



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations

September 6, 2019

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP	
A. The Thrift Savings Plan	I.1
B. Mandiant TSP Testing Overview.....	I.3
II. OBJECTIVES, SCOPE, AND METHODOLOGY	
A. Objectives	II.1
B. Scope and Methodology	II.2
III. FINDINGS AND RECOMMENDATIONS	
A. Introduction.....	III.1
B. Findings and Recommendations from Prior Mandiant Reports	III.2
C. 2019 Findings and Recommendations	III.11
D. Summary of Open Recommendations	III.19
 <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 to determine the status of certain prior Mandiant¹ recommendations, as reported on October 18, 2018, related to the Thrift Savings Plan (TSP) and directed to the Federal Retirement Thrift Investment Board's (the Board or FRTIB) Staff (Agency), and to assess the Agency's Corrective Action Plans (CAPs) process. Our testing was performed as of April 18, 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 audit objectives. Criteria used for this audit are defined in the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which

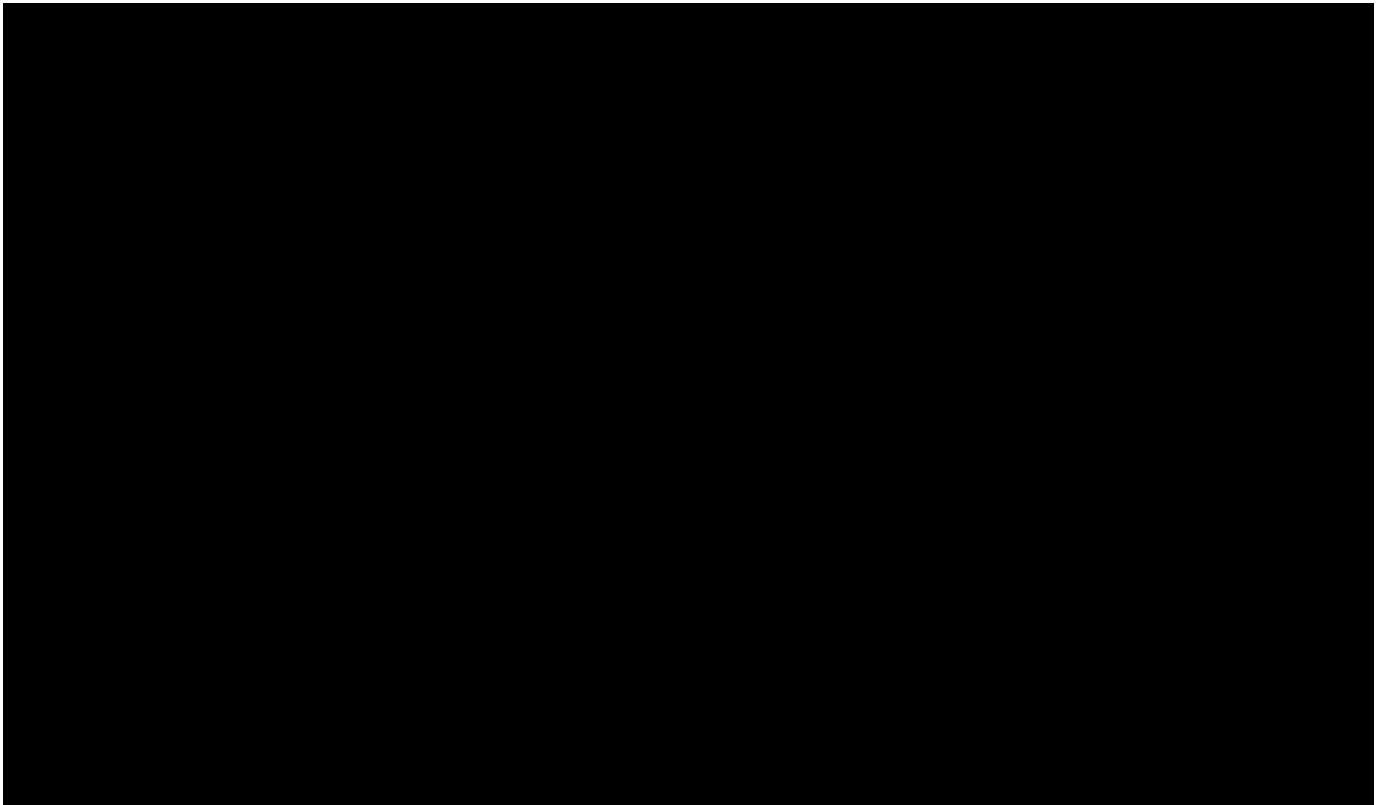
¹ In 2018, the Agency contracted with Mandiant to assess remediation activities for certain recommendations contained in its December 2017 Penetration Testing Report. Mandiant delivered that report after being contracted to assess remediation activities from its previous recommendations contained in three reports entitled *Federal Retirement Thrift Investment Board - FRTIB - External Penetration Test FINAL - v.1.0* (dated July 25, 2015); *Federal Retirement Thrift Investment Board - FRTIB - Internal Penetest [Penetration Test] FINAL - v.1.0* (dated August 25, 2015); and *Federal Retirement Thrift Investment Board - FRTIB - Web Application Assessment FINAL - v.1.0* (dated August 25, 2015).

As noted in its 2018 report, Mandiant determined that 11 of the 12 2017 report's recommendations had been effectively remediated by the Agency. Mandiant obtained additional information regarding the operating environment for the remaining finding, and based on this additional information, classified the original finding as a 'False Positive'.

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 for this performance audit were to:

- Determine whether the Agency implemented certain procedures to review and assert closure of CAPs and related prior year recommendations.
- Determine the status of certain prior Mandiant¹ TSP recommendations. Specifically, we conducted procedures over the following recommendations to determine independently whether they are closed, partially closed, or remain open:



We present four new findings and recommendations related to the Agency’s CAP process, both of which address fundamental controls. Fundamental control recommendations address significant³

² Mandiant performed several tests and differentiated them as follows: tests beginning with “EXT” were performed external to the Agency and focused on non-web site devices; tests beginning with “INT” were performed internal to the Agency; and tests beginning with “WEB” were performed external to the Agency and focused on the websites, www.tsp.gov and www.frtib.gov.

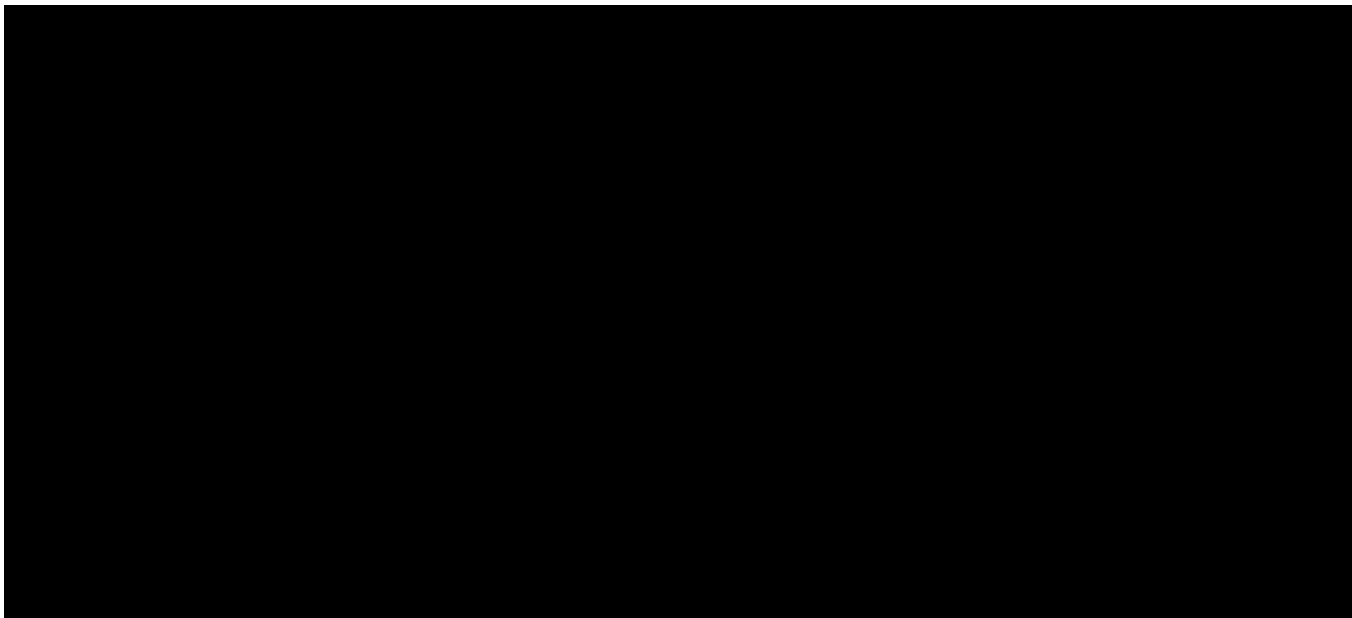
³ *Government Auditing Standards* (2011 Revision) section 6.04 defines significance in the context of a performance audit.

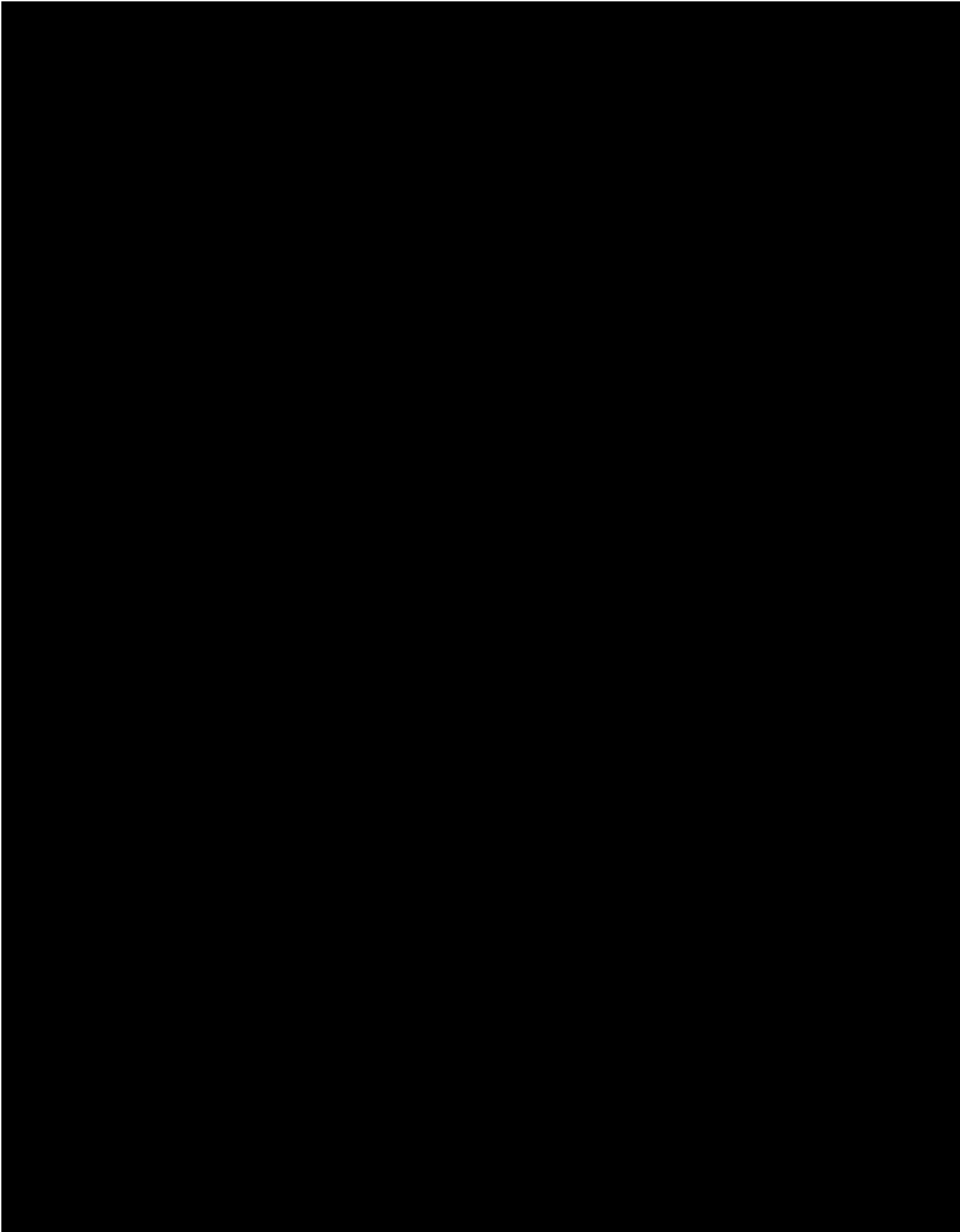
procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. All recommendations are intended to strengthen the Agency's CAP processes. 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.

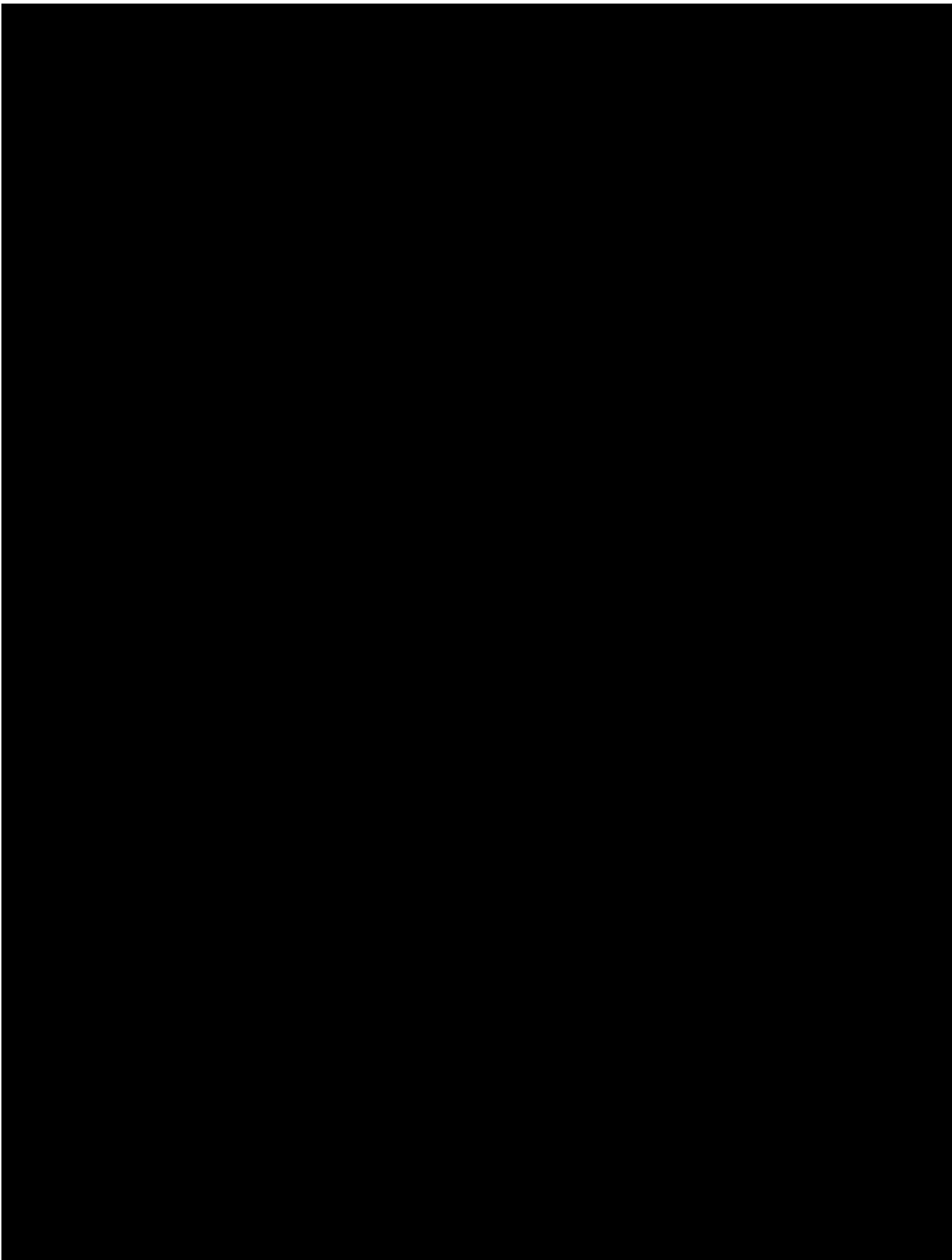
Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. As of April 18, 2019:

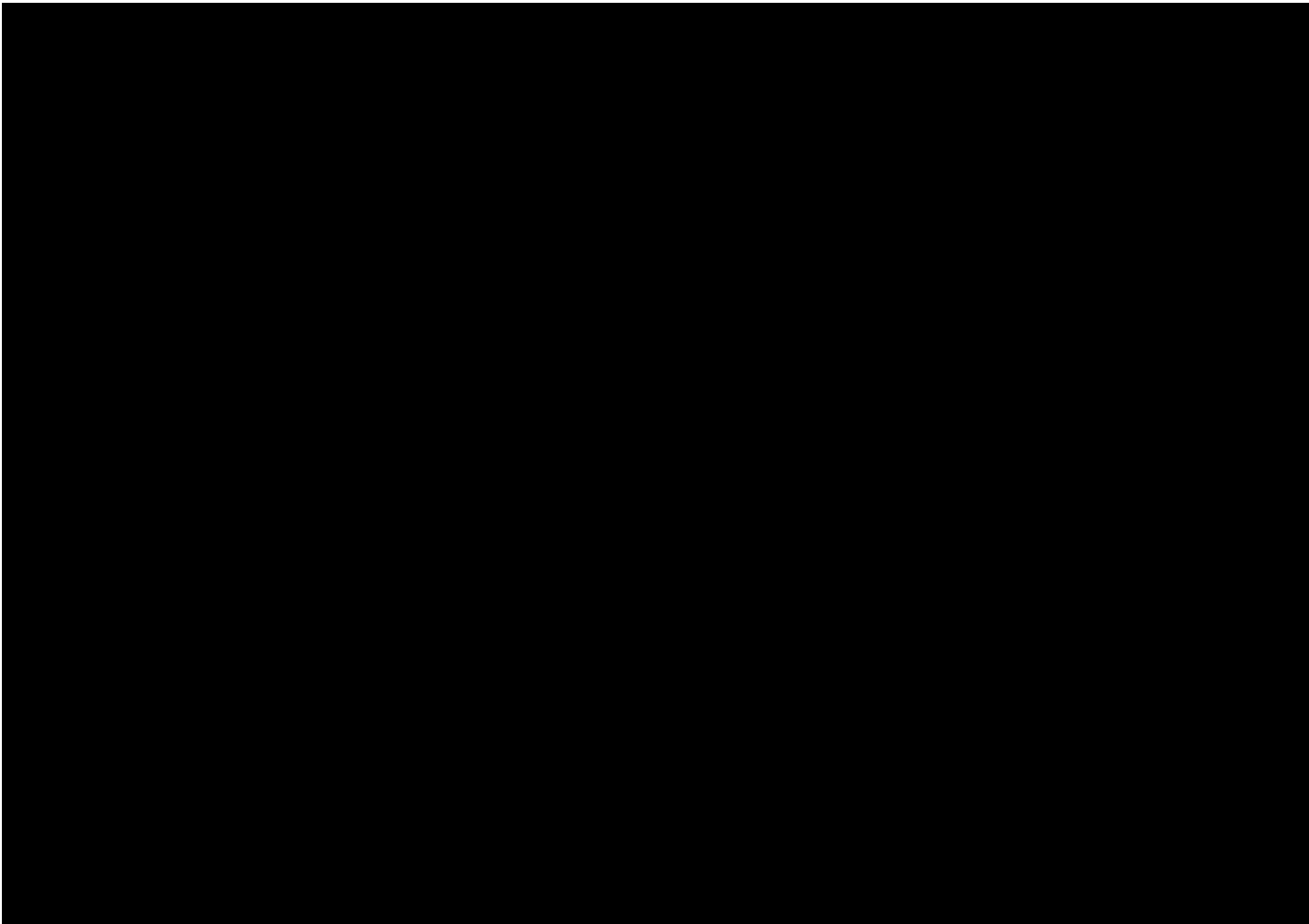
- We conclude that the Agency implemented certain procedures to review and assert closure of CAPs and related prior year recommendations; however, as indicated above, we noted internal control weaknesses in the Agency's CAP process.
- We determined the status of the 12 recommendations previously listed; in summary, all 12 recommendations were implemented and closed. However, as a result of our testing, we noted two new related technical recommendations.

The Agency's responses to the recommendations are included as an appendix to this report (Appendix A). The Agency concurred with the two new technical recommendations and did not concur with the two CAP process recommendations. We address the Agency's specific reasons for non-concurrence in the table below.









Additionally, the Agency's response to both CAP recommendations stated that the number of CAPs tested during the audit was not sufficient to change existing processes and procedures. However, we noted that the Agency's CAP process was designed and implemented as of January 2019, and at the start of our fieldwork, the Agency indicated that three CAP closure packages were completed. As such, we inspected a sample of two CAP closure packages as part of our audit procedures to perform tests of design and implementation. As a result of the procedures performed, we determined the CAP process was not designed and implemented effectively, and as such we did not perform further testing. We determined that the evidence obtained during our audit provides a reasonable basis for our findings and conclusions based on our audit objectives. Therefore, we did not make any changes to our recommendations.

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 6, 2019

II. OBJECTIVES, SCOPE, AND METHODOLOGY

A. Objectives

The U.S. Department of Labor (DOL) Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit to determine the status of certain prior Mandiant¹ recommendations, as reported on October 18, 2018, related to the Thrift Savings Plan (TSP) and directed to the Federal Retirement Thrift Investment Board's (the Board or FRTIB) Staff (Agency), and to assess the Agency's Corrective Action Plans (CAPs) process.

The objectives for this performance audit were to:

- Determine whether the Agency implemented certain procedures to review and assert closure of CAPs and related prior year recommendations.
- Determine the status of certain prior Mandiant TSP recommendations. Specifically, we conducted procedures over the following recommendations to determine independently whether they are closed, partially closed, or remain open:

	Recommendation Number⁷	Name
1.	INT-H-03	[REDACTED]
2.	INT-H-04	[REDACTED]
3.	INT-H-05	[REDACTED]
4.	INT-H-06	[REDACTED]
5.	INT-H-07	[REDACTED]
6.	INT-M-01	[REDACTED]
7.	INT-L-01	[REDACTED]
8.	INT-L-02	[REDACTED]
9.	EXT-M-01	[REDACTED]
10.	EXT-M-02	[REDACTED]
11.	WEB-L-01	[REDACTED]

⁷ Mandiant performed several tests and differentiated them as follows: tests beginning with "EXT" were performed external to the Agency and focused on non-web site devices; tests beginning with "INT" were performed internal to the Agency; and tests beginning with "WEB" were performed external to the Agency and focused on the websites, www.tsp.gov and www.frtib.gov.

	Recommendation Number⁷	Name
12.	WEB-L-02	

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 testing was performed as of April 18, 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 prior Mandiant TSP recommendations and related Agency remediation efforts. 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, and designed and performed tests of controls. We conducted these test procedures at the Agency's headquarters in Washington D.C. In Appendix B, we identify certain documentation provided by Agency and contractor personnel that we reviewed during our performance audit. However, most documentation provided during the performance audit was reviewed and maintained on-site and is not listed in this report because of the sensitive nature of the information.

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 as criteria for this engagement.

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.**