KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan National Defense Authorization Act Pre-Implementation Controls No. 2

December 5, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Members of the Federal Retirement Thrift Investment Board
Washington, D.C.

Michael Auerbach
Acting 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 second performance audit of the Thrift Savings Plan (TSP) National Defense Authorization Act for Fiscal Year 2016[1] (NDAA) pre-implementation controls. Our fieldwork was performed from June 26, 2017 through September 30, 2017, at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2017 through August 31, 2017. Near the end of fieldwork, we received additional documentation through September 2017 in response to our audit inquiries and considered it when concluding on our audit objectives.

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 Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The objectives of our audit over the TSP NDAA pre-implementation controls were to:

[1] Certain components of the NDAA require the automatic enrollment of new uniformed service members into the TSP, payment of both automatic and matching TSP contributions up to a certain level, and the ability for current service members to opt-in to the new program while maintaining the majority of the current military retirement system.

- Determine whether the Agency has continued to develop configuration and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA.

- Determine whether the Defense Finance and Accounting Service has developed configuration and processing procedures for the setup, transfer, management, and reporting of TSP contributions related to the upcoming changes required by the NDAA.

- Determine whether uniformed services have developed and implemented procedures for determining the uniformed services members eligible for enrollment under NDAA and notifying eligible members of their enrollment options.

However, because we were not granted access to personnel, facilities, and documentation timely by the Office of the Assistant Secretary of Defense, we were not able to meet the second and third audit objectives listed above. This situation was discussed promptly with EBSA, and EBSA directed us to complete the audit with the first audit objective only.

We present one new recommendation related to TSP NDAA pre-implementation controls, which addresses fundamental controls. Fundamental control recommendations address significant[2] 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. The recommendation is intended to strengthen TSP NDAA pre-implementation controls. The Agency should review and consider this recommendation for timely implementation. Section III.C presents the details that support the current year finding and recommendation.

In addition, we identified a deficiency that does not require a new recommendation because it is covered under an open recommendation in another EBSA report. This deficiency is reported herein for informational purposes only.

Based upon the performance audit procedures conducted and the results obtained, we have met one of our three audit objectives. We conclude that for the period January 1, 2017 through August 31, 2017, the Agency continued to develop configuration and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required

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

by the NDAA. However, as indicated above, we noted internal control weaknesses in certain TSP NDAA pre-implementation controls.

We also reviewed two prior EBSA recommendations related to TSP NDAA pre-implementation controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, both recommendations have been partially implemented and remain 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 concurs with the two open prior year recommendations; however, the Agency does not concur with Recommendation No. 2017-01. Based on the Agency's response to that recommendation, we revised our criteria to the National Institute of Standards and Technology's Risk Management Framework risk acceptance process. However, the Agency did not resolve the noted deficiency prior to the end of our audit work as the risk mitigation documentation the Agency developed was in draft form at that time.

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

December 5, 2017

I. BACKGROUND OF THE TSP AND THE NATIONAL DEFENSE AUTHORIZATION ACT PRE-IMPLEMENTATION ACTIVITIES

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act of 1986 (FERSA), as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS) and provides a Federal (and, in certain cases, State) income tax deferral on employee contributions and related earnings. The TSP is available to Federal and Postal employees, members of the uniformed services, and members of Congress and certain Congressional employees. The TSP began accepting contributions on April 1, 1987, and as of July 31, 2017, had approximately $511 billion in assets and approximately 5.1 million participants[3].

The FERSA also established the Federal Retirement Thrift Investment Board (the Board) and the position of Executive Director. The Executive Director manages the TSP for its participants and beneficiaries. The Board's Staff (Agency) is responsible for administering TSP operations.

B. National Defense Authorization Act[4]

On November 25, 2015, the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) (NDAA) was signed into law. The NDAA required the creation of a "blended" retirement system for all uniformed services members who enter service beginning January 1, 2018. The current military retirement system establishes a retirement allocation of 2.5 times a service member's pay for their high-three years of service. NDAA changed that calculation for new and certain time-in-service voluntary participants by re-allocating to the TSP up to 0.5 times their pay for the high-three years of service. The project often is referred to as "blended retirement" because of this re-allocation of a portion of the overall military retirement package.

Specifically, NDAA required the automatic enrollment of new uniformed service members into the TSP and provided for immediate, automatic one percent and matching contributions to the TSP for these members. The NDAA also provided to uniformed service members with less than 12

[3] Source: Minutes of the August 28, 2017, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

[4] Source: *Blended Retirement Charter*, dated January 20, 2016.

years of service as of January 1, 2018 the opportunity to elect retirement coverage under this new "blended" retirement system.

Currently, uniformed services members are initiated to the TSP through contact from their service. TSP participant data and transactions include participant name, other verifying information, employee contributions, employer contributions, investment earnings, participant loans, withdrawals, and transfers. New uniformed service participants will follow the existing TSP enrollment, maintenance, and retirement processes established for all participants. The Agency expects enrollment to climb substantially as a result of the automatic and voluntary enrollment of new uniformed service members into the TSP.

1. Configuration Controls[5]

The Agency is responsible for implementing and maintaining configuration controls over its information technology infrastructure. The NDAA implementation relies on these existing configuration controls to address changes necessary to support improvements to this infrastructure, including changes to storage devices, additional network traffic capacity, and increases to processing power and memory.

Risks to the upcoming NDAA implementation may include, but are not limited to, participant data processing bottlenecks, backup and recovery replication issues, and reduced nightly processing performance. Configuration changes at appropriate and different levels of the Agency's information infrastructure could mitigate these risks.

2. Capacity Planning[6]

In order to accommodate the influx of participants, the Agency completed certain capacity planning activities. Capacity planning involves the management and forecasting of data and processing capabilities to meet defined service level requirements. The Agency is primarily responsible for capacity planning efforts, with its technical support contractors and the original equipment manufacturers supporting these efforts. Specific responsibilities include capacity planning, system capability, and hardware performance.

---

[5] Source: *Task Order #42 FRTIB IT Environment Current/Future State Gap Analysis and Recommendations Document,* version 1.0, dated January 31, 2017.

[6] Source: *Blended Capacity Phase 2 Test Plan*, version 1.1, December 12, 2016.

C. TSP System[7]

The TSP Recordkeeping Systems (TSP system) are a collection of applications that store participant data; value accounts daily; process and record loans and withdrawals; record contributions; and process interfund transfer requests for TSP participants and beneficiaries. The design of the TSP system is based on interrelating commercial-off-the shelf (COTS) software that requires the Agency to modify certain business processes to provide enhanced functionality.

The TSP system balances several COTS software packages (e.g., recordkeeping, voice response, accounting, workflow, and imaging) with customized components for enhanced usability (e.g., payroll interfaces, participant support, and reporting). The TSP system is comprised of a dedicated IBM mainframe with the z/OS platform; SunGard's OmniPlus, a COTS 401(k) recordkeeping software application for primary recordkeeping; and IBM blade and Dell rack-mounted servers for ancillary processing. The TSP's client/server environment generally supports the front-end processing, while the mainframe supports the back-end and nightly processing and data repositories. The core recordkeeping software application and supporting infrastructure are housed in the primary data center located in Virginia.

[7] Source: *Serena Business Manager User Guide, Software Change Management*, version (v.) 9.0, dated January 2016

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) National Defense Authorization Act for Fiscal Year 2016 (NDAA) pre-implementation controls.

The objectives of our audit over the TSP NDAA pre-implementation controls were to:

- Determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) has continued to develop configuration and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA.

- Determine whether the Defense Finance and Accounting Service has developed configuration and processing procedures for the setup, transfer, management, and reporting of TSP contributions related to the upcoming changes required by the NDAA.

- Determine whether uniformed services have developed and implemented procedures for determining the uniformed services members eligible for enrollment under NDAA and notifying eligible members of their enrollment options.

However, because we were not granted access to personnel, facilities, and documentation timely by the Office of the Assistant Secretary of Defense, we were not able to meet the second and third audit objectives listed above. This situation was discussed promptly with EBSA, and EBSA directed us to complete the audit with the first audit objective only.

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, 2017 through August 31, 2017. 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 NDAA pre-implementation activities. 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 NDAA pre-implementation activities;
- Examined key reports;
- Examined Agency-developed analytic and forecasting studies; and
- Reviewed NDAA project implementation planning documentation.

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

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.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We performed procedures related to the Thrift Savings Plan (TSP) National Defense Authorization Act for Fiscal Year 2016 (NDAA) pre-implementation controls while conducting a performance audit at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters. Our scope period for testing was January 1, 2017 through August 31, 2017. This performance audit consisted of reviewing applicable policies and procedures and testing manual and automated processes and controls, which included interviewing key personnel, reviewing key reports and documentation (Appendix B), and observing selected procedures.

Our original audit scope included three objectives. However, because we were not granted access to personnel, facilities, and documentation timely by the Office of the Assistant Secretary of Defense, we were not able to meet the following two audit objectives:

- Determine whether the Defense Finance and Accounting Service has developed configuration and processing procedures for the setup, transfer, management, and reporting of TSP contributions related to the upcoming changes required by the NDAA.

- Determine whether uniformed services have developed and implemented procedures for determining the uniformed services members eligible for enrollment under NDAA and notifying eligible members of their enrollment options.

This situation was discussed promptly with EBSA, and EBSA directed us to complete the audit with the Agency-focused audit objective identified in the following paragraph, only.

Based upon the performance audit procedures conducted and the results obtained, we have met one of our three audit objectives. We conclude that for the period January 1, 2017 through August 31, 2017, the Agency continued to develop configuration and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA. However, we noted internal control weaknesses in certain TSP NDAA pre-implementation controls.

We present one new recommendation, presented in Section III.C, related to TSP NDAA pre-implementation controls, which addresses fundamental controls. Fundamental control

recommendations address significant 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. The Agency should review and consider this recommendation for timely implementation. The Agency's response to this recommendation is included as an appendix within this report (Appendix A).

In addition, we identified one deficiency that does not require a new recommendation because it is covered under an open recommendation in another U.S. Department of Labor Employee Benefits Security Administration (EBSA) report. This deficiency is reported herein for informational purposes only.

We also reviewed two prior EBSA recommendations related to TSP NDAA pre-implementation controls to determine their current status. Section III. B documents the status of these prior recommendations. In summary, both recommendations have been partially implemented and remain open.

Section III.C presents the finding and recommendation from this performance audit. Section III.D summarizes each open recommendation.

B. Findings and Recommendations from Prior Reports

The findings and recommendations from prior reports that required follow-up are presented in this section. The discussion below includes the current status of each recommendation.

2016 NDAA Pre-Implementation Recommendation No. 1:

Title: Weaknesses in Blended Retirement Capacity Study

Original Recommendation: To strengthen capacity planning activities related to the NDAA implementation, the Agency should:

a. Evaluate and document the potential impact to the bandwidth load between the production and alternate processing sites with consideration of an increase of 15% or greater traffic increase;
b. Either:
    i. More clearly document the rationale supporting the assumptions leading to a lower maximum enrollee threshold used in initial load analyses and other forecasting activities, or

ii. Increase the maximum number of enrollees based on a worst case scenario, and update the study; and

c. Document the assumptions and expectations leading to the decision to maintain the current hardware and software platforms used in the primary and alternate processing sites.

Reason for Recommendation: We noted the following weaknesses in the Agency's capacity study in support of the blended retirement project (BRP) implementation required by NDAA:

- The capacity study did not document the Agency's consideration of an increase in data replication traffic between the primary data center and the alternate processing site;
- The capacity planning study projected a maximum 750,000 would enroll compared to the possible 1,188,314 maximum number of potential enrollees, but the Agency's justification for the reduced maximum number of enrollees was not documented in the capacity planning and analysis information provided; and
- The capacity study did not evaluate existing hardware and software at the alternate processing site or any upgrades to the alternate processing site needed to meet anticipated capacity demands of the upcoming NDAA implementation.

Status: **Partially Implemented.**

a) During our fieldwork, we were not provided evidence that the Agency had analyzed and improved the communications capabilities between the two data centers. As a result, this portion of the recommendation remains open.

b) The Agency had documented the rationale for using the repeated Monte Carlo simulation to determine the upper limit of enrollees or revise the upper limit to the worst case maximum number of enrollees. As a result, this portion of the recommendation is closed.

c) The Agency had documented the assumptions and expectations that supported the decision to maintain the current hardware and software platforms used in the primary and alternate processing sites. As a result, this portion of the recommendation is closed.

Disposition: **Recommendation Open.**

2016 NDAA Pre-Implementation Recommendation No. 2:

Title: Weaknesses in NDAA Project Management Timelines

Original Recommendation: To strengthen controls over NDAA project management timelines, the Agency should:

a. Re-evaluate and realign conflicting timelines identified across Agency documentation, including the *Part II Plan for Task Order #42 Subtask 2 Blended Retirement Capacity*, *Blended Retirement CSSQ Baseline Agreement: Management Stage Gate #*2, and other remediation plans;
b. Document in the project risk register contingencies such as larger-than-forecast influx of military participants and unexpected increase in network traffic, and prepare mitigation plans with consideration of additional project resources to maintain and support the legally-required implementation date; and
c. Develop and implement test procedures under the 2017 annual disaster recovery test for the additional forecasted influx of new participants expected after the NDAA implementation.

Reason for Recommendation: During our test work, we noted the following weaknesses in several of the Agency's NDAA-related project and subtask timelines:

- The Agency developed a baseline agreement with its contractor for the blended retirement project in August 2016. However, the stated completion date did not support unanticipated and significant contingencies.
- Our analysis of the February 2017 revised capacity plan indicated that, were all the milestones to be completed as documented, the contractor would complete the capacity and other NDAA project subtasks in early December, not the September deadline in the baseline agreement discussed above.
- The revised capacity remediation plan documented several related tasks otherwise outside of the scope of the BRP efforts. These other tasks may adversely impact the Agency's ability to meet the required implementation date.

Additionally, management indicated that the Agency had not planned to perform additional testing for the expected increase in capacity during the annual disaster recovery test.

Status: **Partially Implemented.**

a) We inspected the project timeline documentation, revised in June 2017, that supports the *Part II Plan for Task Order #42 Subtask 2 Blended Retirement Capacity* task order, and noted that the timelines had been re-aligned and included timeframes for remediating the weaknesses identified in the capacity study. As a result, this portion of the recommendation is closed.

b) We inspected the project risk register and noted that the Agency had documented its acceptance of the risk that certain contingencies, such as larger-than-forecast influx of military participants and unexpected increase in network traffic, would cause nightly processing to not be completed within service level-required timeframes. Additionally, we examined documents that supported the Agency's risk acceptance and risk mitigation activities and noted that the Agency had developed a strategy to address an unanticipated influx of new participants. As a result, this portion of the recommendation is closed.

c) As of the end of our fieldwork, the Agency had not yet performed its 2017 disaster recovery test. As a result, this portion of the recommendation remains open.

Disposition: **Recommendation Open.**

C. 2017 Findings and Recommendation

While conducting our performance audit over TSP NDAA pre-implementation controls, we identified two new findings and developed one related recommendation, as one deficiency is covered by an open recommendation in another EBSA report. EBSA requests appropriate and timely action for the recommendation.

RECOMMENDATION TO ADDRESS FUNDAMENTAL CONTROLS

2017-01: Weaknesses in Finalizing Risk Acceptance Documentation

Although the Agency determined that certain NDAA-related risks identified in its risk register could not be avoided, its drafted risk acceptance memorandum was not finalized by the end of our fieldwork. This draft risk acceptance memorandum stated that, while unlikely, the Agency could experience a greater-than-expected influx of new participant accounts to be added to the TSP in a single night. Were it to occur, such an unusual influx would cause significant processing delays that would delay downstream investing and reporting processes.

In addition, we inspected the *Task Order 42 Subtask 3 Capacity Recommended Approach for Processing Enrollments for Blended Retirement System*, version 2.0, dated September 14, 2017, which was watermarked "DRAFT"; the *Standard Operating Procedure New Enrollment Limit Exceeded in API Edits*, dated September 5, 2017, which was watermarked "DRAFT"; and the *Limit Count of New Enrollments Submitted for a Single Unified- Draft*, dated September 5, 2017, a memorandum that was watermarked "DRAFT" and stated that the Agency had mitigating procedures in place should such a scenario occur. However, the final Agency management review and approval of these documents had not yet occurred, or was not documented as having occurred. Therefore, the Agency did not complete the risk acceptance process for the NDAA implementation contingency event. Management indicated they did not plan to finalize and approve the mitigation strategy until closer to the end of calendar year 2017.

The National Institute of Standards and Technology's Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010, states:

> Risk Acceptance
> TASK 5-4: Determine if the risk to organizational operations, organizational assets, [and] individuals […]
> Supplemental Guidance: The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. […] The authorizing official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials, including the organization's risk executive (function). […]

The authorization decision document conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. [p. 35-36]

1. **To strengthen capacity planning activities related to the NDAA implementation, the Agency should finalize risk acceptance documentation and mitigating procedures (e.g., delaying certain transactions for 24 hours to meet service level metrics) related to potential issues of the maximum enrollee processing threshold before NDAA is implemented.**

The risk acceptance weakness may lead the Agency to not be fully prepared to meet the increased demands for information processing and storage after the NDAA implementation, which may lead to unplanned, negative impacts to the Agency's information infrastructure.

2017-02: Insufficient Capacity Testing

During our fieldwork, we noted that Agency policies did not include stress testing requirements based on upcoming capacity needs, such as those related to NDAA implementation. Further, while the Agency relied on a mainframe-specific capacity forecasting report, we noted that the Agency had not fully tested maximum anticipated NDAA-related capacity in the production environment, but rather in a test environment.

We determined that the open service continuity controls recommendation no. 2013-07, *Capacity Planning Weaknesses,* most recently included in the report *Performance Audit of the Thrift Saving Plan Service Continuity Controls,* dated January 31, 2017, addresses this deficiency. Therefore, this specific exception does not require a new recommendation.

The implementation of capacity testing in the production environment will assist the Agency in better managing existing technology resources and forecasting capacity needs.

D. Summary of Open Recommendations

2016 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in Blended Retirement Capacity Study

1. To strengthen capacity planning activities related to the NDAA implementation, the Agency should:
   a. Evaluate and document the potential impact to the bandwidth load between the production and alternate processing sites with consideration of an increase of 15%[8] or greater traffic increase;

Weaknesses in NDAA Project Management Timelines

2. To strengthen controls over NDAA project management timelines, the Agency should:
   c. Develop and implement test procedures under the 2017 annual disaster recovery test for the additional forecasted influx of new participants expected after the NDAA implementation.

2017 RECOMMENDATION

RECOMMENDATION TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in Updating Risk Acceptance Documentation

1. To strengthen capacity planning activities related to the NDAA implementation, the Agency should finalize risk acceptance documentation and mitigating procedures (e.g., delaying certain transactions for 24 hours to meet service level metrics) related to potential issues of the maximum enrollee processing threshold before NDAA is implemented.

[8] Increase of 750,000 participants (i.e., the maximum projected enrollees used in the study) represents a 15% increase in current TSP participants.

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77K Street, NE Washington, DC 20002

December 5, 2017

Mr. Michael Auerbach
Acting Chief Accountant
Employee Benefits Security Administration
United States Department of Labor
Suite 400
122 C Street, N.W.
Washington, D.C. 20001-2109

Dear Michael:

This is in response to KPMG's email of November 30, 2017, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan National Defense Authorization Act Pre-Implementation Controls No. 2 dated December 2017. My comments with respect to this report are enclosed.

Thank you once again for the constructive approach that the Department of Labor and its contractors are taking in conducting the various audits of the TSP. The information and recommendations that are developed as a result of your reviews are useful to the continued improvement of the Thrift Savings Plan.

Very truly yours,

Ravindra Deo

Ravindra Deo

Enclosure

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77K Street, NE Washington, DC 20002

Agency Staff Formal Comments on the
Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan
National Defense Authorization Act
Pre-Implementation Controls No. 2

Prior Year Findings to Address Fundamental Controls

2016-1: Weaknesses in Blended Retirement Capacity Study

To strengthen capacity planning activities related to the NDAA implementation, the Agency should:

a) Evaluate and document the potential impact to the bandwidth load between the production and alternate processing sites with consideration of an increase of 15% or greater traffic increase.

2017 Status

a) At the end of our fieldwork, the Agency was in the process of assessing the potential additional bandwidth load to the production and alternate data centers resulting from the NDAA implementation. The Agency plans to complete this assessment by the end of October. As a result, this portion of the recommendation remains open.

Agency Response:

The Agency concurs with the finding and considers this closed. The Agency performed a documented assessment with projected 15% participant bandwidth and growth over 10 years and concluded the 10GB circuits are sufficient. The Agency performs continuous monitoring on bandwidth utilization, and has alerts configured when utilization exceeds 85%. The Agency completed the network Data Center Interconnects (DCI) circuit upgrades from 1GB to 10GB in August 2016 and finalized in May 2017, as part of an enterprise circuit upgrade effort.

2016-2: Weaknesses in NDAA Project Management Timelines

To strengthen controls over NDAA project management timelines, the Agency should:

c) Develop and implement test procedures under the 2017 annual disaster recovery test for the additional forecasted influx of new participants expected after the NDAA implementation.

2017 Status

c) As of the end of our fieldwork, the Agency had not yet performed its 2017 disaster recovery test. As a result, this portion of the recommendation remains open.

Agency Response:
The Agency concurs with the finding. The Agency acknowledges the request for load testing between the production and alternate data center sites as part of disaster recovery exercise (DRE). The DRE is designed to test the ability to recover mainframe and distributed systems data using tape medium at the alternate data center. The data that is recovered is production data. Since NDAA will not be live in production at the time of the 2017 annual DRE, which occurs the week of November 13th, the data will not include the 2018 influx of new participants.

The Agency will perform the 2018 annual DRE by June 2018. This DRE will include the influx of new participants as a result of the January 2018 implementation of NDAA. The results and analysis of the 2018 annual DRE will be available by October 31, 2018 and the Agency plans to close this finding by December 31, 2018.

2017 Findings to Address Fundamental Controls

2017-1: Weaknesses in Finalizing Risk Acceptance Documentation

To strengthen capacity planning activities related to the NDAA implementation, the Agency should finalize risk acceptance documentation and mitigating procedures (e.g., delaying certain transactions for 24 hours to meet service level metrics) related to potential issues of the maximum enrollee processing threshold before NDAA is implemented.

Agency Response:
The agency does not concur with the finding.

The Agency prepared a risk mitigation strategy, rather than a risk acceptance, for the NDAA capacity and service level metric risk. As a mitigation strategy, the Agency has instituted a change in business process for how it handles enrollment processing on a nightly basis. This new business process accounts for the maximum enrollee processing threshold that could occur with the implementation of the NDAA and will be in place for normal nightly processing going forward. At the time of review, the risk mitigation documentation was in draft form and not finalized or signed; however, this document will be finalized and signed as part of the project documentation during the course of the NDAA implementation. This will be completed prior to go-live in January 2018.

Additionally, the finding applies the “Vulnerability Management Procedures”, effective April 30, 2017, as the relevant criteria. The purpose of the Vulnerability Management procedures is to “provide the Agency with visibility into the known vulnerabilities present on the network and provide a basis for understanding the effectiveness of patching and remediation process…The procedures document specific responsibility for scanning server and workstations for vulnerabilities, and for scanning operating systems and database for configuration compliance. The procedures also cover the process for monitoring deployment of security patches in the FRTIB environment and for engaging responsible parties in the remediation of patches discovered to be missing.” The scope

of the Vulnerability Management procedures only extends to vulnerability management over the IT environment and does not extend to business risk management and service level metrics.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

Federal Retirement Thrift Investment Board's Staff (Agency) Documents and Reports

- Minutes of the August 28, 2017, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov
- *Enterprise Information Security Risk Management (EISRM) Appendix 2: Baseline Security Requirements*, effective May 31, 2015
- *Serena Business Manager User Guide, Software Change Management*, v. 9.0, January 2016
- *Blended Retirement Project Schedule*, dated June 29, 2017
- *Task Order #42 FRTIB IT Environment Current/Future State Gap Analysis and Recommendations Document,* version 1.0, dated January 31, 2017
- *Part II Plan for Task Order #42 Subtask 2 Blended Retirement Capacity*, dated February 16, 2017
- *Blended Capacity Phase 2 Test Plan*, version 1.1, December 12, 2016
- *TO 42 – Blended Retirement Subtask 3 Capacity Remediation Test Approach,* version 1.0, dated May 21, 2017
- *TO 42 – Blended Retirement Sub-Task 2 - Capacity Analysis Phase 2 Business Requirements Document,* version 2.0, dated November 15, 2016
- *TO 42 - Blended Retirement Sub-Task 2 - Capactiy Analysis Project Management Plan,* version 1.5, dated June 29, 2017
- *Task Order #42 Subtask 3 Capacity Recommended Approach for Processing Enrollments for Blended Retirement System*, draft version 2.0, dated September 14, 2017
- *SOP-New Enrollment Limit Exceeded in API Edits-Draft*, version 0.1, dated September 5, 2017
- *API Limit Count of New Enrollments Submitted for a Single Unified - FDD-Draft,* version 1.0, dated September 5, 2017