



Department of Labor

**U.S. Department of Labor
Employee Benefits Security Administration**

**Fiscal Year 2016 Thrift Savings Plan
Fiduciary Oversight Program**

**Presentation
to the**

Federal Retirement Thrift Investment Board

July 25, 2016

-30.0%



Employee Benefits Security Administration TSP Fiduciary Oversight Program Key Contacts

EBSA

- Phyllis Borzi, Assistant Secretary
- Timothy Hauser, Deputy Assistant Secretary for Program Operations
- Ian Dingwall, Chief Accountant
- Michael Auerbach, Chief, Division of Accounting Services
- Jonathan Matzkin, Senior Technical Advisor

Phone Number

(202) 693-8300
(202) 693-8315
(202) 693-8360
(202) 693-8363
(202) 693-8379

KPMG LLP

- Heather Koppe Flanagan, Lead Engagement Partner
- James DeVaul, IT Partner
- Derek Thomas, Engagement Partner
- Howard Simanoff, Lead Senior Manager
- Alvamerry Schaefer, Computer Systems Analyst
- Nathan Faut, Computer Systems Analyst

(202) 533-4012
(703) 286-8382
(202) 533-5402
(202) 533-6090
(703) 286-6956
(703) 286-6883



Employee Benefits Security Administration TSP Fiduciary Oversight Program Presentation to the Federal Retirement Thrift Investment Board

Agenda Item

Page Number

I. Scope of TSP Performance Audits	4
II. Tentative Schedule of Current TSP Performance Audits	8
III. Highlights of Overall Assessment: May 2015 – July 2016	12
IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations	15
V. Summary of Open Recommendations	19
VI. Future EBSA Initiatives	22

Supplemental Information

A. Overview of the EBSA TSP Fiduciary Oversight Program	24
B. Examples of TSP Information Obtained for Each Audit	27
C. Uses of TSP Information Obtained for Each Audit	28
D. Audit and Report Process for Each TSP Performance Audit	29



I. Scope of TSP Performance Audits

	Plan				
	<u>2016</u>	<u>2015</u>	<u>2014</u>	<u>2013</u>	<u>2012</u>
<u>IT-Related Audits</u>					
1. System Enhancements and Software Change Controls	—*	FS	—	FS	—
2. IT Operations Management	—	FS	—	FS	—
3. Computer Access and Security Controls	FS	FS	—	LS	—
4. Technical Security Vulnerability Assessment	—*	SP	—	SP	—
5. Service Continuity Controls	FS	—	—	FS	—
6. Participant Website Controls	—	FS	—	SP	—
7. Mainframe Configuration	FS	—	SP	—	—
8. Special Projects – IT	SP(1)*	—	—	—	—

Process Audits

9. Participant Support/Call Center Operations	FS	FS	—	—	FS
10. Loan Operations	FS	FS	—	—	—
11. Account Maintenance	—	FS	—	FS	—
12. Withdrawals	—*	FS	—	—	—
13. L Fund Operations	FS	FS	—	FS	—

* Reflects plan that requires a task order modification

(1) Mobile Device Security and Governance Review

FS = Full Scope LS = Limited Scope SP = Special Project



I. Scope of TSP Performance Audits (continued)

<u>Other TSP Activities</u>	<u>Plan</u>				
	<u>2016</u>	<u>2015</u>	<u>2014</u>	<u>2013</u>	<u>2012</u>
1. Treasury "G" Fund Investment Operations	–	FS	–	–	–
2. Investment Management Operations ("F", "C", "S" and "I" Funds)	FS	FS	–	FS	–
3. Annuity Operations	FS	FS	–	–	–
4. The Board's Staff	SP(3)*(4)*	FS	SP(2)(3)	–	FS
5. CIA's OIG TSP Audit	–	–	–	–	–

* Reflects plan that requires a task order modification

- (2) Benchmarking analyses of processes and internal controls over contributions, withdrawals, loans, and investment management
- (3) Follow-up on certain prior year recommendations identified as closed by the Agency
- (4) National Defense Authorization Act for Fiscal Year 2016 Pre-Implementation Review

FS = Full Scope

SP = Special Project



I. Scope of TSP Performance Audits (continued)

<u>Uniformed Services</u>	<u>Plan</u>	<u>2015</u>	<u>2014</u>	<u>2013*</u>	<u>2012</u>	<u>2011</u>
<u>2016</u>						<u>and Prior</u>
1. U.S. Marine Corps	-	-	-	-	-	FS
2. U.S. Army	-	-	-	-	-	FS
<u>Federal Agencies</u>						
3. Administrative Office of the U.S. Courts	-	-	-	-	-	R/LS
4. Army - Aberdeen Proving Ground	-	-	-	-	-	LS
5. Army - Defense Personnel Center	-	-	-	-	-	FS
6. Army - Fort Meade	-	-	-	-	-	LS
7. Army - Fort Myers	-	-	-	-	-	R/FS
8. Bolling Air Force Base	-	-	-	-	-	FS
9. Defense Logistics Agency	-	-	-	-	-	FS
10. Department of Agriculture - NFC	FS	-	-	-	-	R/FS
11. Department of Agriculture - Farm Service Agency	-	-	-	-	-	FS
12. Department of the Army - Corps of Engineers	-	-	-	-	-	R/FS
13. Department of Commerce	-	-	-	-	-	R/FS
14. Department of Energy	-	-	-	-	-	R/FS
15. Department of Health and Human Services	-	-	-	-	-	LS
16. Department of Housing and Urban Development	-	-	-	-	-	R/FS
17. Department of Interior - Denver	-	-	-	-	-	R/FS
18. Department of Interior - Interior Business Center	-	-	FS	-	-	-
19. Department of Justice	-	-	-	-	-	R/LS
20. Department of Labor	-	-	-	-	-	R
21. Department of State	-	-	-	-	-	R/FS
22. Department of Transportation - Oklahoma	-	-	-	-	-	R/FS

FS = Full Scope LS = Limited Scope R = Follow-up Review



Federal Agencies (continued)	Plan 2016	2015	2014	2013*	2012	2011 and Prior
------------------------------	--------------	------	------	-------	------	-------------------

* During the 2013 performance audit of the TSP Roth option communications, we selected and conducted procedures at the U.S. Army, U.S. Coast Guard, National Aeronautics and Space Administration, and the Departments of Agriculture, Health and Human Services, Justice, Transportation, Treasury, and Veterans Affairs.



II. Tentative Schedule of Current TSP Performance Audits

Background

- Delays to the 2015 planned audit schedule impacted the timing of both 2015 and 2016 performance audits
- Primary reasons for delays:
 - Implementation of new contractor on-boarding security process
 - Late receipt of certain requested documents and reports
 - Insufficient support initially provided for certain requests
 - Significant additional work in reporting phase after receipt of the Agency's comments on draft reports and new information provided
 - Inability to schedule meetings with appropriate individuals timely
 - Inability to provide accurate information on systems in scope, causing inefficiencies, additional testing, and additional meetings
 - Adhering to new Agency request to provide specific questions ahead of time for meetings



II. Tentative Schedule of Current TSP Performance Audits (continued)

2015 Performance Audits in Progress

Process

Withdrawals

Account Maintenance

Other

The Board's Staff

<u>Work Began</u>	<u>FRTIB Exit</u>
Jan-16	Jul-16
Apr-16	Aug-16
Jun-16	Aug-16



II. Tentative Schedule of Current TSP Performance Audits (continued)

2016 Performance Audits in Progress

IT-Related

Service Continuity Controls

Mainframe Configuration

Other TSP Activities

Annuity Operations

Investment Management Operations

(“F”, “C”, “S” and “I” Funds)

Federal Agencies

National Finance Center

**Work
Began**

**FRTIB
Exit**

Feb-16

Jul-16

Jun-16

Aug-16

Apr-16

Jul-16

May-16

Jul-16

Feb-16

Sept-16



II. Tentative Schedule of Current TSP Performance Audits (continued)

2016 Performance Audits to be Started

IT-Related

Mobile Device Security and Governance Review

Computer Access and Security Controls

Process

L Fund Operations

Loan Operations

Participant Support/Call Center Operations

Other TSP Activities*

National Defense Authorization Act Pre-Implementation Review

Follow-up of certain prior year findings

**Work
Begins**

Aug-16

Aug-16

Aug-16

Aug-16

Nov-16

TBD

TBD

FRTIB

Exit

Oct-16

Oct-16

Sep-16

Feb-17

Feb-17

TBD

TBD

* Reflects plan that requires a task order modification



III. Highlights of Overall Assessment: May 2015 – July 2016

Summary of 2015 Audits Completed as of July 15, 2016

- Number of audits under 2015 task orders: 10 (7 related to the Agency)
- Instances of material non-compliance with FERSA: 0
- Number of closed Agency recommendations: 15
- Number of new Agency recommendations: 48
- Number of closed non-Agency recommendations: 1
- Number of new non-Agency recommendations: 1



III. Highlights of Overall Assessment: May 2015 – July 2016 (continued)

Summary of 2015 Audits Completed as of July 15, 2016, continued

Agency Audit	Scope Period	Prior Year Recs Remaining Open	Prior Year Recs Closed	New Fundamental Recs	New Other Recs
Computer Access and Security Controls	1/1/14 – 12/31/14	6	4	10	0
Loan Operations	1/1/14 – 12/31/14	0	1	0	0
L Fund Operations	1/1/14 – 3/31/15	0	0	1	0
Participant Website	1/1/15 – 12/31/15	0	3	6	1
Participant Support Operations	1/1/14 – 3/31/15	5	6	13	4
System Enhancements and Change Control	7/1/14 – 6/30/15	5	0	5	0
IT Operations Management	1/1/15 – 12/31/15	3	1	7	1
Agency Total		19	15	42	6



III. Highlights of Overall Assessment: May 2015 – July 2016 (continued)

Summary of 2015 Audits Completed as of July 15, 2016, continued

Non-Agency Audit	Scope Period	Prior Year Recs Remaining Open	Prior Year Recs - Closed	New Fundamental Recs	New Other Recs
G Fund Investment Operations	1/1/14 - 12/31/14	0	0	0	0
Annuity Operations	1/1/14 - 12/31/14	0	1	0	1
Investment Management Operations – F, C, S, and I Funds	1/1/14 - 3/31/15	0	0	0	0
Non-Agency Total		0	1	0	1



IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations

Computer Access and Security Controls

- Security authorization and Plan of Action and Milestone controls
- Account administration controls
- Data encryption
- System Security Plans documentation
- System interconnection controls
- Configuration controls
- Personnel security and privacy training controls

L Fund Operations

- Administrator account access controls



IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations (continued)

Participant Website

- Website functional design documentation
- Website content change management
- Data transfer controls
- Website configuration controls
- Website infrastructure controls

Participant Support Operations

- Logical and physical access administration and recertification controls
- Call center technical security controls
- Call recording configuration control
- Call center configuration and patch management controls



IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations (continued)

Participant Support Operations (continued)

- Call center contract oversight
- Call center encryption controls
- Call center security management program
- Call center Rules of Behavior documentation
- Electronic media controls

Systems Enhancement and Change Control

- Production infrastructure security controls
- System security plan and configuration management plan documentation
- Retention of change control documentation
- System change control review controls



IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations (continued)

IT Operations Management

- Database management and vulnerability management controls
- Database data integrity and monitoring controls
- System infrastructure controls
- System interconnection controls
- Hardware maintenance program
- Mainframe infrastructure controls
- Database software monitoring and asset management controls



V. Summary of Open Recommendations

<u>IT-Related Audits</u>	<u>Fundamental Controls</u>	<u>Other Controls</u>	<u>Total</u>	<u># Open Originating Prior to 2015</u>
1. Service Continuity Controls (3)	7	1	8	8
2. System Enhancements and Software Change Controls (5)**	10	1	11	6
3. IT Operations Management (5)	10	1	11	3
4. Computer Access and Security Controls (5)	15	1	16	6
5. Technical Security Vulnerability Assessment (3)	6	--	6	6
6. Participant Website Controls (5)	6	1	7	--
7. Mainframe Configuration (4)	7	1	8	8

** Includes one fundamental controls recommendation from the 2010 Project Management Practices over Certain Thrift Savings Plan Projects and Follow Up on Prior Year Findings performance audit.



V. Summary of Open Recommendations (continued)

<u>Process Audits</u>	<u>Fundamental Controls</u>	<u>Other Controls</u>	<u>Total</u>	# Open Originating Prior to 2015
8. Account Maintenance (3)	--	1	1	1
9. Participant Support/ Call Center Operations (5)	18	4	22	5
10. Withdrawals (1)	4	1	5	5
11. Loan Operations	--	--	--	--
12. L Fund Operations (5)	1	--	1	--



V. Summary of Open Recommendations (continued)

<u>Other TSP Audits</u>	<u>Fundamental Controls</u>	<u>Other Controls</u>	<u>Total</u>	<u># Open Originating Prior to 2015</u>
1. Treasury "G" Fund Investment Operations	--	--	--	--
2. Investment Manager Operations ("F", "C", "S" and "I" Funds)	--	--	--	--
3. Annuity Operations (5)	--	1	1	--
4. Board Staff Operations (2)	1	--	1	1
Total Recommendations	85	13	98	49

(1) The most recent report was 2011.

(2) The most recent report was 2012.

(3) The most recent report was 2013.

(4) The most recent report was 2014.

(5) The most recent report was 2015.



VI. Future EBSA Initiatives

- Complete all audit areas of the TSP Fiduciary Oversight Program at least once every three years.
- Conduct pre-implementation reviews of the National Defense Authorization Act's impact on the TSP.
- Perform other special projects as appropriate.



Department of Labor





A. Overview of the EBSA TSP Fiduciary Oversight Program

1. EBSA's TSP Fiduciary Oversight Responsibility

The Thrift Saving Plan (TSP) was authorized by Congress under the Federal Employees' Retirement System Act of 1986 (FERSA) (Public Law 99-335).

The Employee Benefits Security Administration (EBSA), through the statutory reference to the Secretary of Labor [5 USC 8477(g)], is responsible for establishing a program to carry out audits to determine the level of compliance with the requirements of FERSA relating to fiduciary responsibilities and prohibited activities of fiduciaries.



A. Overview of the EBSA TSP Fiduciary Oversight Program (continued)

2. EBSA's Approach to the TSP Fiduciary Oversight Program

EBSA's TSP audit procedures are designed to comply with *Government Auditing Standards*, published by the U.S. Government Accountability Office (GAO), for conducting the following audits:

- Performance audits, including assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses; and
- Financial-related audits, including reviews of certain financial information



A. Overview of the EBSA TSP Fiduciary Oversight Program (continued)

3. EBSA's TSP Fiduciary Oversight Program

EBSA's Program is designed to determine whether:

- The fiduciaries are acquiring, protecting, and using TSP resources effectively, efficiently, and solely in the interest of TSP participants and beneficiaries;
- The fiduciaries have complied with FERSA and other applicable laws and regulations;
- The TSP program activities, functions, and organization are cost effective and efficient; and
- EBSA's previous TSP recommendations have been adequately acted upon.



B. Examples of TSP Information Obtained for Each Audit

- Prior audit reports
- Organization charts
- Position descriptions
- Flowcharts
- Policies and procedures documents
- Relevant contracts
- Descriptions of support systems
- Identification of key TSP control points
- EBSA, Federal Retirement Thrift Investment Board members, and Agency management concerns



C. Uses of TSP Information Obtained for Each Audit

- Test internal controls
- Test TSP transactions and activities for compliance with applicable laws, regulations, and contracts
- Address EBSA, Federal Retirement Thrift Investment Board, and Agency concerns, as practicable
- Update EBSA's TSP Fiduciary Oversight Program Manual



D. Audit and Report Process for Each TSP Performance Audit

- Preliminary planning meeting(s)
- Entrance conference
- Completion of field work
- Agency's initial review of pre-exit conference draft report (or sections thereof)
- Exit conference
- Agency's 30 day technical review period of draft report
- Preliminary final report, forwarded to the Executive Director for formal written response to DOL EBSA
- Final report including the Executive Director's formal written response to DOL EBSA
- The Executive Director's presentation of report and formal written response to DOL EBSA at scheduled meetings of the Board
- Summarized final report forwarded to DOL Deputy Assistant Secretary for Program Operations for appropriate further action, if necessary
- DOL's and contractors' presentation of significant findings and recommendations and current year's TSP audit plan annually at a scheduled Board meeting

