



Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Year Recommendations

July 22, 2020

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. TSP System.....	I.1
C. TSP Penetration Testing Overview.....	I.2
D. Overview of Assessment, Mitigation, and Remediation of Findings	I.2
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 Certain Prior Mandiant and EBSA Reports	III.3
C. Findings and Recommendations Identified during Previous EBSA Status Determination Performance Audits	III.16
D. 2020 Findings and Recommendations	III.21
E. Summary of Open Recommendations	III.27
<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.

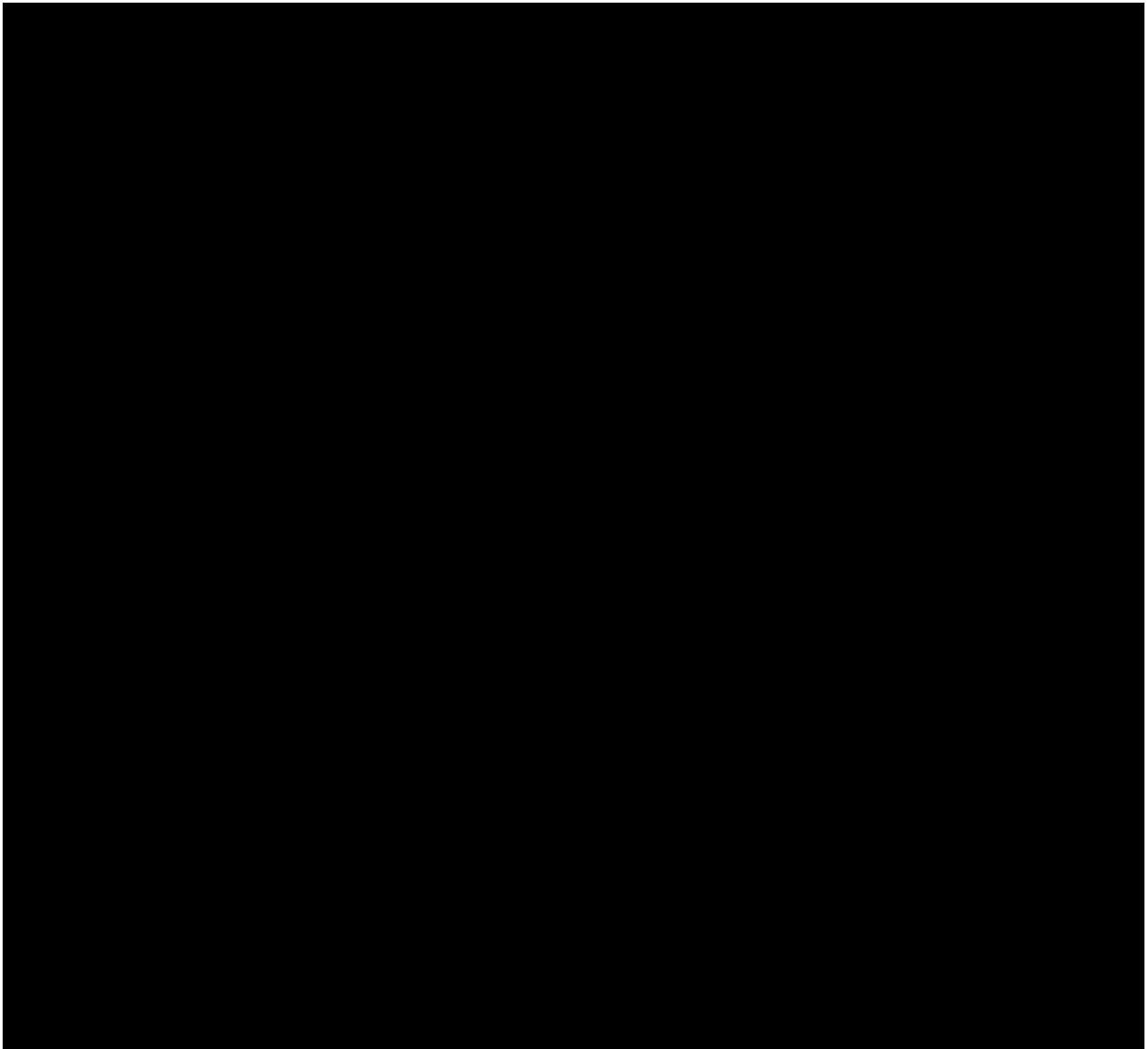
As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit to determine:

- The Federal Retirement Thrift Investment Board’s (the Board or FRTIB) Staff’s (Agency) process for managing risk related to penetration testing results and other information technology (IT) related findings and recommendations related to the Thrift Savings Plan (TSP) and directed to the Agency – this testing covered the period October 1, 2018 through December 31, 2019; and
- The status of certain prior Mandiant¹ recommendations and EBSA sub-recommendations² related to the TSP - this testing was performed as of November 26, 2019.

Our fieldwork was performed from December 12, 2019 to May 1, 2020, primarily at the Agency’s headquarters in Washington, D.C.

² We determined the status of seven prior EBSA sub-recommendations included in the report titled *Performance Audit of the Thrift Savings Plan Mobile Device Security and Governance Controls*, dated September 27, 2018. 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).

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 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 developed and implemented certain policies and procedures to assess, classify, monitor, and mitigate risks related to penetration testing results and other IT-related findings and recommendations.
- Determine the status of certain prior Mandiant¹ recommendations and EBSA sub-recommendations². Specifically, we conducted procedures over the following recommendations and sub-recommendations to determine independently whether they are closed, partially closed, or remain open:
- Determine the status of the following prior EBSA TSP open recommendations:
 - Recommendation No. 2016-01 reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Audit Recommendations*, dated April 26, 2017; and
 - Recommendation Nos. 2019-01, 2019-02, 2019-03, and 2019-04 reported in *Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations*, dated September 6, 2019.

We present three new findings and recommendations related to the Agency’s process for managing risk related to penetration test results and other IT-related findings and recommendations, all of which address fundamental controls. Fundamental control recommendations address significant³ 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 processes for managing risk related to penetration test results and other IT-related

³ *Government Auditing Standards* section 8.15 defines significance in the context of a performance audit.

findings and recommendations. The Agency should review and consider these recommendations for timely implementation. Section III.D 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.

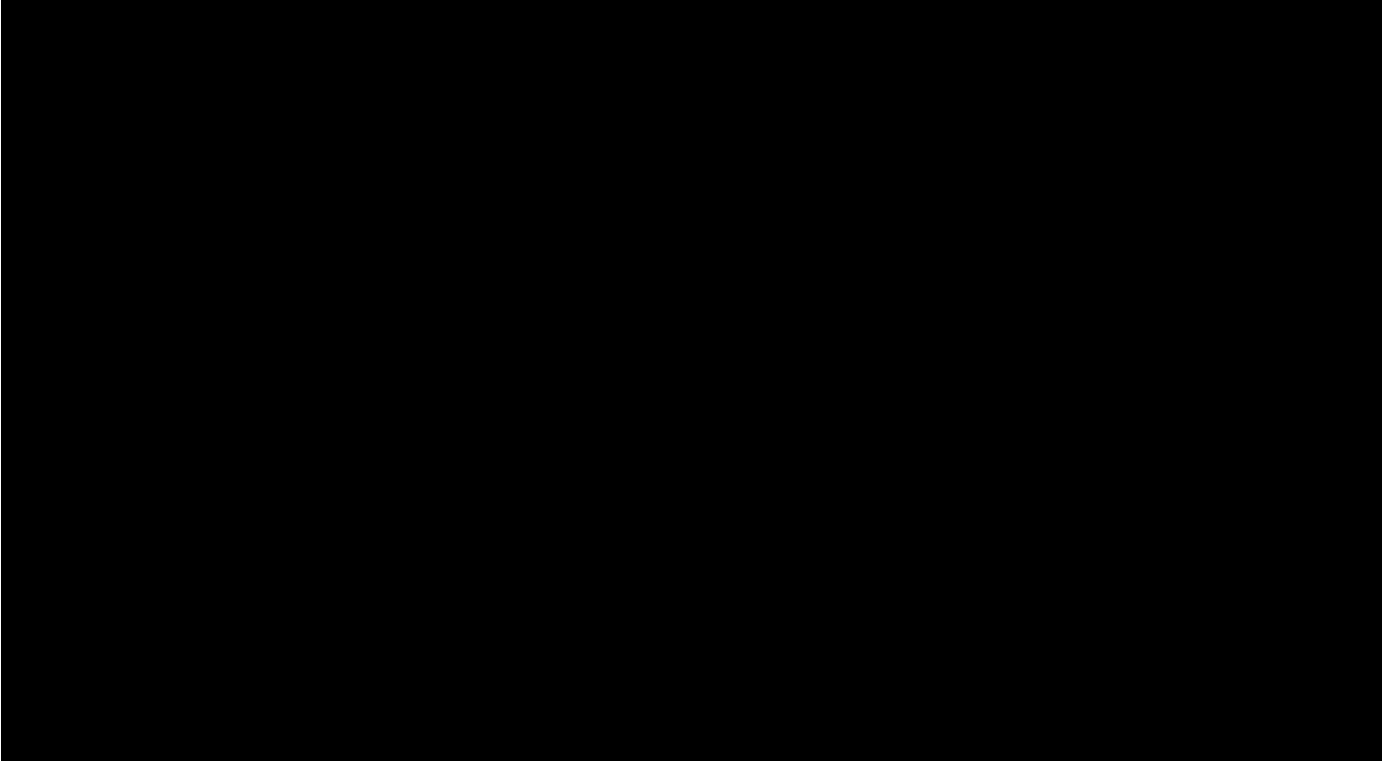
- We conclude that for the period October 1, 2018 through December 31, 2019, the Agency developed and implemented certain policies and procedures to assess, classify, monitor, and mitigate risks related to penetration testing results and other IT-related audit findings. As indicated above, we noted weaknesses in the Agency's related process.
- As of November 26, 2019, we determined the status of the 16 recommendations and sub-recommendations previously listed. Section III.B documents the status of these prior recommendations and sub-recommendations. In summary, 13 recommendations and sub-recommendations were implemented and closed, and three sub-recommendations were not implemented but are considered closed.

We also reviewed the following five prior EBSA TSP recommendations to determine their current status:

- Recommendation No. 2016-01 reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Audit Recommendations*, dated April 26, 2017; and
- Recommendation Nos. 2019-01, 2019-02, 2019-03, and 2019-04 reported in *Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations*, dated September 6, 2019.

Section III.C documents the status of these prior recommendations. In summary, all five recommendations were not implemented and remain open.

The Agency's responses to the recommendations are included as an appendix to this report (Appendix A). The Agency concurred with the three new recommendations and two prior year recommendations and did not concur with the two prior year Corrective Action Plan (CAP) process recommendations. We address the Agency's non-concurrence in the table below.



In addition, we noted in the Agency's response to recommendation no. 2020-03 that management concurs and considers the recommendation closed. However, Agency management did not provide evidence that they required all Technical Vulnerability Remediation and CAP documentation supporting the remediation activity summary statements throughout the remediation process to be retained as audit evidence either in service tickets or by reference in those tickets. The Agency also did not indicate when the noted documentation retention requirement went into effect. As such, we did not make any changes to our recommendation.

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

July 22, 2020

II. OBJECTIVES, SCOPE, AND METHODOLOGY

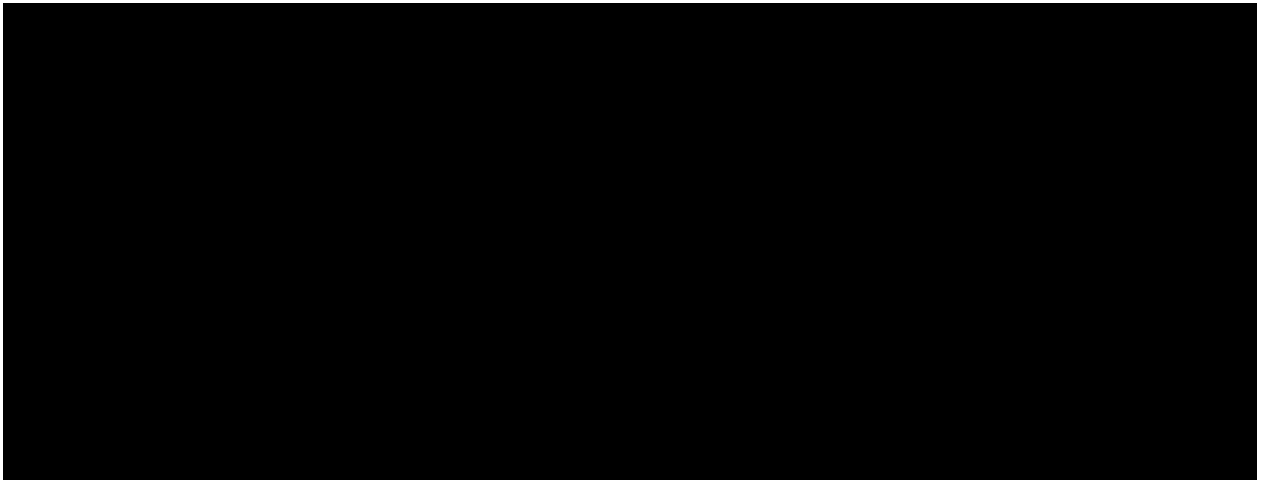
A. Objectives

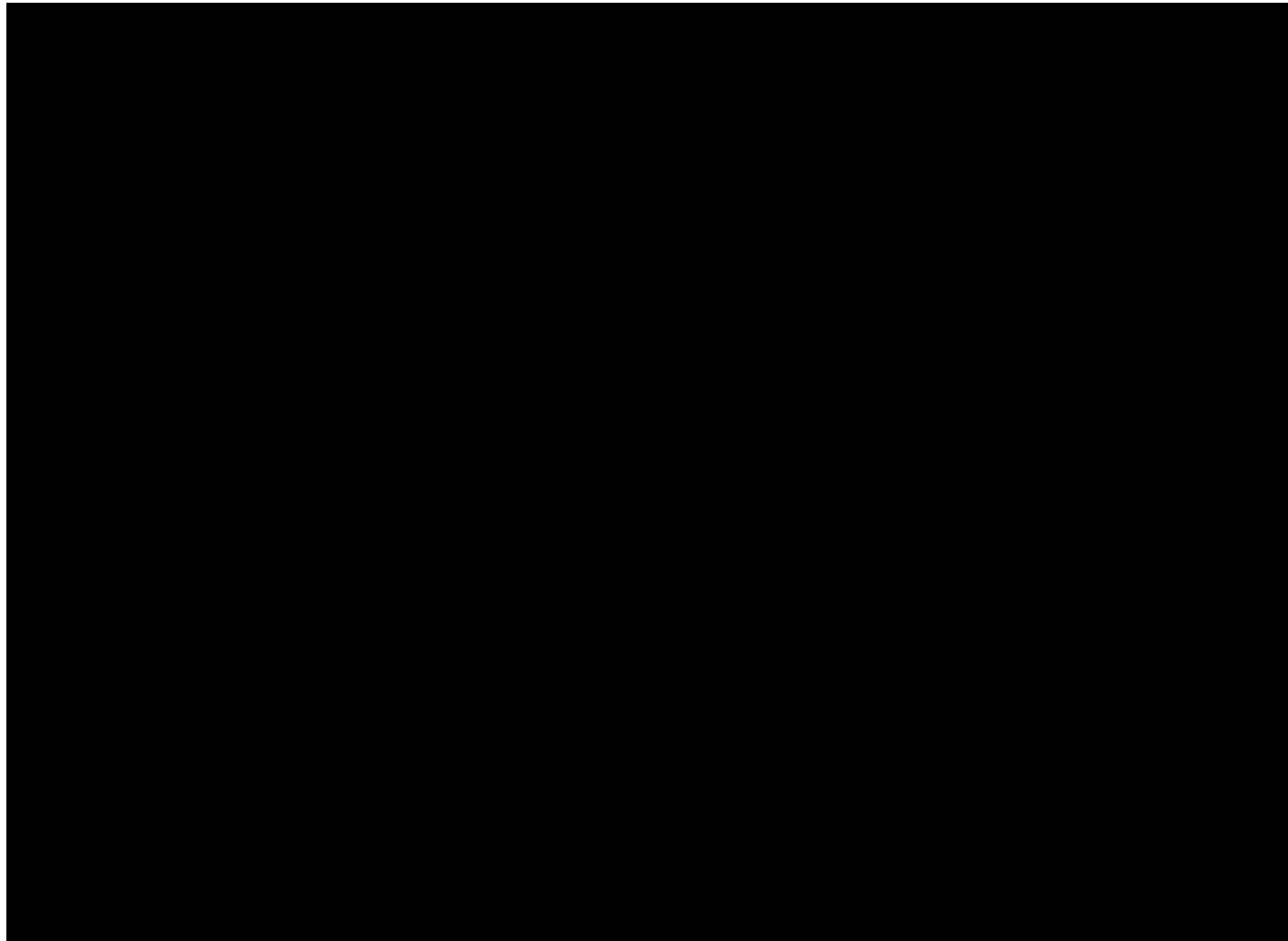
The U.S. Department of Labor (DOL) Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit to determine:

- The Federal Retirement Thrift Investment Board's (the Board or FRTIB) Staff's (Agency) process for managing risk related to penetration testing results and other information technology (IT) related findings and recommendations related to the Thrift Savings Plan (TSP) and directed to the Agency; and
- The status of certain prior Mandiant¹ recommendations and EBSA sub-recommendations² related to the TSP as of November 26, 2019.

The objectives for this performance audit were to:

- Determine whether the Agency developed and implemented certain policies and procedures to assess, classify, monitor, and mitigate risks related to penetration testing results and other IT related findings and recommendations.
- Determine the status of certain prior Mandiant¹ recommendations and EBSA sub-recommendations². Specifically, we conducted procedures over the following recommendations and sub-recommendations to determine independently whether they are closed, partially closed, or remain open:



- 
- Determine the status of the following prior EBSA TSP open recommendations:
 - Recommendation No. 2016-01 reported in *Performance Audit of the Thrift Savings Plan Status Determination of Certain Prior Audit Recommendations*, dated April 26, 2017; and
 - Recommendation Nos. 2019-01, 2019-02, 2019-03, and 2019-04 reported in *Performance Audit of the Thrift Savings Plan Corrective Action Plans Process and the Status Determination of Certain Prior Year Recommendations*, dated September 6, 2019.

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 scope period for Objective 1 was October 1, 2018 through December 31, 2019, and for Objective 2 was as of November 26, 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 IT and 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.**