



Department of Labor

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

**Fiscal Year 2009 Thrift Savings Plan
Fiduciary Oversight Program**

**Presentation
to the
Federal Retirement Thrift Investment Board
February 17, 2009**



Department of Labor

Employee Benefits Security Administration TSP Fiduciary Oversight Program Key Contacts

EBSA

	<u>Phone Number</u>
• Alan Lebowitz, Deputy Assistant Secretary	(202) 693-8316
• Timothy Hauser, Associate Solicitor	(202) 693-5590
• Ian Dingwall, Chief Accountant	(202) 693-8361
• Michael Auerbach, Chief, Division of Accounting Services	(202) 693-8363
• William Bailey, Senior Auditor, FERSA Compliance	(202) 693-8372

KPMG LLP

• Diane Dudley, Client Service Partner	(202) 533-3002
• Heather Flanagan, Engagement Partner	(202) 533-4012
• Don Farineau, EDP Partner	(202) 533-4320
• Derek Thomas, Senior Manager	(202) 533-5402
• Mark Munster, Computer Systems Analyst	(202) 533-4194



Employee Benefits Security Administration TSP Fiduciary Oversight Program

Presentation to the Federal Retirement Thrift Investment Board

<u>Agenda Item</u>	<u>Page Number</u>
I. Overall Assessment for Fiscal Year 2008	4
II. Summary of Significant Issues	6
III. Future EBSA Initiatives	8
IV. Scope of TSP Performance Audits	9
V. Tentative Schedule of Fiscal Year 2009 TSP Audits	13
VI. Summary of Open Recommendations	14
<u>Supplemental Information</u>	
A. Overview of the EBSA TSP Fiduciary Oversight Program	18
B. Examples of TSP Information Obtained for Each Audit	22
C. Uses of TSP Information Obtained for Each Audit	23
D. Audit and Report Process for Each TSP Performance Audit	24
E. Overview of the TSP Performance Audit Objectives	25



I. Overall Assessment for Fiscal Year 2008

- No instances of material non-compliance with FERSA came to our attention.
- The Agency has elements of an information security program in place to help protect the confidentiality, availability and integrity of TSP data and system resources.
- The Agency has processes in place to help control TSP application changes and to assist in IT capital planning decision-making.
- The Agency has and continues to implement a configuration management plan that includes procedures and a standard set of tools to aid in the tracking and completion of change requests.



I. Overall Assessment for Fiscal Year 2008 (continued)

- The Agency has a program in place to implement a business assurance strategy, particularly controls related to backup procedures, conducting contingency planning, providing environmental controls and conducting capacity planning over the TSP Systems.
- Significant recommendations are still open. The FY 2009 TSP audit program includes oversight of progress.



II. Summary of Significant Issues

- **System Security**
 - Complete and implement the TSP security related policies and procedures.*
 - Document, implement, and enforce logical access controls over privileged users to help ensure only authorized access to sensitive areas of TSP systems.*
 - Evaluate and apply the level of technical controls over the TSP systems (applications and networks) recommended by the TSP System Security Plan.*
 - Conduct a comprehensive risk assessment and Privacy Impact Assessment over the TSP systems and related system components.
 - Complete, implement, and monitor policies related to protecting sensitive and PII information and the PII incident response and notification plan.
 - Conduct a formal E-Authentication risk assessment to evaluate the authentication level for the TSP Web.

* Communicated at prior Board Meeting(s).



II. Summary of Significant Issues (continued)

- **System Enhancements and Development Lifecycle/Software Change Controls**
 - Adopt, implement, and enforce an SDLC methodology and a project management methodology with the Agency's contractors to strengthen processes and controls.
 - Conduct a capability assessment of the TSP applications' design to coincide with consideration of business processes and the future design requirements of the TSP modernization plan.
 - Evaluate the current IT Strategic Plan for gaps related to planned IT capital investments, and formalize and document the Agency's IT capital planning procedures used to make decisions for TSP IT portfolio investments.
- **Service Continuity**
 - Evaluate current and historical system resource utilization and disk storage data and compare them to the planned requirements to help validate whether the forecasted TSP system requirements are reasonable.
 - Maintain proper documentation to demonstrate daily backups and scheduled maintenance are performed in accordance with the contract's statement of work and ensure backup tapes are encrypted.



III. Future EBSA Initiatives

As funding permits:

- Complete initiatives as directed by the Secretary of the Department of Labor.
- Complete a second audit cycle of all daily valuation TSP processes (initially completed in FY 2004 and FY 2005).
- Complete audits of uniformed services TSP operations, initiated by DOL in FY 2004.



IV. Scope of TSP Performance Audits

	<u>Plan 2009</u>	<u>2008</u>	<u>2007</u>	<u>2006</u>	<u>2005</u>
<u>IT-Related Audits</u>					
1. System Enhancements and Software Change Controls	—	FS	—	—	—
2. IT Operations Management/Mainframe	—	—	—	—	SP
3. Computer Access Controls and Security	LTD	FS	FS	—	—
4. Security Penetration and Vulnerability Assessment	—	SP(3)	SP(3)	—	—
5. Service Continuity Controls	—	LTD	—	SP	—
<u>Process Audits</u>					
6. Account Maintenance	—	—	—	—	—
7. Participant Support/Call Center Operations	FS	—	—	SP(1)	SP(2)
8. Withdrawals	—	—	—	—	FS
9. Loan Operations	—	—	—	—	SP

(1) Clintwood call center only

(2) Cumberland call center only

(3) Reported as part of the Computer Access report

FS = Full Scope

LTD = Limited Scope

SP = Special Project



IV. Scope of TSP Performance Audits (continued)

<u>Other Non-Agency TSP Activities</u>	<u>Plan</u> <u>2009</u>	<u>2008</u>	<u>2007</u>	<u>2006</u>	<u>2005</u>
1. Treasury “G” Fund Investment Operations	–	–	–	FS	–
2. Investment Manager Operations (“F”, “C”, “S” and “I” Funds)	–	–	–	FS	–
3. Annuity Operations	–	–	FS	–	–
4. Board’s Staff Operations	–	–	LTD	–	–

FS = Full Scope

LTD = Limited Scope

SP = Special Project



IV. Scope of TSP Performance Audits (continued)

<u>Uniformed Services</u>	<u>Plan 2009</u>	<u>2008</u>	<u>2007</u>	<u>2006</u>	<u>2005</u>	<u>2004 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/LTD
4. Army - Aberdeen Proving Ground	—	—	—	—	—	LTD
5. Army - Defense Personnel Center	—	—	—	—	—	FS
6. Army - Fort Meade	—	—	—	—	—	LTD
7. Army - Fort Myers	—	—	—	—	—	R/FS
8. Bolling Air Force Base	—	—	—	—	—	FS
9. Defense Logistics Agency	—	—	—	—	—	FS
10. Department of Agriculture - NFC	—	—	—	—	—	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 & Human Resources	—	—	—	—	—	LTD
16. Department of Housing and Urban Development	—	—	—	—	—	R/FS
17. Department of Interior - Denver	—	—	—	—	—	R/FS
18. Department of Justice	—	—	—	—	—	R/LTD
19. Department of Labor	—	—	—	—	—	R
20. Department of State	—	—	—	—	—	R/FS

FS = Full Scope

LTD = Limited Scope

R = Follow-up Review



IV. Scope of TSP Performance Audits (continued)

<u>Federal Agencies (continued)</u>	<u>Plan 2009</u>	<u>2008</u>	<u>2007</u>	<u>2006</u>	<u>2005</u>	<u>2004 and Prior</u>
21. Department of Transportation - Oklahoma	—	—	—	—	—	R/FS
22. Department of Veterans Affairs	—	—	—	—	—	R/FS
23. DFAS - Charleston and Army - Ft. Monmouth	—	—	—	—	—	FS
24. DFAS - Columbus and Defense Logistics Agency	—	—	—	—	—	FS
25. DFAS - Denver and North Island Naval Air Station	—	—	—	—	—	R/FS
26. DFAS - Pensacola and Naval Sea System Command	—	—	—	—	—	FS
27. Environmental Protection Agency	—	—	—	—	—	FS
28. Federal Bureau of Investigation	—	—	—	—	—	FS
29. Federal Deposit Insurance Corporation	—	—	—	—	—	FS
30. General Services Administration	—	—	—	—	—	R/FS
31. Government Accountability Office	—	FS	—	—	—	—
32. House of Representatives	—	—	—	—	—	R
33. Kelly Air Force Base - San Antonio	—	—	—	—	—	R/FS
34. NASA	—	—	—	—	—	FS
35. National Security Agency	—	—	—	—	—	LTD
36. Naval Publications and Forms Center	—	—	—	—	—	R/LTD
37. Naval Research Laboratory	—	—	—	—	—	R/FS
38. Naval - Supply Center, Norfolk	—	—	—	—	—	R/LTD
39. Navy - Atlantic Fleet	—	—	—	—	—	LTD
40. Navy - Norfolk Naval Shipyard	—	—	—	—	—	R/LTD
41. Navy Regional Finance Center	—	—	—	—	—	R/FS
42. Nuclear Regulatory Commission	—	—	—	—	—	FS
43. Postal Service	—	—	—	—	—	R/FS
44. Treasury (Includes IRS)	—	—	—	—	—	FS

FS = Full Scope

LTD = Limited Scope

R = Follow-up Review



V. Tentative Schedule of Fiscal Year 2009 TSP Audits

<u>Performance Audits</u>	<u>Work Begins</u>	<u>FRTIB Exit</u>
Participant Support Process	TBD*	TBD
Computer Access Controls and Security	TBD*	TBD

* Preliminary planning meetings scheduled for late February.



VI. Summary of Open Recommendations

<u>IT-Related Audits</u>	<u>Fundamental Controls</u>	<u>Efficiency/ Effectiveness</u>	<u>Total</u>	<u># Open Originating Prior to 2008</u>
1. System Enhancements and Software Change Controls (1)	3	--	3	--
2. IT Operations Management/Mainframe (4)	1	--	1	1
3. Computer Access Controls and Security (1)	6	--	6	4
4. Security Penetration and Vulnerability (6)	--	--	--	--
5. Service Continuity Controls (1)	2	--	2	--
6. Post-implementation Review of the New System (5)	1	--	1	1



VI. Summary of Open Recommendations (continued)

<u>Process Audits</u>	<u>Fundamental Controls</u>	<u>Efficiency/ Effectiveness</u>	<u>Total</u>	<u># Open Originating Prior to 2008</u>
7. Account Maintenance (5)	--	1	1	1
8. Participant Support/ Call Centers (3)	--	3	3	3
9. Withdrawals (4)	--	4	4	4
10. Loan Operations (4)	--	1	1	1

**VI. Summary of Open Recommendations (continued)**

<u>Other Non-Agency TSP Activities</u>	<u>Fundamental Controls</u>	<u>Efficiency/ Effectiveness</u>	<u>Total</u>	<u># Open Originating Prior to 2008</u>
1. Treasury "G" Fund Investment Operations	--	--	--	--
2. Investment Manager Operations ("F", "C", "S" and "I" Funds)	--	--	--	--
3. Annuity Operations (2)	1	2	3	3
4. Board's Staff Operations (2)	1	--	1	1
Total Non-agency Recommendations	<u>15</u>	<u>11</u>	<u>26</u>	<u>19</u>

(1) The most recent report was FY 2008.

(2) The most recent report was FY 2007.

(3) The most recent report was FY 2006.

(4) The most recent report was FY 2005.

(5) The most recent report was FY 2004.

(6) Findings reported within the Computer Access report.



Department of Labor

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 (FERSA) of 1986 (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 Fiduciary Oversight Program

EBSA's TSP audit procedures are designed to comply with *Government Auditing Standards*, published by the 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 Fiduciary Oversight Program

EBSA's Program is designed to determine whether:

- The fiduciaries are acquiring, protecting, and using TSP resources economically, efficiently, and solely in the interest of TSP participants and beneficiaries;
- The fiduciaries have complied with FERSA and 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.



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

4. Other Benefits

Besides discharging the Secretary of Labor's statutory responsibilities for a TSP audit program, the EBSA Fiduciary Oversight Program provides the following benefits to TSP participants and beneficiaries:

- Certain audit assurances that their retirement assets are properly protected; and
- Potential opportunities for greater future cost savings through implementation of EBSA-identified enhancements to TSP system operations.



B. Examples of TSP Information Obtained for Each Audit

- Prior audit reports
- Organization charts
- Position descriptions
- Flowcharts
- Narratives describing work flows
- Descriptions of support systems
- Identification and evaluation 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 and regulations
- Conclude on the TSP fiduciaries' overall FERSA-related compliance
- Address EBSA, Federal Retirement Thrift Investment Board, and Agency concerns, as practicable
- Provide input for Congressional testimony
- 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 (Program Operations) for appropriate further action, if necessary
- DOL and contractors present significant findings and recommendations and next year's TSP audit plan annually at a scheduled Board meeting



E. Overview of the TSP Performance Audit Objectives

IT-Related Audits

1. System Enhancements and Software Change Controls
Determine whether: (1) policies and procedures are in place to control development, alteration and configuration of TSP software applications, (2) a software development lifecycle is followed for the development of TSP software applications, and (3) controls are in place over the authorization, testing, approval, and implementation of changes to existing application software and such changes are supported by appropriate documentation.
2. IT Operations Management/Mainframe
Determine the adequacy of operational efficiencies and management effectiveness in scheduling, hardware operations management, and physical access to IT equipment and information.
3. Computer Access Controls and Security
Determine whether controls safeguarding computerized access to data and programs are in place to prevent unauthorized use, modification, damage, or loss.



E. Overview of TSP Performance Audit Objectives (continued)

IT-Related Audits (continued)

4. Security Penetration and Vulnerability Assessment
Determine whether technical controls are in place to safeguard information resources and assets and to detect and respond to breaches to the TSP technical architecture.
5. Service Continuity Controls
Determine whether (1) a business continuity and disaster recovery program for all critical TSP systems exists, is operational, and is periodically tested; (2) critical system and production data are backed up on a regular basis, and backup tapes are stored off-site and periodically tested; (3) arrangements have been made for alternate data processing and telecommunication facilities; and (4) data processing, storage and transfer limits, and bottlenecks in the TSP environment are managed to enhance processing efficiency and availability.
6. Post-implementation Review of the New System
Document the controls and operation of the new TSP system, and review the accuracy of the data conversion.



E. Overview of TSP Performance Audit Objectives (continued)

Process Audits

7. Account Maintenance*

Determine whether (1) participant account balances accurately record summary and detail contributions and earnings, (2) processing occurs timely, (3) control procedures have been established and are in place for processing error corrections and breakage/lost earnings according to legal requirements, (4) participant forfeitures and forfeiture restorations are proper and accurate, and (5) participant account balances accurately reflect “G”, “F”, “C”, “S”, “I” and “L” Fund balances as elected by participants.

8. Participant Support/Call Centers*

Determine whether (1) TSP information remitted to the participant is accurate and timely, (2) participant inquiries are resolved properly and timely, and (3) confirmation and reject notices are processed accurately and timely.



E. Overview of TSP Performance Audit Objectives (continued)

Process Audits (continued)

9. Withdrawals*

Determine whether (1) procedures and controls are in place to ensure proper, accurate, and timely input, processing, disbursing, and recording of participant post-separation and in-service withdrawals; (2) policies and procedures relating to abandoned accounts protect the interest of former participants; and (3) the Agency is using reasonable methods for locating “lost” participants.

10. Loan Operations*

Determine whether procedures and controls are in place to ensure proper, accurate, and timely input, processing, and output of loan data.

*These process performance audits include testing of the process’s related application controls. This non-statistical testing determines whether the application controls over input, processing, and output are in place and functioning at the process level. Thus, conclusions on the operations at the process level are based on both automated and manual controls.



E. Overview of TSP Performance Audit Objectives (continued)

Other Non-Agency TSP Activities

1. Treasury “G” Fund Investment Operations

Determine whether the interest rate paid on “G” Fund investments is derived in accordance with FERSA and Agency requirements and whether the Treasury’s application of the interest rate to “G” Fund investments is accurate.

2. Investment Manager Operations (“F”, “C”, “S” and “I” Funds)

Determine whether (1) TSP transactions are processed accurately and timely, (2) investment management operations comply with FERSA, including conditions of applicable cross-trading and in-kind exemptions, (3) proxies of the “C”, “S” and “I” Funds are voted in accordance with applicable fiduciary standards, and (4) the vendor is complying with provisions of the contract between the Agency and the vendor.

3. Annuity Operations

Determine whether the vendor is processing TSP annuities in compliance with applicable FERSA provisions and TSP regulations.



E. Overview of TSP Performance Audit Objectives (continued)

Other Non-Agency TSP Activities (continued)

4. Board's Staff (Agency) Operations

Determine whether Agency policies and procedures comply with FERSA and provide for effective management control over daily TSP operations. This task includes reviews of the Agency's procurement practices and the Agency's EDP general control environment.

5. Review of CIA OIG TSP Audit

Determine whether the CIA OIG TSP audit report and supporting workpapers comply with TSP audit objectives set forth in the DOL EBSA Fiduciary Oversight Program and with applicable interagency (e.g., DOL, CIA, and GAO) agreements.



E. Overview of TSP Performance Audit Objectives (continued)

Agency TSP Activities

1. Federal Agency/Uniformed Services Audits

Full Scope: Completion of all applicable TSP Fiduciary Oversight Program modules.

Follow-up Review: Determine the status of prior EBSA recommendations.