. The Thrift Savings Plan	I.1
B. Overview of the TSP Participant Website	I.1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	
A. Objectives	II.1
B. Scope and Methodology	II.1
III. FINDINGS AND RECOMMENDATIONS	
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Reports.....	III.2
C. 2019 Findings and Recommendations	III.8
D. Summary of Open Recommendations	III.14
 <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 Benefit 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) participant website controls. Our fieldwork was performed from November 20, 2018 through March 29, 2019, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2018 through December 31, 2018.

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 audit objectives. Criteria used for this audit are defined in the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes the National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our audit over the TSP participant website controls were to:

- Determine whether the Agency implemented certain procedures related to: (1) securing participant communications and transactions via the Web through password and user identification configuration settings, system edit checks regarding certain indicative data

updates, and transaction types; (2) managing website configuration changes; and (3) monitoring threats to participant data from external threats via the Web and social media.

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of the Thrift Savings Plan Participant Website*, dated May 12, 2016.

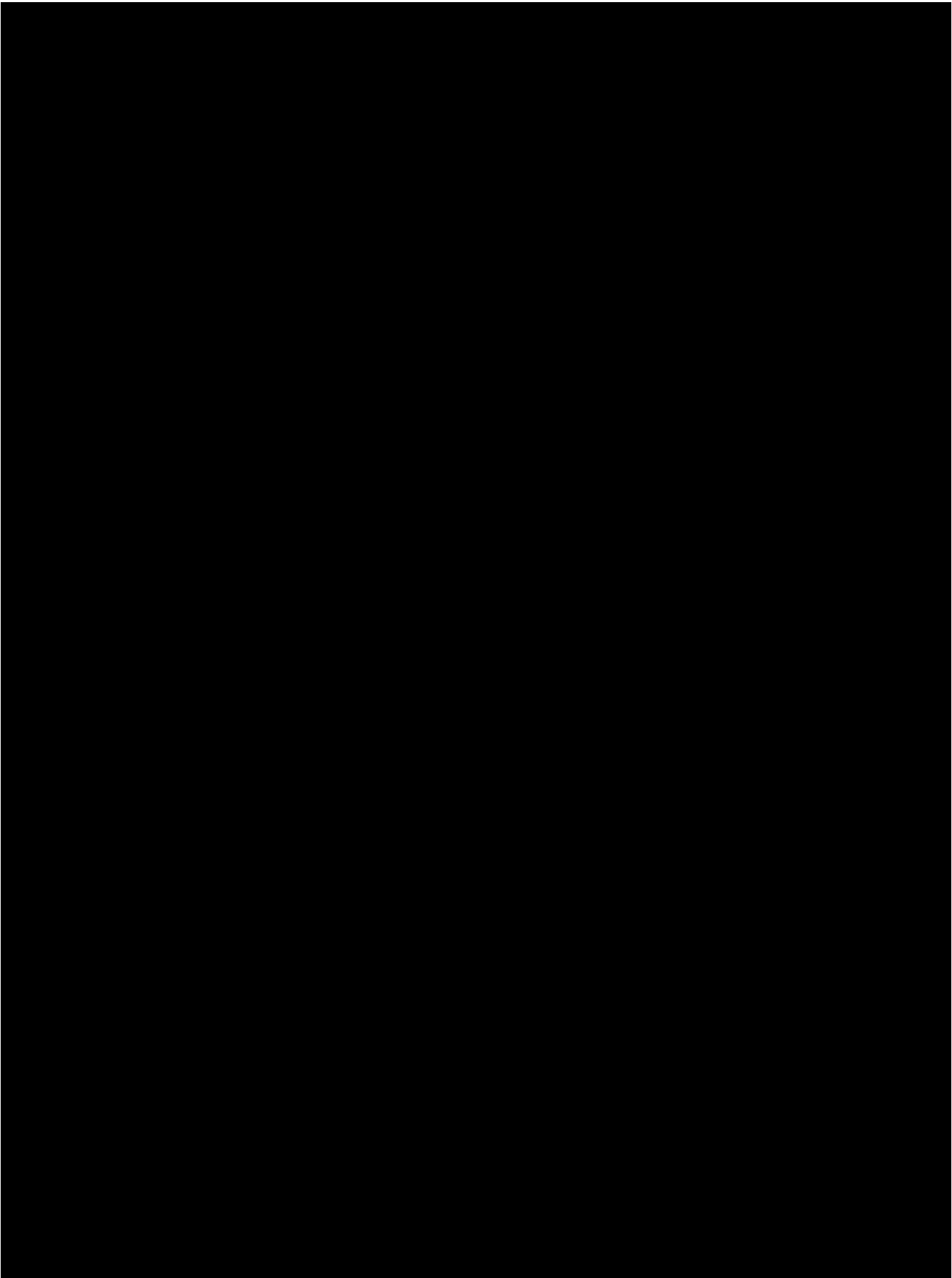
We present three new findings and recommendations related to TSP participant website controls, all of which address fundamental controls. Fundamental control recommendations address significant¹ procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. All recommendations are intended to strengthen TSP participant website 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.

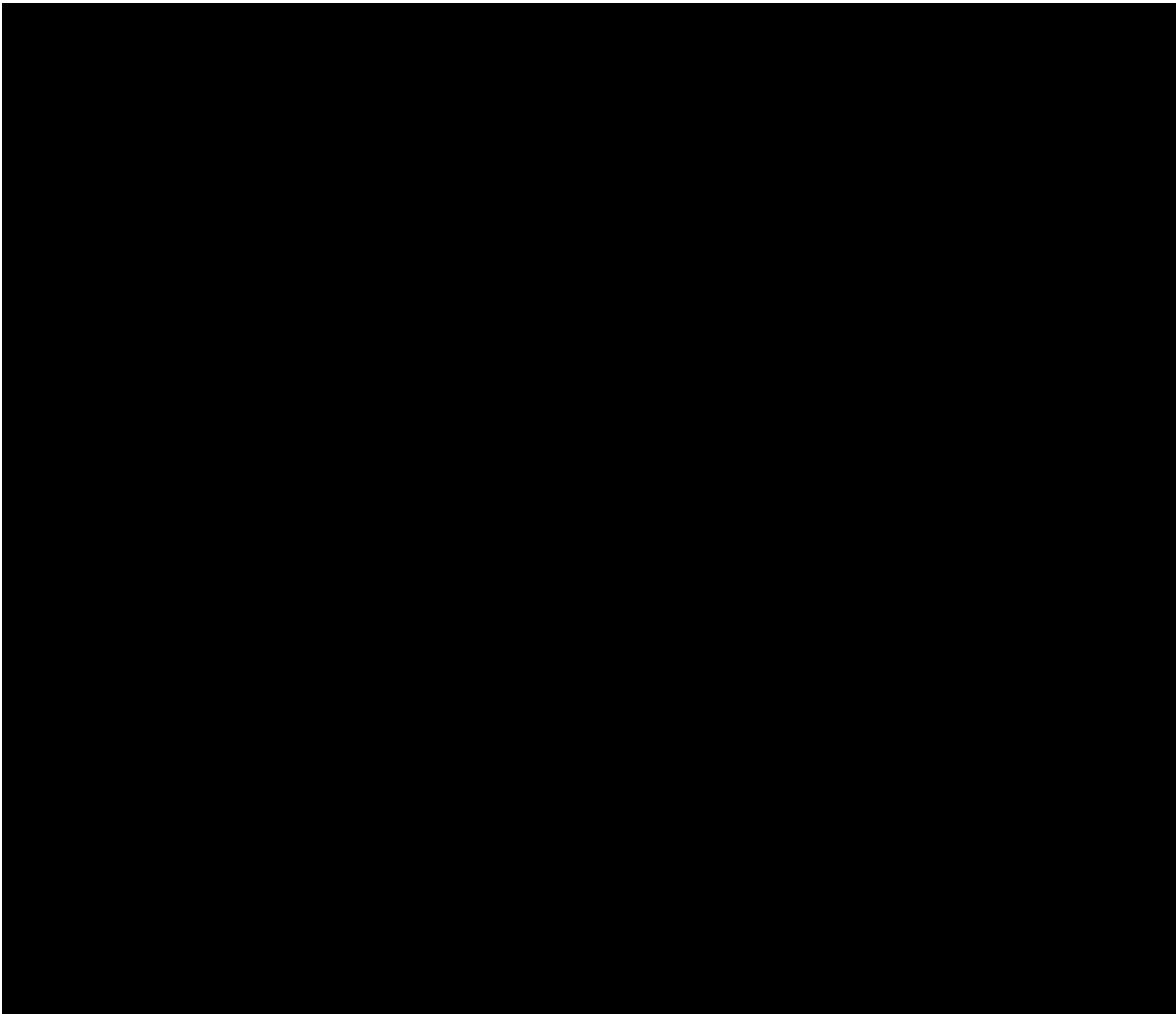
Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2018 through December 31, 2018, the Agency implemented certain procedures related to (1) securing participant communications and transactions via the Web through password and user identification configuration settings, system edit checks regarding certain indicative data updates, and transaction types; (2) managing website configuration changes; and (3) monitoring threats to participant data from external threats via the Web and social media. However, as indicated above, we noted internal control weaknesses in certain TSP participant website controls.

We also reviewed five prior EBSA recommendations related to TSP participant website controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, two recommendations have been implemented and closed, and three recommendations have been partially implemented and remain open.

The Agency's response to the recommendations are included as an appendix within the report (Appendix A). The Agency concurred with all recommendations, except for the following:

¹ *Government Auditing Standards* section 6.04 defines significance in the context of a performance audit.





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 Benefit 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 27, 2019

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) participant website controls.

The objectives of our performance audit were to:

- Determine whether the Agency implemented certain procedures related to: (1) securing participant communications and transactions via the Web through password and user identification configuration settings, system edit checks regarding certain indicative data updates, and transaction types; (2) managing website configuration changes; and (3) monitoring threats to participant data from external threats via the Web and social media.
- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of the Thrift Savings Plan Participant Website*, dated May 12, 2016.

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, 2018 through December 31, 2018. 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 to develop a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with the TSP participant website controls. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we conducted interviews, collected and inspected auditee-provided documentation and evidence, participated in process walk-throughs, and

designed and performed tests of controls³. We conducted these test procedures at the Agency's 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 and contractor personnel that we reviewed during our performance audit.

Our performance audit procedures included using haphazard, non-statistical sampling to select samples of the following:

- Incidents related to the TSP.gov website for follow-up and resolution;
- Changes on the TSP.gov for evidence of approval prior to migration into production;
- Individuals with access to modify the TSP.gov website for evidence of approval and appropriateness;
- Daily validation controls over participant data loaded to the MyAccount website; and
- TSP.gov website cryptographic session reviews.

Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the sample items we tested and were not extrapolated to the population.

Testing procedures were based on the objectives and control areas for information security and access controls in the Government Accountability Office's *Federal Information System Controls Audit Manual*. In addition, the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, was used to evaluate the status of the Agency's control environment.

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.

³ We obtained and utilized certain information technology system settings in the test environment related to participant website controls. The Agency represented that such settings were functionally and technically the same as those in production from January 1, 2018 through December 31, 2018.

**This report contains Sensitive Information
and will not be posted.**