U.S. Department of Labor
Employee Benefits Security Administration

Fiscal Year 2018 Thrift Savings Plan
Fiduciary Oversight Program

Presentation
to the
Federal Retirement Thrift Investment Board
April 23, 2018

Employee Benefits Security Administration
TSP Fiduciary Oversight Program
Key Contacts

EBSA	Phone Number
• Preston Rutledge, Assistant Secretary	(202) 693-8300
• Jeanne K. Wilson, Deputy Assistant Secretary for Policy	(202) 693-8300
• Timothy Hauser, Deputy Assistant Secretary for Program Operations	(202) 693-8315
• Michael Auerbach, Chief Accountant	(202) 693-8363
• Jonathan Matzkin, Senior Technical Advisor	(202) 693-8379
• Kenneth Robinson, Senior Auditor	(202) 693-8377

KPMG LLP	
• Heather Koppe Flanagan, Lead Engagement Partner	(202) 533-4012
• James DeVaul, IT Partner	(703) 286-8382
• Derek Thomas, Engagement Partner	(202) 533-5402
• LeeAnne Racelis, Lead Senior Manager	(202) 533-3596
• Alvamerry Schaefer, Computer Systems Analyst	(703) 286-6956
• Nathan Faut, Computer Systems Analyst	(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	9
III.	Highlights of Overall Assessment: May 2017 – April 2018	12
IV.	Summary of Areas Addressed by Recent Fundamental Control Recommendations	14
V.	Summary of Open Recommendations	20
VI.	Other Considerations for the Board	26
VII.	Future EBSA Initiatives	27

Supplemental Information

A.	Overview of the EBSA TSP Fiduciary Oversight Program	29
B.	Examples of TSP Information Obtained for Each Audit	32
C.	Uses of TSP Information Obtained for Each Audit	33
D.	Audit and Report Process for Each TSP Performance Audit	34

I. Scope of TSP Performance Audits

IT-Related Audits	Plan 2018	2017	2016	2015	2014
1. System Enhancements and Software Change Controls	–	–	–	FS	–
2. IT Operations Management	–	–	–	FS	–
3. Computer Access and Security Controls	–	FS	FS	FS	–
4. Service Continuity Controls	–	–	FS	–	–
5. Participant Website Controls	–	–	–	FS	–
6. Mainframe Configuration	FS	–	FS	–	SP
7. Special Projects – IT	SP(1)(2)(4)(5)	SP(2)(3)(4)	SP(1)(2)(4)	–	–

(1) Mobile Device Security and Governance Controls
(2) Status Determination of Certain Prior Audit Recommendations
(3) Insider Threat Controls
(4) National Defense Authorization Act for Fiscal Year 2016 related reviews
(5) Limited General IT Control Review over Remote TSP Contractor Sites

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

I. Scope of TSP Performance Audits (continued)

Process Audits	Plan 2018	2017	2016	2015	2014
1. Participant Support/Call Center Operations	FS	–	FS	FS	–
2. Loan Operations	FS	–	FS	FS	–
3. Account Maintenance	FS	FS	–	FS	–
4. Withdrawals	–	FS/SP(6)	–	FS	–
5. Lifecycle Funds Operations	–	–	FS	FS	–

(6) Implementation of the Defending Public Safety Employees' Retirement Act

FS = Full Scope SP = Special Project

I. Scope of TSP Performance Audits (continued)

Other TSP Activities	Plan 2018	2017	2016	2015	2014
1. "G" Fund Investment Operations	FS	–	–	FS	–
2. Investment Management Operations ("F", "C", "S" and "I" Funds)	–	FS	FS	FS	–
3. Annuity Operations	FS	–	FS	FS	–
4. The Board's Staff	FS	–	–	FS	SP(7)(8)

(7) Benchmarking analyses of processes and internal controls over contributions, withdrawals, loans, and investment management
(8) Follow-up on certain prior year recommendations identified as closed by the Agency

FS = Full Scope SP = Special Project

I. Scope of TSP Performance Audits (continued)

Uniformed Services	Plan 2018	2017	2016	2015	2014	2013* and Prior
1. U.S. Marine Corps	–	–	–	–	–	FS
2. U.S. Army	–	–	–	–	–	FS
Federal Agencies						
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

I. Scope of TSP Performance Audits (continued)

Federal Agencies (continued)	Plan 2018	2017	2016	2015	2014	2013* and Prior
23. Department of the Treasury (includes IRS)	–	–	–	–	–	FS
24. Department of Veterans Affairs	–	–	–	–	–	R/FS
25. DFAS (as Uniformed Services Payroll Service Provider)	–	–	–	–	–	FS
26. DFAS - Charleston and Army - Ft. Monmouth	–	–	–	–	–	FS
27. DFAS - Columbus and Defense Logistics Agency	–	–	–	–	–	FS
28. DFAS - Denver and North Island Naval Air Station	–	–	–	–	–	R/FS
29. DFAS - Pensacola and Naval Sea System Command	–	–	–	–	–	FS
30. Environmental Protection Agency	–	–	–	–	–	FS
31. Federal Bureau of Investigation	–	–	–	–	–	FS
32. Federal Deposit Insurance Corporation	–	–	–	–	–	FS
33. General Services Administration	–	–	–	–	–	R/FS
34. Government Accountability Office	–	–	–	–	–	FS
35. House of Representatives	–	–	–	–	–	R
36. Kelly Air Force Base - San Antonio	–	–	–	–	–	R/FS
37. National Aeronautics and Space Administration	–	–	–	–	–	FS
38. National Security Agency	–	–	–	–	–	LS
39. Naval Publications and Forms Center	–	–	–	–	–	R/ LS
40. Naval Research Laboratory	–	–	–	–	–	R/FS
41. Naval - Supply Center, Norfolk	–	–	–	–	–	R/ LS
42. Navy - Atlantic Fleet	–	–	–	–	–	LS
43. Navy - Norfolk Naval Shipyard	–	–	–	–	–	R/ LS
44. Navy Regional Finance Center	–	–	–	–	–	R/FS
45. Nuclear Regulatory Commission	–	–	–	–	–	FS
46. Postal Service	–	–	–	–	–	R/FS

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

* 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

2017 Performance Audits in Reporting Phase – Both to Be Issued by Mid-May 2018

IT–Related Audits

Insider Threat Controls

Computer Access and Security Controls

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

2018 Performance Audits in Progress

	Work Began	FRTIB Exit
IT-Related Audits		
Mainframe Configuration	Feb-18	May-18
Limited GITC Review - Remote TSP Contractor Sites	Mar-18	May-18
Process Audits		
Loan Operations	Feb-18	May-18
Other TSP Activities		
"G" Fund Investment Operations	Dec-17	Mar-18
The Board's Staff	Dec-17	Apr-18
Annuity Operations	Mar-18	May-18

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

2018 Performance Audits to be Started

	Work Begins	FRTIB Exit
IT-Related Audits		
Mobile Device Security and Governance Controls	Apr-18	June-18
Status Determination of Certain Prior Audit Recommendations	May-18	July-18
National Defense Authorization Act for Fiscal Year 2016 Post-Implementation Review	May-18	July-18
Process Audits		
Account Maintenance	May-18	July-18
Participant Support / Call Center Operations	May-18	July-18

III. Highlights of Overall Assessment: May 2017– April 2018

Summary of Audits Completed since May 2017 (through April 2, 2018)

Number of audits completed	14 (13 related to the Agency)
Instances of material non-compliance with FERSA	0
Number of closed Agency recommendations	16
Number of new Agency recommendations	65
Number of closed Other Entity recommendations	0
Number of new Other Entity recommendations	0

III. Highlights of Overall Assessment: May 2017 – April 2018 (continued)

Summary of Audits Completed since May 2017 (through April 2, 2018) (continued)

Agency Audit	Scope Period	Prior Year Recs Remaining Open	Prior Year Recs Closed	New Fundamental Recs	New Other Recs
Mainframe	7/1/15 - 6/30/16	6	2	18	0
Computer Access	10/1/15 - 9/30/16	13	3	11	0
NDAA #1	1/1/16 - 12/31/16	N/A	N/A	2	0
NDAA #2	1/1/17 - 8/31/17	2	0	1	0
Mobile Device	10/1/15 - 9/30/16	N/A	N/A	11	0
Status Determination of PY Recs #1	*	N/A	N/A	1	0
Status Determination of PY Recs #2	**	1	N/A	0	0
L Fund Operations	4/1/2015 - 9/30/2016	1	0	3	1
Loans	10/1/15 - 9/30/16	N/A	N/A	0	3
Participant Support	1/1/16 - 12/31/16	14	8	6	0
Withdrawals	7/1/15 - 12/31/16	1	2	4	3
Defending Public Safety Employees' Retirement Act ***	1/1/16 - 12/31/16	N/A	N/A	N/A	N/A
Account Maintenance	2/1/16 - 2/28/17	0	1	0	1
Investment Management Operations ("F","C", "S", and "I" Funds)	4/1/16 - 3/31/17	N/A	N/A	N/A	N/A
Agency Total		38	16	57	8

* The scope of this audit included review of the status of certain Mandiant audit recommendations as reported on July 25, 2015 and August 25, 2015.

** The scope of this audit included review of the status of certain Mandiant audit recommendations as reported on July 25, 2015 and August 25, 2015 and a review of Department of Homeland Security penetration test recommendations issued on May 18, 2016.

*** The finding noted in this audit is included as part of a recommendation included in the Withdrawals audit.

IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations

Mainframe Configuration (2016)

- Excessive privileges
- Password security
- Operating system planning
- Access controls and user accountability
- Database inconsistencies and abnormalities
- Internet tools
- Production and non-production environments
- Service level metrics
- Unassigned resource risks
- Batch job submission
- Data migration
- Audit logs

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

Computer Access and Security Controls (2016)

- Identity and access management and password configuration
- Contractor management
- System security documentation, POA&Ms, and risk acceptance
- PII inventory
- Security awareness training
- Interconnection service agreements
- Data loss prevention tool
- Security incident reporting

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

National Defense Authorization Act Pre-Implementation (2016 and 2017)

- Blended retirement capacity study
- Project management timelines
- Updating risk acceptance documentation

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

Mobile Device Security and Governance Controls (2016)

- Mobile device governing structure
- Policies and procedures over mobile devices
- Excessive administrative access to server
- Configuration management, including password configuration
- Incident monitoring
- Mobile device approvals, enrollment, and removals
- BoardBook application security
- Vulnerability scanning of mobile device server

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

Status Determination of Certain Prior Audit Recommendations (2016)

- Risk assessment of third-party connections

Lifecycle Funds Operations (2016)

- Shared database accounts
- Outdated version of ColdFusion
- Configuration management procedures

Participant Support / Call Center Operations (2016)

- Call center password requirements, physical and logical access, and internet access
- Call center media disposal
- Call center privacy impact assessment

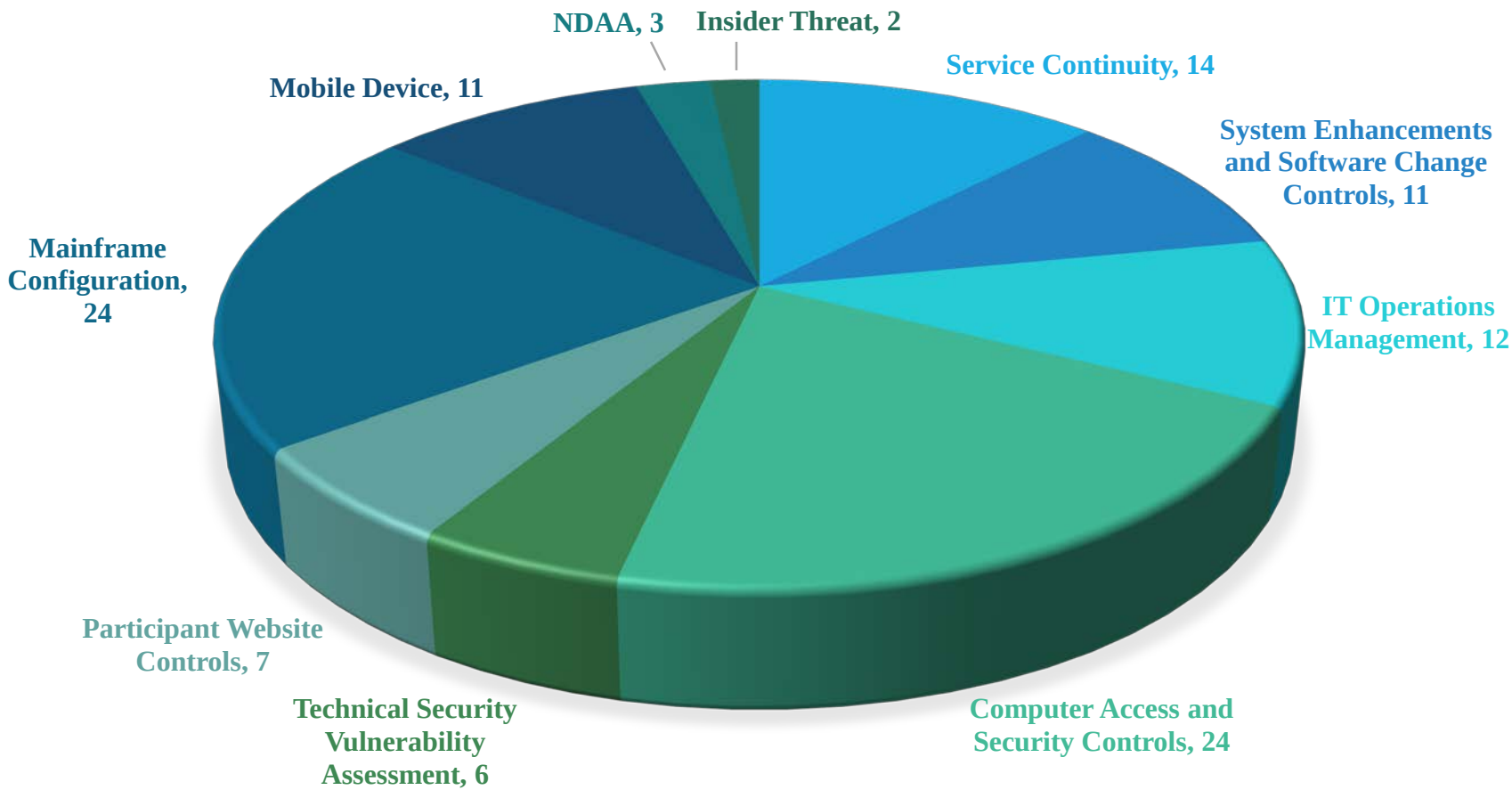
IV. Summary of Areas Addressed by Recent Fundamental Control Recommendations (continued)

Withdrawals (2017)

- System edit checks for in-service withdrawals
- Policies and procedures over verification of marital status and notary seal requirements
- Documentation for certain system processes and controls

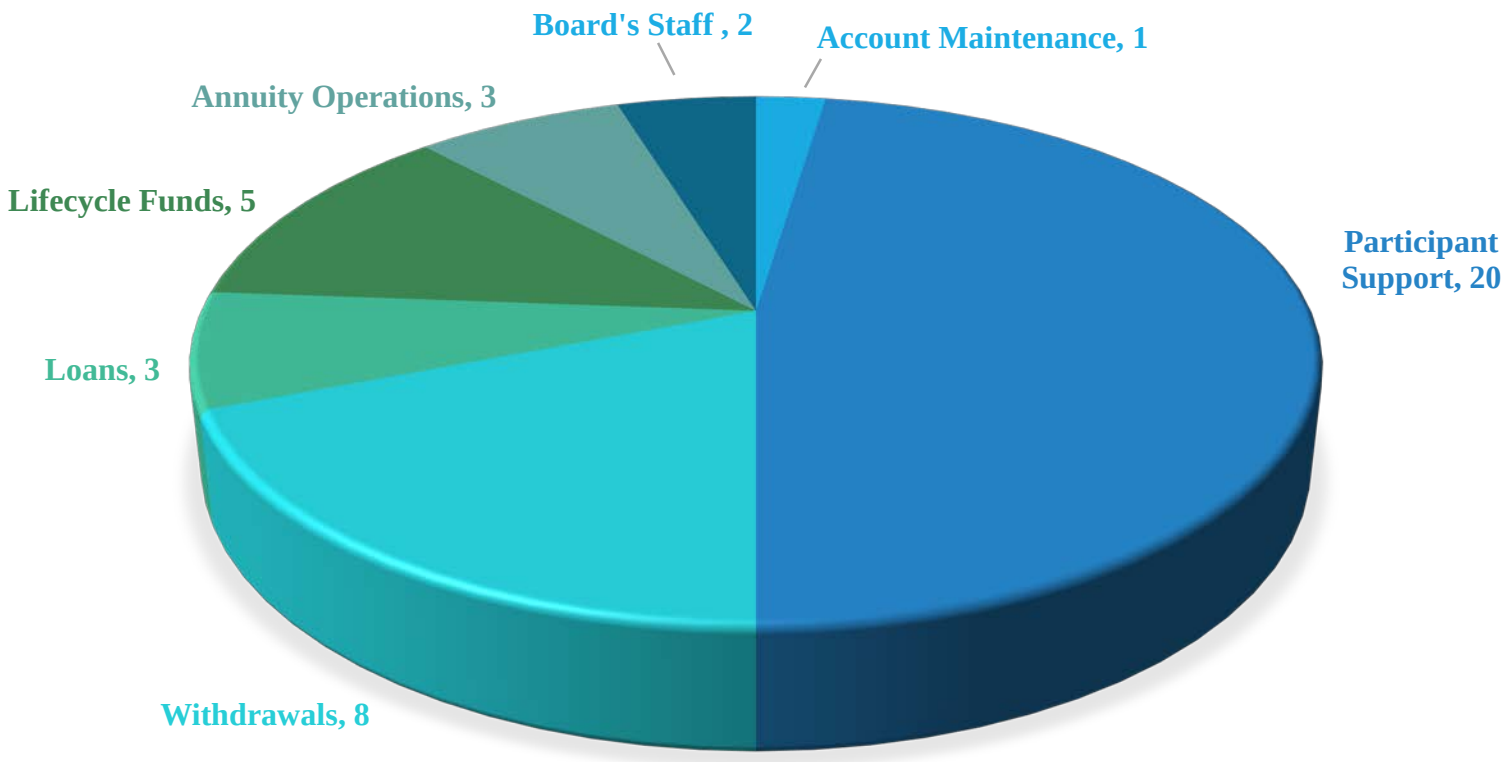
V. Summary of Open Recommendations

OPEN RECOMMENDATIONS - IT-RELATED AUDITS



V. Summary of Open Recommendations (continued)

OPEN RECOMMENDATIONS - PROCESS AND OTHER AUDITS



V. Summary of Open Recommendations (continued)

IT-Related Audits	Fundamental Controls	Other Controls	Total	# Open Originating Prior to 2017
1. System Enhancements and Software Change Controls (2)**	10	1	11	11
2. IT Operations Management (2)***	11	1	12	12
3. Computer Access and Security Controls (3)	23	1	24	24
4. Technical Security Vulnerability Assessment (1)	6	--	6	6
5. Service Continuity Controls (3)	12	2	14	14
6. Participant Website Controls (2)	6	1	7	7
7. Mainframe Configuration (3)	24	--	24	24

** 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.
***Includes one fundamental controls recommendation from the *2016 Status Determination of Prior Year Recommendations* performance audit.

V. Summary of Open Recommendations (continued)

IT-Related Audits	Fundamental Controls	Other Controls	Total	# Open Originating Prior to 2017
8. Mobile Device Security and Governance (3)	11	--	11	11
9. National Defense Authorization Act Implementation (4)	3	--	3	2

V. Summary of Open Recommendations (continued)

Process Audits	Fundamental Controls	Other Controls	Total	# Open Originating Prior to 2017
1. Participant Support/ Call Center Operations (3)	18	2	20	20
2. Loan Operations (3)	--	3	3	3
3. Account Maintenance (4)	--	1	1	--
4. Withdrawals (4)	5	3	8	1
5. Lifecycle Funds Operations (3)	4	1	5	5

V. Summary of Open Recommendations (continued)

Other TSP Audits	Fundamental Controls	Other Controls	Total	# Open Originating Prior to 2017
1. "G" Fund Investment Operations	--	--	--	--
2. Investment Management Operations ("F", "C", "S" and "I" Funds)	--	--	--	--
3. Annuity Operations (3)	2	1	3	3
4. The Board's Staff (2)	1	1	2	2
Total Recommendations	136	18	154	145

(1) The most recent report was 2013.

(2) The most recent report was 2015.

(3) The most recent report was 2016.

(4) The most recent report was 2017.

VI. Other Considerations for the Board

- Help the organization keep its eye on the ball: long-term value creation
- Be particularly sensitive to risks posed by the tone at the top and culture throughout the organization
- Expect disruption to continue full-force, with technology and "digital" at its core
- Learn to live with cyber risk – and continue to refine the board's discussions about cyber risk and security

Source: KPMG Board Leadership Center's *On the 2018 Private Company Board Agenda*

VII. Future EBSA Initiatives

- Complete all audit areas of the TSP Fiduciary Oversight Program at least once every three years.
- Perform other special projects as appropriate.

Supplemental Information

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 members, and Agency management 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 walk-through meetings and field work
- Agency's initial review of pre-exit conference draft report (or sections thereof)
- Exit conference
- Agency's 14 day review period of draft report 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