KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan National Defense Authorization Act Pre-Implementation Controls

May 11, 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 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 December 7, 2016 through March 27, 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, 2016 through December 31, 2016. At the end of fieldwork, we received additional documentation through March 2017 in response to our initial findings and recommendations and updated them accordingly.

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*.

[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.

The objective of our audit over the TSP NDAA pre-implementation controls was to determine whether the Agency is developing security and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA.

We present two new findings and recommendations related to TSP NDAA pre-implementation controls, both of which address fundamental controls in the area of capacity planning. 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. Both recommendations are intended to strengthen TSP NDAA pre-implementation controls. The Agency should review and consider these recommendations for timely implementation. Section III.B 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 January 1, 2016 through December 31, 2016, the Agency developed certain security and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA. However, as indicated above, we noted internal control weaknesses in certain TSP NDAA pre-implementation controls.

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 the 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

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

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

May 11, 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 December 31, 2016, had approximately $495 billion in assets and approximately 5.0 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. NDAA requires the creation of a new "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. The Act changes 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, the Act requires the automatic enrollment of new uniformed service members in the TSP and provides for immediate automatic (1 percent) and matching contributions to the TSP for these members. NDAA also provides to uniformed service members with less than 12 years of

[3] Source: Minutes of the January 23, 2017, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

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

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 name, social security number, date of birth, address, employment code, 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. Security Controls[5]

The Agency is responsible for implementing and maintaining a security program and enforcing its requirements and controls. The NDAA implementation relies on these existing security program controls.

Security assessments of the blended retirement program review the current risk and unforeseen consequences to the existing TSP infrastructure. 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.

2. Capacity Planning[6]

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

---

[5] Source: *Enterprise Information Security Risk Management (EISRM) Appendix 2: Baseline Security Requirements*, effective May 31, 2015.

[6] Source: *Enterprise Information Security Risk Management (EISRM) Appendix 2: Baseline Security Requirements*, effective date May 31, 2015.

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, December 2014

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 objective of our audit over the TSP NDAA pre-implementation controls was to determine whether the Agency is developing security and capacity planning controls for the setup, transfer, and ongoing recordkeeping of contributions related to upcoming changes required by the NDAA.

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, 2016 through December 31, 2016. 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;
- Reviewed NDAA project implementation planning documentation; and
- Inspected a non-statistical sample of NDAA planning monthly status meeting reports.

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, 2016 through December 31, 2016. At the end of fieldwork, we received additional documentation through March 2017 in response to our initial findings and recommendations and updated them accordingly. 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.

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, 2016 through December 31, 2016, the Agency developed certain security 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 two new recommendations, presented in Section III.B, related to TSP NDAA pre-implementation controls, both of which address 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 these recommendations for timely implementation. The Agency's responses to these recommendations are included as an appendix within this report (Appendix A).

We noted no prior recommendations requiring follow-up during our performance audit.

Section III.B presents the findings and recommendations from this performance audit. Section III.C summarizes each open recommendation.

B. 2016 Findings and Recommendations

While conducting our performance audit over TSP NDAA pre-implementation controls, we identified two new findings and developed related recommendations. The U.S. Department of Labor Employee Benefits Security Administration requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2016-01: Weaknesses in Blended Retirement Capacity Study

During the scope period, Agency management solicited a capacity study from its technology infrastructure support vendor in support of the blended retirement project (BRP) implementation required by NDAA. Based on our review of the final capacity study titled, *Task Order #42 FRTIB IT Environment Current/ Future Gap Analysis and Recommendations Document,* dated January 31, 2017, we noted the following weaknesses:

- 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 cited in the presentation titled *Forecast of New TSP Accounts in 2018 Due to the Blended Retirement System*, created June 1, 2016. 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.

The Agency did not properly evaluate and document the assumptions used and certain aspects of the technical infrastructure to inform the final capacity planning report for relevance to the NDAA implementation. This weakness occurred because of lack of management oversight and an overreliance on contracted support.

The Agency's *Enterprise Information Security and Risk Management (EISRM): Baseline Security Requirements,* effective May 31, 2015, states:

RA-3 Risk Assessment

1. The Information System Security Officer SHALL:
    1.1. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

> RA-3 Risk Assessment
>
> Control: The organization: […]
>
> a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

The Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated September 2014, states:

> 7.05 Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Significance refers to the effect on achieving a defined objective.
>
> 7.06 Management estimates the significance of the identified risks to assess their effect on achieving the defined objectives at both the entity and transaction levels. Management estimates the significance of a risk by considering the magnitude of impact, likelihood of occurrence, and nature of the risk. […] The nature of the risk involves factors such as the degree of subjectivity involved with the risk and whether the risk arises from fraud or from complex or unusual transactions. The oversight body may oversee management's estimates of significance so that risk tolerances have been properly defined.

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;

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

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.

The capacity planning weaknesses may lead to decreased computing, recordkeeping, and data replication backup performance upon implementation. Without proper capacity planning activities at both the primary and alternate processing sites, the Agency may not be prepared fully to meet the increased demands for information processing and storage after the NDAA implementation, which may lead to unplanned impacts on the Agency's information infrastructure.

2016-02: Weaknesses in NDAA Project Management Timelines

During our testwork, we noted weaknesses in several of the Agency's NDAA-related project and subtask timelines. We identified the following weaknesses:

- The Agency developed a baseline agreement with its contractor for the blended retirement project in August 2016[9]. The agreement indicates that the information infrastructure support contractor expects to complete its project responsibilities on or before September 1, 2017. However, our review of the agreement and its related project plan indicates that this completion date does not support unanticipated and significant contingencies. Examples of such unplanned contingencies include the following:
  - A larger-than-forecast influx of new participants;
  - Last-minute procurement and implementation of additional dedicated network bandwidth between the production and alternate processing sites; and
  - Last-minute procurement and installation of additional hard drive space, processing power, and memory to meet a larger-than-forecast influx of new participants.

[9] *Blended Retirement CSSQ Baseline Agreement: Management Stage Gate* #2

- In response to an initial capacity planning study for the BRP, the Agency's contractor submitted a revised capacity remediation plan in February 2017[10]. This revised plan outlined the steps needed to remediate the issues identified in the initial capacity study. Our analysis of the revised capacity plan indicates 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, compressed timeframe limits the Agency's ability to respond to unexpected events and project delays.
- 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. Specifically, we noted:
  - The remediation plan included deferred testing of 12 subtasks, including key job scheduling functionality, without a scheduled future date;
  - The remediation plan discussed the need to turn on additional processing engines within the production mainframe to support an expected influx of 750,000 participant records. However, considerations related to purchasing and turning on equivalent engines at the alternate processing center were not documented; and
  - The remediation plan identified other, non-NDAA projects that could impact the NDAA project, such as upgrading the operating system that has reached the end of life support; upgrading hardware supporting the virtualization environment for distributed systems at both data centers; increasing the mainframe data throughput capability; and adding new hard drives.

These dependencies are critical in meeting the success of the BRP. They were, however, not fully considered under the revised capacity remediation plan, which has a projected completion end date of December 2017. While Agency management stated that the contractor will complete BRP-support services prior to December, the contractor is not yet required contractually to do so.

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.

We determined that any and all of these conditions could jeopardize the Agency's ability to meet the January 1, 2018 NDAA implementation date, infrastructure resilience, or system security.

[10]Titled *Part II Plan for Task Order #42 Subtask 2 Blended Retirement Capacity*, dated February 16, 2017.

The Agency did not properly consider unanticipated contingencies because of the lack of appropriate planning and understanding of the environment. Additionally, the Agency overly relied on contractor support to fully identify and evaluate relevant risks on behalf of the Agency.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

CP-2 Contingency Plan […]

2. The Information System Security Officer SHALL: […]

2.2. Develop a contingency plan for the information system that: […]

2.2.4. Provides recovery objectives, restoration priorities, and metrics, including:

- Order of restoration, including dependencies
- Recovery Time Objectives (RTOs) for system components
- Recovery Point Objectives (RPOs) for data contained in those systems […]

RA-3 Risk Assessment

1. The Information System Security Officer SHALL:

1.1. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits

1.2. Document risk assessment results in a risk assessment report […]

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

CP-2 Contingency Plan

Control: The organization:

a. Develops a contingency plan for the information system that: […]

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; […]

e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; [...]

(2) Contingency Plan | Capacity Planning

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: […] Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning. […]

RA-3 Risk Assessment

Control: The organization: […]

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits […]

e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

2. 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.

By not fully considering unanticipated contingencies and system interdependencies, the Agency risks missing the legally-required NDAA implementation deadline and jeopardizes the stability, integrity, and accessibility of several or all elements of the information infrastructure.

C. 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% 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.

Weaknesses in NDAA Project Management Timelines

2. To strengthen controls over the NDAA project management timelines, the Agency should:
   a. Re-evaluate and realign conflicting timelines identified across the 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.

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

May 11, 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 on May 5, 2017, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan National Defense Authorization Act Pre-Implementation, dated May 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,

Suzanne Lasin for Ravindra Deo

Ravindra Deo
Acting Executive Director

Enclosure

Executive Director's Staff Informal Comments on the
Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan
National Defense Authorization Act Pre-Implementation

2016-1: Weakness 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%[8] or greater traffic increase;

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

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.

Agency Responses:

a. The Agency concurs with the recommendation. In August 2016 the Agency replaced the data circuit between the production and alternate processing site. The new circuit increases capacity from 1Gbps to 10Gbps. The full implementation of the circuit will be completed by November 30, 2017.

b. The Agency concurs with the recommendation. The Agency will document more clearly the rationale supporting the assumptions leading to a lower maximum enrollee threshold used in initial load analysis and other forecasting activities. The Agency will complete this action by July 31, 2017.

c. The Agency concurs with the recommendation. The Agency will 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 by July 31, 2017.

2016-2: Weaknesses in Project Management Timelines

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;

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; and

Agency Responses:

a. The Agency concurs with the recommendation. During the fieldwork, the Agency provided a high level timeline for the remediation work to be completed. Since the pre-implementation audit fieldwork phase, the team created a more detailed project plan which included documenting the remediation work to be completed and tested by October 31, 2017.

b. The Agency concurs with the recommendation. The Agency has conducted a review of the project risk register, which resulted in no new high findings and considers this recommendation closed.

c. The Agency concurs with the recommendation. The BC/12 mainframe located in the disaster recovery site is sized and will be configured to support the expected production processing load after implementation of Blended Retirement. The disaster recovery mainframe BC/12 will only be used to process production data in the case of a disaster recovery event.

   The Agency believes the BC/12 mainframe will be capable of processing the expected production workload until January 2023 based on the current and expected configuration and processing capacity of the BC/12, current and expected processing capacity, the IBM CP3000 report, and the Agency's expected future growth in participant numbers.

   The Agency will conduct its 2017 Disaster Recovery testing in November 2017. The Agency will close this recommendation by December 31, 2017.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

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

- Minutes of the January 23, 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*, December 2014
- *Blended Retirement Charter*, dated January 20, 2016
- *Blended Retirement Baseline*, August 31, 2016
- *Blended Retirement Project Management Plan (PMP)* version 1.3, dated July 28, 2016
- *Blended Retirement Project PMP Attachments*, dated July 28, 2016
- *Blended Retirement Project Schedule*, dated January 12, 2017
- *Blended Retirement Communications Plan* version 1.0, last modified January 12, 2017
- *Blended Capacity Status Meeting Minutes*, various dates
- *IT Functional Status Meeting Minutes*, various dates
- *Project Team Status Meeting minutes*, various dates
- *Blended Phase 1 Change Management Security Impact Analysis Worksheet*, dated November 29, 2016
- *Blended Phase 2 Change Management Security Impact Analysis Worksheet*, dated December 21, 2016
- *Blended Functional Projects IT Risks*, no date provided
- *Task Order #42 Blended Retirement Preliminary Capacity Study "Quick Look"* version 1.3, dated November 14, 2016
- *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
- *Gaps and Recommendations Full List*, dated February 16, 2017
- *TO 42-Blended Retirement Sub-Task 2-Capactiy Analysis Business Requirements Document*, version 0.7, dated October 10, 2016