



CONTROLLED UNCLASSIFIED INFORMATION

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Independent Verification & Validation (IV&V) and Penetration Test Remediation Process

September 23, 2021

CONTROLLED UNCLASSIFIED INFORMATION

CONTROLLED UNCLASSIFIED INFORMATION

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	i
I. BACKGROUND OF THE TSP AND IV&V AND PENETRATION TEST REMEDICATION PROCESS	
A. The Thrift Savings Plan	I.1
B. TSP System	I.1
C. Overview of the IV&V Process	I.2
D. TSP Penetration Testing and Tracking Overview	I.3
II. OBJECTIVES, SCOPE, AND METHODOLOGY	
A. Objectives	II.1
B. Scope and Methodology	II.1
III. FINDINGS AND RECOMMENDATIONS	
A. Introduction	III.1
B. Finding and Recommendation Deemed Closed by the Agency’s IV&V Process	III.4
C. Findings and Recommendations from Certain Prior Penetration Tests	III.5
D. Findings and Recommendations Identified during Previous EBSA Status Determination Performance Audits	III.27
E. 2021 Finding and Recommendation	III.36
F. Summary of Open EBSA Recommendations	III.38
<u>Appendices</u>	
A. Agency’s Response	A.1
B. Key Documentation and Reports Reviewed	B.1

CONTROLLED UNCLASSIFIED INFORMATION

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, DC

As a 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) independent verification & validation (IV&V) and penetration test remediation process. We performed our fieldwork remotely from February 4, 2021 through July 23, 2021. Our scope period for testing was from January 1, 2020 to December 31, 2020.

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 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 objectives of our audit over the TSP IV&V and penetration test remediation process were to:

- Determine whether the Agency implemented certain procedures to (a) define and implement a formal process for IV&V over prior EBSA findings and recommendations, to include the role of independent third parties to assess finding and recommendation closure packages; and (b) risk rank, prioritize, and resolve penetration test results;

CONTROLLED UNCLASSIFIED INFORMATION

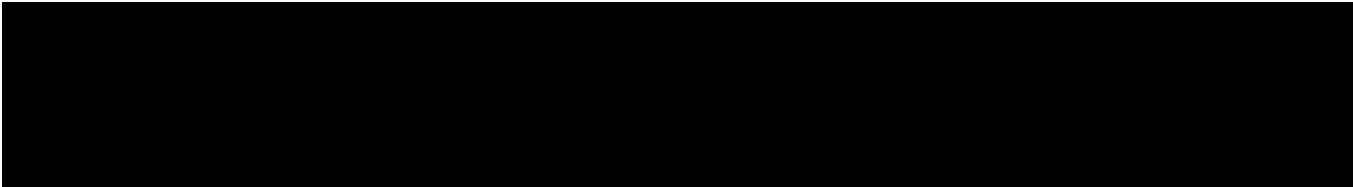
- Assess that the findings deemed to be closed by the IV&V process are closed, partially closed, or remain open;
- Assess whether the Agency's vulnerabilities over critical and high risk penetration test results were remediated or mitigated; and
- Assess the status of the prior EBSA TSP open recommendations identified in the EBSA report *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020.

We present one new finding and recommendation, which addresses a fundamental control. 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. This recommendation is intended to strengthen the TSP IV&V and penetration test remediation process. The Agency should review and consider this recommendation for timely implementation. Section III.E presents the details that support the current year finding and recommendation.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives.

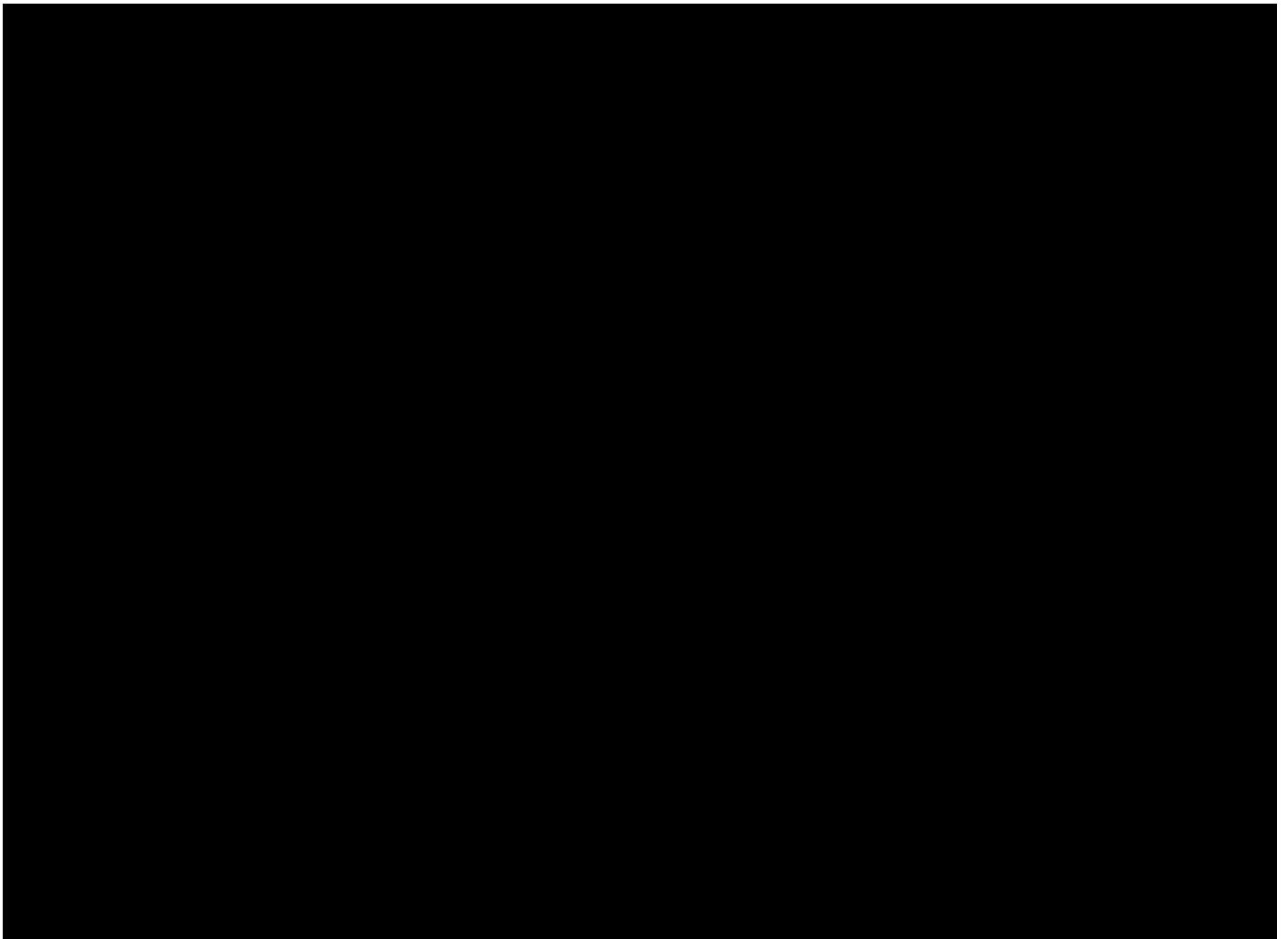
- We conclude that for the period January 1, 2020 through December 31, 2020, the Agency implemented certain procedures to (a) define and implement a formal process for IV&V over prior EBSA findings and recommendations, to include the role of independent third parties to assess finding and recommendation closure packages; and (b) risk rank, prioritize, and resolve penetration test results. However, we noted an internal control weakness in the Agency's related process.
- As of December 9, 2020, we determined the status of the following finding deemed closed by the Agency's IV&V process:

¹ *Government Auditing Standards* section 8.15 defines significance in the context of a performance audit.

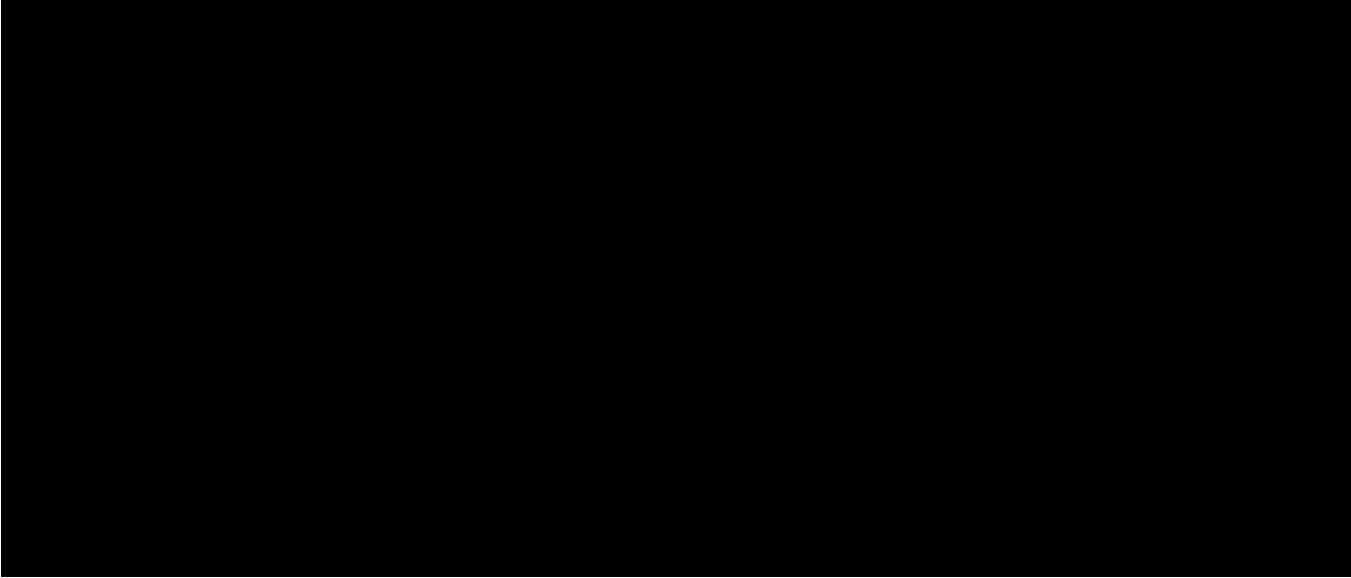


Section III.B documents our assessment of the status of the EBSA TSP sub-recommendation² noted above. In summary, we report that the sub-recommendation was implemented and closed.

- As of December 9, 2020, we also determined whether the Agency remediated or mitigated the following 19 critical and high vulnerabilities identified in prior penetration test results:



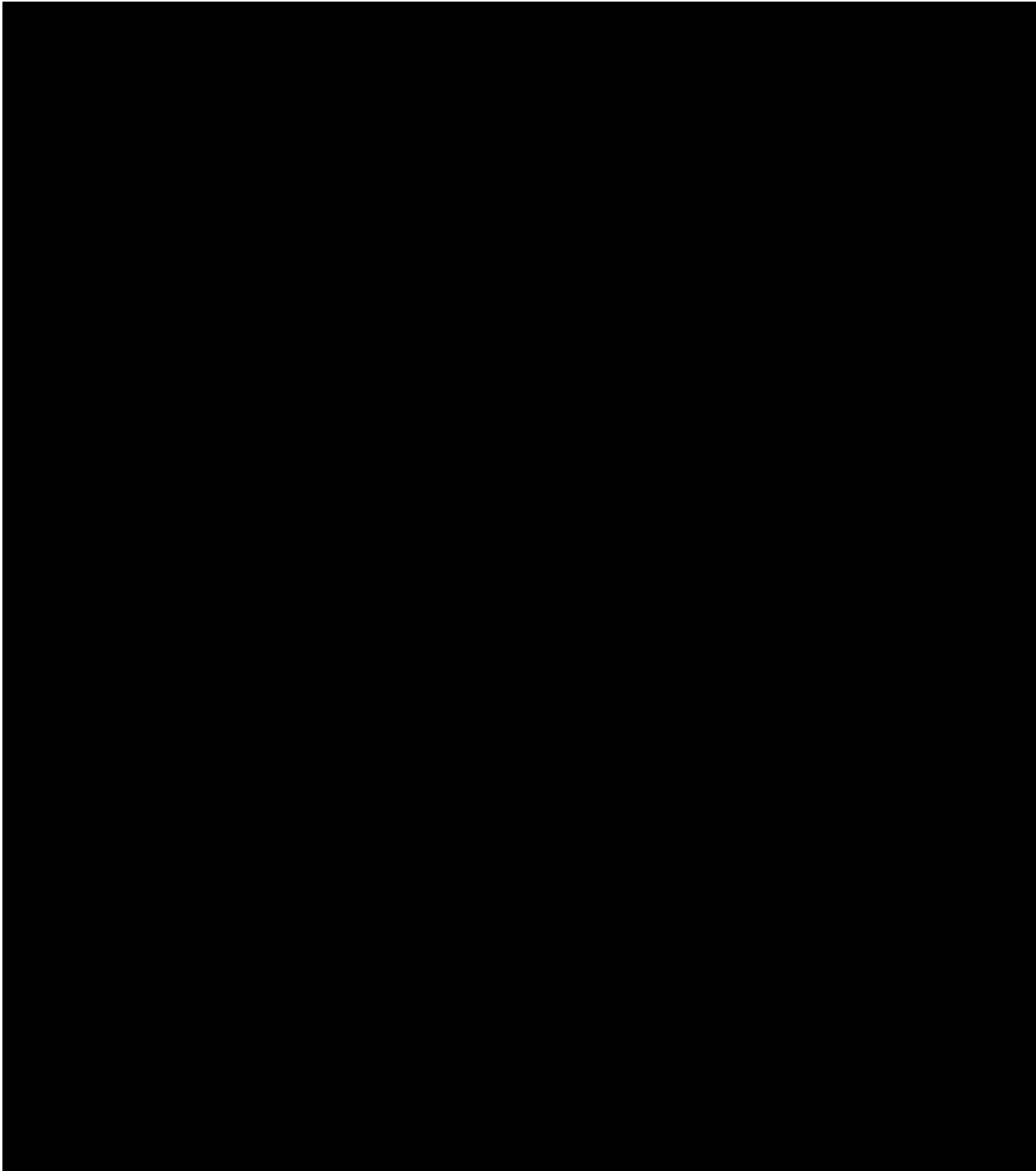
² Certain EBSA prior year recommendations have multiple components; for purposes of this report, we refer to these components as “sub-recommendations.” Recommendations are identified by a number (e.g., No. 2018-1), while sub-recommendations are identified by a number and a letter (e.g., No. 2018-2a).



Section III.C documents our assessment of the status of the 19 critical and high prior penetration test recommendations noted above. In summary, we report that 18 recommendations were implemented and closed, and one was partially implemented and remains open.

- As of December 9, 2020, we also reviewed the eight prior EBSA TSP recommendations reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020 to determine their current status. Section III.D documents the status of these prior recommendations. In summary, two recommendations were implemented and closed, one recommendation was partially implemented but is considered closed, four recommendations were partially implemented and remain open, and one recommendation was not 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 for the following:



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

CONTROLLED UNCLASSIFIED INFORMATION

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

September 23, 2021

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) independent verification & validation (IV&V) and penetration test remediation process.

The objectives of our performance audit were to:

- Determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) implemented certain procedures to (a) define and implement a formal process for IV&V over prior EBSA findings and recommendations, to include the role of independent third parties to assess finding and recommendation closure packages; and (b) risk rank, prioritize, and resolve penetration test results – this testing covered the period January 1, 2020 through December 31, 2020;
- Assess that the findings deemed to be closed by the IV&V process are closed, partially closed, or remain open – this testing was performed as of December 9, 2020;
- Assess whether the Agency's vulnerabilities over critical and high risk penetration test results were remediated or mitigated – this testing was performed as of December 9, 2020; and
- Assess the status of the prior EBSA TSP open recommendations identified in the EBSA report *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations*, dated July 22, 2020 -- this testing was performed as of December 9, 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 each objectives is identified in Section II.A. 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.

CONTROLLED UNCLASSIFIED INFORMATION

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 IV&V and penetration test remediation 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 related to the TSP IV&V and penetration test remediation process to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Participated in process walk-throughs for the IV&V process and the penetration test remediation process;
- Inspected applicable contracts and procedures for IT support services;
- Inspected policies that established the requirements for the IV&V process;
- For a selection of EBSA recommendations that underwent the IV&V process, re-performed testing to determine if the status classification was appropriate; and
- For a selection of new or re-assessed penetration test findings, inspected for evidence of the Agency's risk ranking, prioritization, and resolution of penetration test results.

We conducted these test procedures remotely in coordination with personnel primarily from the Agency's headquarters in Washington, D.C. and 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.

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