



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Mobile Device Security and Governance Controls

September 27, 2018

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND THE MOBILE DEVICE SECURITY AND GOVERNANCE PROGRAM	
A. The Thrift Savings Plan	I.1
B. Mobile Governance and Strategy.....	I.1
C. Mobile Device Management Solution	I.2
D. Tracking and Monitoring of Mobile Devices	I.3
E. Configuration Management of Mobile Devices ⁶	I.3
F. Other Supporting Infrastructure.....	I.4
II. OBJECTIVE, 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 Report	III.2
C. 2018 Findings and Recommendations	III.13
D. Summary of Open Recommendations	III.31
 <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) mobile device security and governance controls. Our fieldwork was performed from April 23, 2018 through July 18, 2018, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was May 1, 2017 through April 30, 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 objectives. Criteria used for this audit is 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 at the Agency over the TSP mobile device security and governance controls were to determine whether (1) management developed a mobile device security and governance program; (2) management established controls for tracking and monitoring mobile devices; and (3) management established controls for configuring, updating, and removing mobile devices from the TSP network.

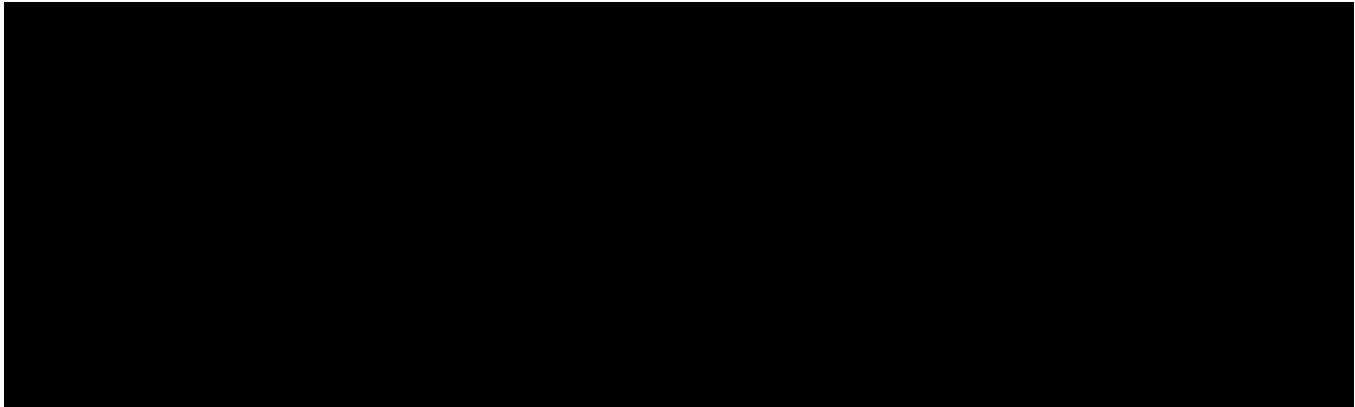
We present 11 new findings and recommendations related to TSP mobile device security and governance controls, all of which address fundamental controls. Fundamental control

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 mobile device security and governance 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.

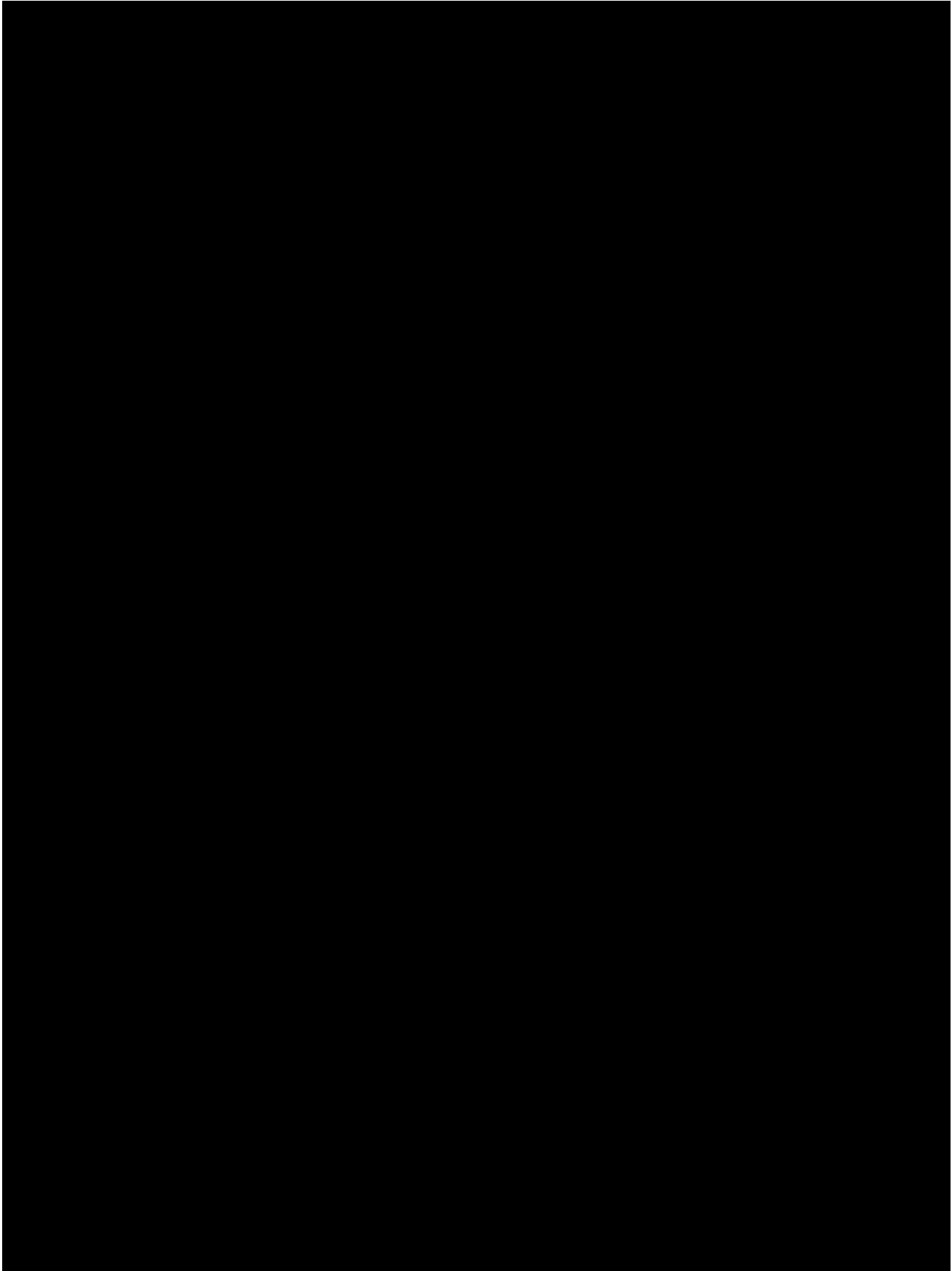
Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period May 1, 2017 through April 30, 2018, (1) management had not developed a mobile device security and governance program; (2) management had not established controls for tracking and monitoring mobile devices; and (3) management had not established controls for configuring, updating, and removing mobile devices from the TSP network. As indicated above, we noted internal control weaknesses in all areas of the TSP mobile device security and governance controls within our audit objectives.

We also reviewed 11 prior EBSA recommendations related to TSP mobile device security and governance controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, three recommendations have been implemented and closed, six recommendations have been partially implemented and remain open, one recommendation was partially implemented and closed, and one recommendation has not been implemented and remains open.

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, except 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

September 27, 2018

II. OBJECTIVE, 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) mobile device security and governance controls.

The objectives of this performance audit at the Federal Retirement Thrift Investment Board's Staff (Agency) were to determine whether (1) management developed a mobile device security and governance program; (2) management established controls for tracking and monitoring mobile devices; and (3) management established controls for configuring, updating, and removing mobile devices from the TSP network.

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 May 1, 2017 through April 30, 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 mobile device security and governance process. 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 to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Participated in process walk-throughs for mobile device administration activities and mobile device security and governance monitoring activities;
- Inspected applicable contracts and procedures for information technology support services;

- Inspected system documentation for evidence of implementation and ongoing monitoring of mobile devices;
- Inspected the population of mobile device users for evidence of baseline configuration actions, removal activities, and administrative monitoring;
- Inspected the population of mobile device administrators for evidence of least privilege access;
- Inspected a [REDACTED] sample of terminated employees and contractors for evidence of removal from the mobile device management tool;
- Inspected a [REDACTED] sample of new mobile device requests for evidence of appropriate approval; and
- Inspected a [REDACTED] sample of monthly vulnerability reports.

We conducted these test procedures primarily at the Agency’s headquarters in Washington, DC. In Appendix B, we identify the key documentation provided by Agency personnel that we reviewed during our performance audit. [REDACTED]

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 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.**