THRIFT
SAVINGS
PLAN

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
1250 H Street, NW   Washington, DC 20005

February 5, 2007

Mr. Ian Dingwall
Chief Accountant
Employee Benefits Security
  Administration
United States Department of Labor
200 Constitution Avenue, N.W.
Suite 400
Washington, D.C. 20210

Dear Ian:

This is in response to your letter dated January 9, 2007, transmitting the KPMG LLP report entitled "Employee Benefits Security Administration Review of the Thrift Savings Plan Disaster Recovery and Continuity of Operations" dated March 3, 2006 (Updated with additional information obtained through October 3, 2006).

We are pleased to note that the auditors concluded that the Agency has demonstrated the ability to recover mainframe and supporting operations in the event of a declared disaster.

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.

I also want to thank you for your efforts in closing prior year recommendations.

Sincerely,

Thomas K. Emswiler

Thomas K. Emswiler
Acting Executive Director

Enclosure

Executive Director's Comments on the
Employee Benefits Security Administration's "Review of the
Thrift Savings Plan Disaster Recovery Capability",
dated March 3, 2006

Recommendations To Address Fundamental Controls:

2005 Mainframe Operations Recommendation No. 1:

The Agency's Senior Information Security Officer (SISO) should:

- Update and approve the TSP Security Plan to encompass the breadth of management, operational, and technical controls of the TSP system. This includes leveraging and incorporating the finalized data security standard elements, updated data classification rankings resulting from the most recent risk assessment, and updated incident handling procedures.

Comment: We concur with this recommendation. The original TSP Security Plan was completed and signed by the outgoing CIO in 2005. The succeeding CIO initiated a comprehensive review, which is nearing completion and which will address these issues.

- Update, approve and promulgate security awareness training requirements for contractors and verify that all contractor staff attends security awareness training and attendance is tracked consistent with federal criteria.

Comment: We concur with this recommendation and consider it to be closed. The Agency procured a leading edge IT Security awareness training program in 2006, and all personnel accessing FRTIB systems are required to take and pass the graded training. In fact, as of January 31, 2007, over 500 Agency and contractor employees have taken the training. All Agency or contractor new hires are required to take this training.

- Perform or require background investigations, commensurate to the level of position sensitivity designated by the job role, for contractor staff that are exposed to Agency information or information resources and retain evidence of investigation completion.

Comment: We concur with this recommendation and consider it to be closed. Contractor staff's access to the TSP system and call center networks is contingent on review and approval of a successful background investigation. The contractor is responsible for initiating the background investigation and forwarding the results to the appropriate FRTIB COTR for review. The FRTIB COTR reviews the findings against the Agency's guidelines and makes a determination based on those guidelines. The COTR (or designee) then notifies the contractor's Security Officer when a background investigation has been reviewed and approved so that appropriate system access can be granted. Using the example of a Participant Service Representative at the Clintwood call center, the SI International Security Officer then notifies the Clintwood Network Administrator (and other appropriate personnel) when access has been established. The Clintwood Human Resources Manager tracks separated employees and notifies the Clintwood Network Administrator of the separations in order to remove access from the LAN. The Human Resources Manager concurrently notifies the SI-International Security Officer in order to remove access to the PSR and PowerImage applications. Access to the PSR and PowerImage applications is centrally managed through the OmniSecurity software, a COTS tool that centrally manages logical access parameters, such as password length and composition and concurrent logins.

- Implement service level reporting for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management, consistent with contract requirements.

Comment: We concur with this recommendation. These requirements will be included in the follow on contracts for the operation of the data centers.

2005 Mainframe Operations Recommendation No. 2:

The Agency's SISO should:

- Document the process for and report the results of reviewing access rights to global security settings, administrative authorities and sensitive system datasets settings on a semi-annual basis and consistent with account recertification efforts for excessive or inappropriate access permissions. In addition, ACIDs that have been inactive for 180 days must be reviewed and removed if no longer required.

Comment: We concur with this recommendation. We are in the process of doing this as part of a major reconfiguration of the TSP mainframe. SI has hired an expert in CA's Top Secret software, and an exhaustive review is underway to update the policies and procedures so that they will provide appropriate access separation from development, test and production areas, as well as from systems and applications.

- Update logical access control policies and procedures to include recertification of accounts on a semi-annual basis and requirements for obtaining, maintaining, and controlling access to sensitive system utilities and functions.

Comment: We concur with this recommendation. We are in the process of doing this as part of a major reconfiguration of the TSP mainframe. SI has hired an expert in CA's Top Secret software, and an exhaustive review is underway to update the policies and procedures so that they will provide appropriate access separation from development, test and production areas, as well as from systems and applications. A semi-annual review process will be put in place as part of this activity.

2005 Mainframe Operations Recommendation No. 3:

The Agency's SISO should document and communicate configuration management procedures to capture and track scheduled or requested changes from authorization through testing and approval for use in the production environment.

Comment: We concur with this recommendation. The Agency has invested in a comprehensive, commercial off the shelf (COTS) software suite, and we are in the process of implementing it at this time. The Serena advanced software suite will provide advanced version control for team-based development. Serena's version manager organizes, manages and protects software assets to support software configuration management across the enterprise.

2006 Recommendations to Address Fundamental Controls:

2006 Recommendation No. 1:

The Agency should conduct a formal recovery site evaluation of risk and strengthen its procurement practices related to sole source selections. A formal risk assessment would identify controls in operation, evaluate potential vulnerabilities with existing controls, and provide a documented basis to make the necessary business decisions either to mitigate or accept known risks, e.g., stacking of commercial fertilizing agents and access to an underground delivery tunnel. Document vendor justification in accordance with Federal Acquisition Regulations (FAR) and ensure such documentation is produced and maintained in the future. Specifically, Agency management should:

- Conduct and document a risk assessment of the present disaster recovery site location. The risk assessment should be conducted in accordance with Agency requirements and OMB guidance, including an evaluation of any weaknesses identified at the site. The Agency's assessment should include documentation of the effectiveness of controls and countermeasures in place to manage risk to an acceptable level.

Comment: We concur with this recommendation with respect to the need for risk assessments of the Disaster Recovery site. With respect to the procurement of the Pittsburgh site, we note that the Agency complied with the FAR, in this case, for the reasons given in the sole source justification. The former Director of Automated Systems visited the site to determine if the site met appropriate requirements, and determined that it did. The current CIO has visited the site multiple times, and concurs with the assessment of his predecessor.

We note that there is nothing preventing the disaster recovery site from providing uninterrupted service to the TSP participants, and, in fact, the Agency continues to make positive progress in this area. The report cites fertilizer, which was never a threat, and is no longer present. The fertilizer issue was explained in great detail by the Chief Information Officer, and he provided them with the Materials Safety Data Sheet (MSDS) showing that this is not a problem. The report cites a delivery truck tunnel and mall freight which are not considered significant threats, given the anonymity of the disaster recovery site. In summary, the Pittsburgh DR site is anonymous; that is, it is in no way overtly connected with the TSP, or with any other customer. The profile of this facility is one of "hiding in the open," and it would serve minimal benefit to the TSP participants were we to relocate to an overt, hardened site with the obvious security measures that must accompany such a site.

- Enforce controls over sole source procurement processes, including the retention of documentation that supports the Agency's vendor selection.

Comment: We concur with this recommendation and consider it to be closed. As noted above, we believe that we conducted the procurement of both the primary and backup data centers in accordance with the FAR and that the sole source was justified for the backup data center for the reasons stated in the documentation, which was retained and was provided to the auditors.

2006 Disaster Recovery Capability Recommendation No. 2:

The Agency should improve its Disaster Recovery and Continuity of Operations Program by updating the required documentation to ensure clear communication and training for a timely recovery of operations in the event of business disruption or a disaster. Specifically, we recommend that the Agency:

- Update, finalize, and disseminate all business continuity documentation (i.e., Business Continuity Plan, Business Assurance Plan, Business Continuity Checklist, and Business Continuity Contact Information), and train the requisite personnel.

Comment: We concur with this recommendation. However, plans still in progress are usable and, because of ongoing change management, will never be truly "final". Again, the effectiveness of these plans was shown by their utility in overcoming Hurricane Katrina. We have phone trees in place. We have organizational lists showing who is in charge of each facet of the system and how to contact them. The CIO recently completed market research and procured the Living Disaster Recovery System (LDRPS) by Strohl Systems. LDRPS is an industry leading software solution for the development and maintenance of business continuity plans. In the meantime, FRTIB has a tested plan.

- Plan for and complete comprehensive service continuity testing exercising all relevant business continuity components with relevant stakeholders. Also consider administering periodic training and performing a tabletop exercise with the business assurance team members to ensure complete and accurate coverage of the business continuity processes.

Comment: We concur with this recommendation. Training for some Agency and contractor staff is planned for February 2007. In addition the Agency will perform periodic tabletop testing at the business unit level, as well as conducting a comprehensive annual test.

- Document and perform backup tape restoration procedures on the disaster recovery mainframe to ensure that data can be successfully restored from tape.

Comment: We concur with this recommendation with respect to ensuring data can be successfully restored from tape. The Agency will adopt a practice of periodically testing tapes for restorability, or will implement software controls that verify this. However, we do not concur that performing comprehensive tape restoration is a good practice or a responsible way to spend business continuity dollars.

U.S. Department of Labor

Employee Benefits Security Administration
Washington, D.C. 20210

January 9, 2007

Mr. Gary A. Amelio
Executive Director
Federal Retirement Thrift Investment Board
1250 H Street, N.W., Suite 200
Washington, D.C. 20005

Re: "Employee Benefits Security Administration Review of the Thrift Savings Plan Disaster Recovery and Continuity of Operations," dated March 3, 2006 (Updated with additional information obtained through October 3, 2006)

Dear Gary:

Please find enclosed ten copies of the above report that communicate KPMG LLP's initial review of TSP's disaster recovery and continuity of operations capabilities at TSP's Pittsburgh, Pennsylvania, site.

Overall, the Agency has demonstrated the ability to recover mainframe and supporting operations in the event of a declared disaster. However, we report several significant matters that potentially pose site specific access and operational risks that could impact the TSP's recovery facility. Additionally, other significant matters, previously reported but yet to be corrected, represent additional potential risks to the disaster recovery site's continuity of operations ability.

We request your written response to the report's recommendations within 30 days. Your response should provide planned actions with respective target dates or reasons for non-compliance or disagreement. If I can be of assistance, please contact me at 693-8361 or Mr. William Bailey at 693-8372.

Sincerely,
W/H Bailey
for
IAN DINGWALL
Chief Accountant

Encl

Employee Benefits Security Administration

Review of the Thrift Savings Plan

Disaster Recovery and Continuity of Operations

March 3, 2006

(Updated with additional information obtained through October 3, 2006)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we performed a special project to assess the Thrift Savings Plan (TSP) disaster recovery and continuity of operations capabilities. We performed this special project at the Federal Retirement Thrift Investment Board Staff (the Agency) offices in Washington, D.C., SI International in Reston, Virginia, and at Switch and Data's disaster recovery facility in Pittsburgh, PA. Our fieldwork was performed from January 31 through March 3, 2006.[1] This is our first special project of the disaster recovery capability of the TSP recordkeeping system since the Agency implemented the new system in June 2003.

In the wake of Hurricane Katrina, the tragic events of Oklahoma City, and September 11, 2001, the TSP fiduciaries must exercise constant vigilance over the safety and security of the federal government's personnel and property, including the ability to restore TSP data and operations timely and cost effectively. Unlike the legacy system's 48-hour recovery requirement, the new TSP recordkeeping system recovery goal is set at 24 hours or less. In October 2004, through sole source selection, the Agency chose SI International to implement and to operate a disaster recovery operation using computer hardware, software, and networking equipment owned by the Agency. SI International subcontracts with Jacob and Sundstrom to provide related system programming services, and with Switch and Data to provide the disaster recovery facility located in Pittsburgh, PA.

While electronic transmissions to the backup site act as the primary data backup mechanism, SI International has implemented tape backup solutions for mainframe, UNIX, and Windows platforms for the production mainframe as a secondary backup measure. Tape backups are sent off-site weekly to the data storage vendor, Iron Mountain, in Sterling, VA. The TSP data is transmitted to the disaster recovery facility on a daily basis. Incremental backups occur hourly and capture only those changes that occurred since the last backup. A full backup is performed weekly. In addition, all backups performed at the Reston data center are written to tape and stored off-site by a vendor in an access-controlled facility. To keep both primary and disaster recovery sites synchronized, SI International provides electronic replication of essential production software and data to maintain the production environment using StorageTek (STK)

[1] Our assessment of certain information obtained through October 3, 2006, but related to the period of review has been incorporated into this report. In addition, certain management representations have been provided and are incorporated as necessary, but were not verified as part of this review.

virtual array (SVA) disk systems with Snapshot software to minimize the volume of data transfer necessary.

The TSP business assurance and continuity plans apply to the functions, operations, and resources necessary to restore and to resume TSP system operations as it is installed at the primary location, Reston, VA. As mentioned earlier, the TSP disaster recovery site is located in Pittsburgh, PA. This site has the computer equipment, operational and application software, network infrastructure, mainframe and server connectivity required to serve as the alternate production operations site until the Reston, VA data center is functioning again, or a new site is fully operational. The approach to business assurance for the TSP system consists of four key steps: (1) Notification Procedures, (2) Damage Assessment Procedures, (3) Recovery Phase, and (4) Return to Normal Operations. In order to facilitate the business continuity procedures, a series of checklists have been drafted to identify the requisite tasks, task owners, and task dependencies to be followed in a business continuity or disaster recovery scenario.

In February of 2006, under the direction of the Agency, SI International conducted a business continuity test that focused solely on restoring mainframe capabilities, testing limited access and functionality of supporting TSP applications, and running parallel batch processes at the Pittsburgh, PA disaster recovery facility. On February 23 and 24, 2006, we observed this planned business continuity test, which included testing for mainframe accessibility and functionality of certain TSP applications[2]. Because the Agency relies on one-way data replication from the production mainframe to the backup mainframe, test cases for the various TSP applications and the various reports produced were used to verify the accuracy and completeness of the data on the backup mainframe to the production mainframe. The Agency demonstrated its ability to restore the mainframe and TSP applications at the Pittsburgh, PA recovery site. SI International used various check-in points over the course of the two day period to communicate testing progress and the results of planned test cases. Any deviations from expected results in the planned test cases were dealt with during check-in meetings with corrective action plans being created to address any open items. Lessons learned from the exercise were captured to facilitate updates to the Agency's documentation and future tests.

[2] Supporting systems include: Participant Service Representative (PSR), Court Order Document Imaging System (CODIS), AdHoc Query tool, Asset Manager Interface (AMI), Cash Flow Investment System (CFIS), PowerImage (PI), Agency Payroll Interface (API), Federal Reserve Board Interface (FRBI), TSP Reporting Interface System (TRIS), Savantage, TSP Public Web, and Obligation Tracking and Invoicing System (OTIS).

The scope of our fieldwork procedures included the examination of disaster recovery policies and procedures and related information technology (IT) general controls in place at the recovery facility in Pittsburgh, PA from October 1, 2005, through March 1, 2006. We designed our engagement procedures to comply with the objectives for performance audits as defined by *Government Auditing Standards,* issued by the Government Accountability Office (see Section I.B). Detailed objectives of this engagement are enumerated within Section I.A. Summary objectives for conducting this work include: (1) assessing the general controls of the disaster recovery site, (2) assessing planning and preparation to continue operations during a disaster and when recovering from a disaster, and (3) following up on certain prior year findings and recommendations related to operations of the TSP system.

We accomplished these objectives by (1) obtaining an understanding of the contractor and subcontractor arrangement for operating the backup data center located in Pittsburgh, PA, (2) performing a walk-through of the backup data center operations, (3) testing select IT general controls, (4) reviewing the activities undertaken by the Agency to solicit and select the current contractor and backup data center site location, and (5) reviewing the status of prior EBSA TSP recommendations as well as the Agency's applicable formal responses.

Overall, based on interviews conducted (Appendix A), documents inspected (Appendix B), and test procedures performed within the FY 2006 Disaster Recovery Capability audit program, we conclude that the Agency has demonstrated the ability to recover mainframe and supporting operations in the event of a declared disaster. However, we observed matters that potentially pose site specific access risks that could impact the TSP's recovery facility. Specifically, we noted a delivery truck tunnel that runs directly beneath the site. We also noted that unloaded freight is routinely stored in areas adjacent to the data center, including, during our walk-through procedures, approximately 50 sacks of an undetermined fertilizing agent stacked against an external wall to the data center. (See Section III. C. for additional discussion.)

We report 2 new recommendations that address fundamental controls as part of our FY 2006 engagement. Our recommendations will collectively contribute to the implementation of a strengthened service continuity program. We recommend that:

1. The Agency should conduct a formal recovery site evaluation of risk and strengthen its procurement practices related to sole source selections. A formal risk assessment would identify controls in operation, evaluate potential vulnerabilities with existing controls, and provide a documented basis to make the necessary business decisions to either mitigate or

accept known risks, e.g., stacking of undetermined fertilizing agents and access to an underground delivery tunnel. Document vendor justification in accordance with Federal Acquisition Regulations (FAR) and ensure such documentation is produced and maintained in the future. Specifically, Agency management should:

- Conduct and document a risk assessment of the present disaster recovery site location. The risk assessment should be conducted in accordance with Agency requirements and OMB guidance, including an evaluation of any weaknesses identified at the site. The Agency's assessment should include documentation of the effectiveness of controls and countermeasures in place to manage risk to an acceptable level.
- Enforce controls over sole source procurement processes, including the retention of documentation that supports the Agency's vendor selection.

Without completing a thoroughly documented risk assessment of the TSP disaster recovery site, the Agency is not fully able to report to the TSP fiduciaries (i.e., Board members and the Agency's Executive Director) whether potential risks associated with establishing the TSP's disaster recovery site operations at its current location are acceptable. Also, without the Agency's performing adequate market research justifying the cost estimate used to sole source add-on services for the current disaster recovery site operations contract, the Agency is not fully able to report to the TSP fiduciaries the cost effectiveness of this use of TSP assets on behalf of TSP participants.

2. The Agency should improve its Disaster Recovery and Continuity of Operations Program by updating the required documentation to ensure clear communication and training for a timely recover of operations in an event of a business disruption or disaster. Specifically, we recommend that the Agency:

   - Update, finalize, and disseminate all business continuity documentation, (i.e., Business Continuity Plan, Business Assurance Plan, Business Continuity Checklist, and Business Continuity Contact Information), and train the requisite personnel and stakeholders.
   - Plan for and complete comprehensive service continuity testing exercising all relevant business continuity components with relevant stakeholders. Also consider administering periodic training and performing a tabletop exercises with the business assurance team members to ensure complete and accurate coverage of the business continuity processes.
   - Perform periodic backup tape restoration procedures at the disaster recovery site.

Without final, approved business continuity documentation and completed service continuity testing, the TSP's fiduciaries' ability to safeguard TSP participants from lost data and disrupted service and to provide orderly and efficient resumption of operations in the event of an actual disaster may be at risk.

These recommendations have been communicated over the course of the engagement. The Agency has represented that it has already taken or plans to implement the recommendations described above. Management's representations as of September 2006 were not verified as part of this special project.

We also reviewed the status of four prior recommendations. One recommendation was communicated in our FY 2004 report, "Post-Implementation Review of the New Thrift Savings Plan Recordkeeping System, December 12, 2003," and the remaining three were communicated in our FY 2005 report, "Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005." The FY 2004 recommendation addressed the disaster recovery capabilities of the TSP system, including the need for routine testing. This recommendation has been partially implemented and is considered closed. As part of this report, we have included the open portion in FY 2006 Recommendation No. 2. One FY 2005 recommendation is partially implemented but remains open with the other two FY 2005 recommendations. All three FY 2005 recommendations communicate fundamental control weaknesses over information security policy, logical access controls, and configuration management policies and procedures. (See Section III. B. for additional discussion.)

Section I of this report discusses the EBSA's objectives, scope and methodology, and the organization of the report. Section II is an overview of the disaster recovery site operations and the related IT general control environment. Section III presents the details the support the current year and the status of prior year findings and recommendations. The Agency should review and consider all recommendations for timely implementation. Agency senior management members worked with us to develop the recommendations. We discussed these recommendations with the appropriate Agency representatives (Appendix C). Responses were positive and constructive.

I. INTRODUCTION

A. Objectives

KPMG LLP was contracted by the U.S. Department of Labor, Employee Benefits Security Administration (EBSA) to perform services under Section 8477(g) of the Federal Employees' Retirement System Act (FERSA) of 1986, as amended. These services included a special project related to the Thrift Savings Plan (TSP) disaster recovery capabilities and a review of the status of prior applicable recommendations.

The specific objectives of this special project were to:

- Assess the TSP disaster recovery program to determine whether policies, procedures, and related information technology (IT) controls at the disaster recovery site in Pittsburgh, PA are in place to restore TSP operations in the event of a disaster;
- Assess the completeness of the continuity of operations and disaster recovery planning for the TSP, including any tests and corrective actions taken; and
- Follow-up related prior year findings and recommendations. Specifically, assess the status of recommendation number 2004-3 related to the TSP system's disaster recovery capabilities and reported in "Post-Implementation Review of the New Thrift Savings Plan Recordkeeping System, December 12, 2003;" and recommendation numbers 2005-1, 2005-2, and 2005-3 related to security program policies and procedures, logical access controls, and configuration management policies and procedures reported in "Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005."

B. Scope and Methodology

We performed the engagement in accordance with the EBSA TSP Fiduciary Oversight Program, which is designed to comply with *Government Auditing Standards* issued by the Government Accountability Office (GAO). In particular, we designed our engagement to conform with a performance audit defined by the *Government Auditing Standards,* as "an objective and systematic examination of evidence for the purpose of providing an independent assessment of the performance and management of a program against objective criteria as well as assessments that provide a prospective focus or that synthesize information on best practices or cross-cutting issues." We performed our engagement in four phases: (1) planning, (2) arranging for the engagement with the Federal Retirement Thrift Investment Board Staff (Agency), (3) testing and interviewing, and (4) report writing.

The planning phase was designed to ensure that team members developed a collective understanding of the activities and controls associated with the backup mainframe operations and data center. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we conducted interviews, collected and inspected documentation and evidence, and performed observation and walk-through activities. We conducted these test procedures primarily at SI International's location in Fair Oaks, VA; Agency headquarters in Washington, DC; and at the Switch and Data backup data center for the TSP in Pittsburgh, PA.

Testing procedures over IT general control areas at the backup data center were categorized based on the objectives and control areas of the GAO's *Federal Information System Controls Audit Manual* (FISCAM). The FISCAM areas include testing of the design and effectiveness of security policies, access controls, system software controls, change controls, segregation of duties controls, and service continuity controls.

Procedures for testing the TSP's disaster recovery capability included a two-day site visit to SI International, which covered the inspection and analysis of business continuity preparedness and disaster recovery testing documentation. When our test procedures over IT general controls required us to select a sample of a population for testing, we used a judgmental sample selection methodology. Accordingly, our conclusions are applicable to the sample we tested, and were not extrapolated to the population.

The report-writing phase entailed drafting a preliminary report, conducting our exit conference (Appendix C), providing a formal draft report to the Agency for review, and preparing and issuing the final report.

C. Organization of Report

Section II includes an overview of the TSP, a summary of the disaster recovery site contract management, and a description of the disaster recovery capability and related general control environment. Section III presents all findings and recommendations addressed by this report.

II. OVERVIEW OF THE DISASTER RECOVERY SITE OPERATIONS

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act (FERSA) of 1986, as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS). The TSP 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 Congressional employees. For FERS participants, the TSP also provides agency automatic (1 percent) and matching contributions. The TSP began accepting contributions on April 1, 1987, and as of December 31, 2005, had approximately $173 billion in assets and 3.6 million participants.

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

B. Disaster Recovery Site Contract Management

Our first objective was to assess the TSP disaster recovery program to determine whether policies, procedures, and related information technology (IT) controls at the disaster recovery site in Pittsburgh, PA, are in place to restore TSP operations in the event of a disaster. The need for current and effective disaster recovery capability was demonstrated in September 2004 when the TSP recordkeeper, U.S. Department of Agriculture National Finance Center (NFC), in New Orleans, LA, was closed because of threats from Hurricane Ivan. Accordingly, the disaster recovery plan was exercised.

The Agency determined that a 48-hour recovery goal would no longer suffice to support the daily-valued processing required for the TSP system and supporting business functions. On October 21, 2004, the Director, Office of Automated Systems, issued a memorandum to the Acting Deputy Director, Administration, regarding the selection of disaster recovery site operations, which stated that several alternatives for providing disaster recovery in 24 hours or less had been evaluated and concluded that contracting with SI International for the new disaster recovery data center and its operation afforded a unique opportunity to save costs by sharing resources to operate and maintain both the Reston, VA data center and the disaster recovery site. For this reason, the Agency considered SI International the sole source for the work, quoting Federal Acquisition Regulation (FAR) section 6.302-1(a)(2)(ii) and 41 United States Code 253(c) as justification for contracting without providing for full and open competition.

SI International is required to provide a functioning disaster recovery site and monthly status reports. To keep both primary and disaster recovery sites synchronized, SI International provides electronic replication of essential production software and data to maintain the production environment using StorageTek (STK) virtual array (SVA) disk systems with Snapshot software to minimize the volume of data transfer necessary. While electronic transmissions to the backup site act as the primary data backup mechanism, SI International has implemented tape backup solutions for mainframe, UNIX, and Windows platforms for the production mainframe as a secondary backup measure, with tape backups being sent off-site to the data storage vendor, Iron Mountain, in Sterling, VA.

C. Disaster Recovery Capability and Related Assessments

This section contains a description of the disaster recovery testing, continuity of operations plan (COOP), and the disaster recovery site's IT general control environment.

a. Disaster Recovery Testing

Our second objective was to assess the completeness of the continuity of operations and disaster recovery planning for the TSP, including any tests and corrective actions taken during the most recent testing. Since the implementation of the daily-valued TSP recordkeeping system (TSP system) in June 2003, the TSP system's disaster recovery capabilities had not been formally or comprehensively tested. Delays were caused by subsequent procurement of a new mainframe and transition of hosting operations to Reston, VA.

During 2006, under the direction of the Agency, SI International conducted a series of phased business continuity tests, focusing solely on bringing up the disaster recovery mainframe, testing limited access and functionality of supporting TSP applications, and running batch processes. On January 26 and 27, 2006, SI International conducted internal preparations for the scheduled test on February 23 and 24, 2006. This preparation included a series of tasks to establish connectivity and interoperability to the disaster recovery mainframe. For example, Jacob and Sundstrom, the subcontractors who perform system engineering duties on the mainframe, broke and then reestablished the link from the Reston Data Center (RDC) to the backup data center. Then, OmniPlus was tested for interface to the applications, the DB2 databases were loaded and the team leads tested the applications' operability and data interfaces and dependencies. Issues from this review were noted for resolution before the next test. On February 9 and 10, 2006, the entire upcoming business continuity test cycle was run. The entire nightly batch cycle was run to process the VTRAN transactions and produce the PreNote 1 and PreNote 2 reports.

On February 23 and 24, 2006, the planned testing was performed, which included testing for mainframe accessibility and functionality. Specifically, this testing included an analysis of accessibility and functionality of certain TSP applications (i.e., Participant Service Representative (PSR), Court Order Document Imaging System (CODIS), AdHoc Query tool, Asset Manager Interface (AMI), Cash Flow Investment System (CFIS), PowerImage (PI), Agency Payroll Interface (API), Federal Reserve Board Interface (FRBI), TSP Reporting Interface System (TRIS), Savantage, TSP Public Web, and Obligation Tracking and Invoicing System (OTIS)), and the disaster recovery mainframe's performance of various batch processes (i.e., Unified, PreNote1 and PreNote2) and reporting accuracy (i.e., PF/FC balancing reports, master file record count, GL109 pre- and post- transition and additional management reports). Because the Agency relies on one-way data replication from the production mainframe to the backup mainframe, test cases for the various TSP applications and the various reports produced were used to verify the accuracy and completeness of the data on the backup mainframe. See Section II.C.c.6., Service Continuity, for additional details on the data replication process.

b. Continuity of Operations Plan

The TSP business continuity plan applies to the functions, operations, and resources necessary to restore and resume TSP system operations as it is installed at the primary location. As mentioned earlier, the TSP disaster recovery site is located in Pittsburgh, PA. This site has the computer equipment, operational and application software, network infrastructure, mainframe and server connectivity required to serve as the alternate production operations site until the RDC is functioning again, or a new site is fully operational. The business assurance architecture is designed with a recovery time objective (RTO)[3] of 4 hours and a recovery point objective

[3] RTO is the period of time in which systems, applications, or functions must be recovered after an outage. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. (Source: www.drj.com)

(RPO)[4] of 1 hour. The approach to business assurance for the TSP system consists of four key steps: (1) Notification Procedures, (2) Damage Assessment Procedures, (3) Recovery Phase, and (4) Return to Normal Operations, described below.

1. Notification Procedures

In the event that the RDC becomes inoperable, the following sequence of events would occur to bring the backup site into service:

- The first responder notifies the RDC Operations Manager of the emergency.
- The RDC Operations Manager notifies the Agency's Director of Automated Systems and TSP Project Manager (i.e., COTR), and the VP SI Financial Systems (SI Program Manager) of the situation.
- The SI Program Manager contacts TSP Applications and Call Center managers. The RDC Operations Manager notifies the staff. The COTR notifies all other parties. He (or an authorized TSP agent) communicates with the media or any other external parties.
- The SI Program Manager, the RDC Operations and TSP Application managers (also known as the Business Assurance Team (BAT) or their designated successors) meet to begin the process of assessing the damage and executing the plan to get the backup systems fully operational. Managers notify team members and direct them to complete the assessment procedures to determine the extent of damage and estimated recovery time and to begin the process of bringing the backup systems on-line.
- The BAT members assess the damage for their assigned areas and report findings to other BAT members.
- The BAT members launch a coordinated effort to get the backup site fully operational. This includes ensuring that the correct individual is in place to perform the responsibilities for that assignment, such as switching communications and network connectivity from the RDC to the backup site, validating server connectivity for internal applications and external entities, synchronizing mainframe and server databases and files, copying database incremental updates and OmniPlus files to the appropriate targets at the backup site, and validating application operability.

[4] RPO is the maximum amount of data loss the business can incur in an event. It is the targeted point in time to which systems and data must be recovered after an outage as determined by the business unit. (Source: www.drj.com)

When the backup site is fully operational and services are available, the SI Program Manager communicates status to the COTR. The COTR decides whether operations will commence at the backup site and communicates the decision to the appropriate parties.

2. Damage Assessment Procedures

In an emergency, the TSP's top priority is to preserve the safety and health of its staff. The RDC Operations Manager would verify that personnel are not endangered and then determine the following (*first assessment*):

- The cause of the disruption;
- The potential for additional disruption or damage;
- The affected physical area and status of physical infrastructure; and
- The status of IT equipment functionality and inventory, including items that will need to be replaced, and the estimated time to repair services to normal operations.

The RDC Operations Manager is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site. In addition, the RDC Operations Manager will notify the alternate site that a contingency event has been declared and to prepare the facility for the transfer of operations. The remaining personnel will also be contacted with information regarding the general status of the incident. The BAT team leads would notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

For each TSP subsystem (and associated databases) suspected of suffering injury, the appropriate software team will determine equipment loss or damage, software disruption, data loss and/or other serious consequences of the event, as well as possible remediation. If the TSP subsystem can be operationally tested, testing should be performed. The following questions are examples of those that should be asked and the answers documented:

- At exactly what point did the TSP subsystem fail (date and time)? What was the relation to the daily processing cycle?
- What was the extent of loss to TSP data? Would normal database recovery methods have preserved much of the data? How much data would have to be re-entered into the TSP system?
- What was the extent of damage to equipment, vendor-provided software, communication features, and electronic and hardcopy files?
- How much of the TSP subsystem software is re-usable?

- Could a possible remediation or recovery strategy be developed (inclusive or exclusive of the concepts expressed in this document)?

The questions and answers should be provided to management to influence the recovery operations.

3. Recovery Phase

The procedures for recovering the TSP system at the alternate site include:

- Ensuring that the correct individual is in place to perform the responsibilities for that assignment;
- Switching communications and network connectivity from the RDC to the backup site;
- Validating server connectivity for internal applications and external entities;
- Synchronizing mainframe and server databases and files; and
- Validating application operability.

4. Return to Normal Operations

This section discusses activities necessary for restoring TSP system operations at the TSP original data center or a new site, which would need to be selected. When the data center has been restored, TSP system operations must transition back from the alternate site. The goal is to provide a seamless transition of operations from the alternate site to the data center.

All equipment and software should be restored and/or rebuilt to recover the desired production environment:

- Each team should test all relevant equipment, communications, network infrastructure, and application functionality at the RDC or the new operations site.
- Once each team has verified proper operating status, the system should synchronize the databases and files for both the server and mainframe.

Once the RDC or the new location is operational, the following sequence of events should occur:

- The RDC Operations Manager will communicate that the original or new site is ready for production operations. He will notify the COTR and Program Manager that the equipment is installed, fully operational and equipped for production operations, the communication and network infrastructure are in place and tested, applications are functioning correctly, the correct software version is installed, data replication from the backup site to the original or new site is working correctly, and mainframe and server databases and files are in sync.

- The COTR will authorize the transition back to the original or new site and will notify the appropriate parties.
- The BAT members will convene to discuss ways to improve the business assurance planning documentation capture lesson learned for subsequent tests.

Once the RDC is handling the processing, the recovery site should resume asynchronous transmission to the backup site.

In order to facilitate the business continuity procedures, a series of checklists have been created to identify the requisite tasks, task owners, and task dependencies to be followed in a business continuity or disaster recovery scenario. The checklists contain procedures for the following topics:

- Notification and assessment
- API and FRBI
- CODIS
- CFIS
- DB2 (API and AdHoc)
- Reston Payroll Office (RPO)
- System Administration
- AdHoc Query Tool
- PI
- TRIS
- OmniPlus
- Obtaining status and verifying operability of Business Assurance Site (BAS)
- TSP Web
- Integrated Voice Response (IVR)
- OTIS
- Reporting, Notices, and Statements
- Call Center Managers
- Site Management
- PSR
- AMI
- Lockbox
- Accounting

According to the Agency, each business continuity process and system has points of contact and lines of succession for communication in order to facilitate timely notification to the assigned party or their backup(s). In addition, supplemental documentation has been identified to be used in emergency situations where TSP system operational expertise and documentation is lacking. The documents pertain to TSP software configuration management, TSP mainframe security, TSP system security, TSP security policies and procedures, tape retention, TSP system and technical architectures, TSP system government property list, and the TSP application list.

c. Disaster Recovery Site's IT General Control Environment

This section provides a high-level description of the controls in place over the backup mainframe operations at the Pittsburgh, PA, disaster recovery site, specifically covering the six *Federal Information Systems Control Audit Manual* (FISCAM) general control areas we tested.

1. Security Program

The backup mainframe operations are governed by the Agency's draft TSP Security Plan and supplemental draft TSP policies and procedures related to data security, access administration, and security awareness training. Additional procedures for conducting background investigations, obtaining signed non-disclosure agreements, and responding to security incidents are documented. The Agency and its contractors are bound by the requirements of the draft TSP Security Plan and supporting security-related polices and procedures. In addition, contractors are responsible for adhering to the security-specific requirements and responsibilities documented in their contractual statements of work.

The Agency uses a risk assessment process to aid in determining adequate, cost-effective security measures, identifying threats and vulnerabilities, and determining the effectiveness of current or proposed safeguards. While a formal risk assessment over the disaster recovery site data center has not been conducted, the Executive Director and the immediately prior Director of Automated Services communicated on-the-record during the December 20, 2004, Board Members' meeting that they had visited the Pittsburgh disaster recovery site data center and "were satisfied with the site" selection.

As communicated in the EBSA's 2005 TSP audit report, "Post-Implementation Review of the Thrift Savings Plan Mainframe Operations," security awareness training is to be administered to all TSP system users. The training includes leaving workstations unattended, reporting suspicious activity, using passwords or privileges improperly, granting excessive access rights, protecting information resources, and safeguarding private and sensitive data.

Both production mainframe and disaster recovery operations rely on contractors. Background investigations are required for contractors working with the TSP system. Minimum investigation procedures include a criminal and financial history check. (Prior to the Agency's contract with SI International, the NFC managed the background investigation process and maintained the investigation results on behalf of the Agency.) In addition, the Agency requires contractors holding designated positions to sign non-disclosure agreements, verifying that the contractor understands and agrees to the responsibilities and conditions set forth when handling "proprietary information" and "confidential and sensitive information."

The draft TSP Security Plan contains procedures for identifying reportable incidents, which include system hardware or software changes that occur without prior notice or approval, successful or unsuccessful attempts to gain unauthorized access to the system or system data, unauthorized disclosure of sensitive information, denial of service, and unauthorized use of the system to process or store data.

2. Access Controls (Logical Security and Physical Security)

Logical Security

Logical access configuration on the disaster recovery mainframe is copied from the primary mainframe using data replication tools (see Table 1). At a scheduled time each day, logical access configuration files and datasets are replicated, transferred and stored on the disaster recovery mainframe. The data replication process provides for minimal recovery time for logical access setup and configuration in the event of a disaster. Logical access to the mainframe is protected through the use of Computer Associates (CA) Top Secret Security Management software. CA-Top Secret Accessor IDs (ACIDs) and profiles are used to assign access to the mainframe's resources, which include the TSP system's sensitive files and datasets. While the configuration of logical access files and datasets is replicated to the disaster recovery mainframe via asynchronous, one-way replication, the disaster recovery mainframe logical access is capable of being changed directly by approved Administrators.

ACIDs are categorized in three ways: by person, by started task, or by external agency. In order to obtain an ACID, a candidate must successfully pass a background investigation and have a supervisor, manager or a recognized point of contact with the Agency submit a request via e-mail to the Security Application Team. The Security Application Team forwards the request to the Program Manager or Senior Information Security Officer (SISO) for approval or rejection. Access is granted by the system's Security Administrator based on a user's job role, and assigned on a least privilege basis commensurate with the responsibilities of that job. All access requests are maintained via e-mail history. In order to delete an ACID, a manager or supervisor must submit the request via e-mail to the Security Application Team. ACIDs are removed upon notification by the system's Security Administrator upon an employee's or contractor's separation or transfer from Agency service.

The Security Application Team reviews system-generated audit logs for potentially unauthorized activities or erroneous transactions. The Top Secret Security Utility (TSS UTIL) reports provide the Security Application Team with a listing of every violation and error that occurred on the mainframe. Violations consist of unauthorized attempts to access datasets or execute a command that the ACID does not have the privilege to perform. Errors typically consist of accidental attempts to access unauthorized areas or errors that conflict with global security configuration parameters (i.e., TSS MODIFY STATUS). The Security Administrator reviews the TSS UTIL logs on a daily basis. In addition, ACIDs are reviewed on a semi-annual basis by the SISO in order to determine whether the level of access for the approved ACID is commensurate to the individual's current job responsibilities; inappropriate or excessive access is then changed or revoked.

Logical access to sensitive system files must also be protected to preclude access violations potentially harmful to the TSP system. Just like the mainframe in the RDC, the TSP disaster recovery mainframe has many sensitive datasets that contain configurable settings that, if altered or incorrectly configured, could expose the mainframe and resident files and data to potential risk of corruption or deletion. Access to these sensitive datasets is assigned on a least-privilege basis by the Security Administrator. Full access (i.e., ALL or UPDATE) to these datasets is typically restricted to system programmers and security administrators. Restricted access (i.e., READ) is granted only to those with a need to know.

The following is a partial list[5] of sensitive system datasets on the mainframe for which access should be protected and restricted:

[5] MVS System Data Set Definition, March 2001

- SYS1.PARMLIB - a required partitioned dataset that contains IBM-supplied and installation-created members, which contain lists of system parameter values.
- SYS1.PROCLIB – a required partitioned dataset that contains the source job control language (JCL) used to perform certain system functions. The source JCL can be for system tasks or processing program tasks.
- SYS1.LINKLIB – a required partitioned dataset that contains programs and routines referred to by the XCTL, ATTACH, LINK, and LOAD macro instructions, as well as nonresident system routines. SYS1.LINKLIB also contains the assembler program, the linkage editor, the utility programs, and some service aids.
- SYS1.LPALIB – a required partitioned dataset that contains all the modules loaded into the pageable link pack area (PLPA). Those modules include system routines, service routines, data management access methods, nonresident machine-check handler modules, authorization and accounting exit routines, and logon mode tables.
- SYS1.NUCLEUS – a required partitioned dataset that contains the resident portion of the control program in two members, IEAVEDAT (DAT-off) and IEANUC0x (DAT-on); the nucleus initialization program (NIP); and programs for hardware configuration definition (HCD) used by the initial program load (IPL).
- SYS1.SVCLIB – a required partitioned dataset that contains some online test executive program (OLTEP) and appendage modules.
- SYS1.MACLIB – a required partitioned dataset that contains macro definitions.
- SYS1.MIGLIB – a required partitioned dataset or partitioned dataset extended (PDSE) that is the system load library for the interactive problem control system (IPCS) and all component and subsystem dump exit modules. The component and subsystem dump exits that must function during SNAP processing must also reside in SYS1.LPALIB.
- SYS1.VTAMLIB - an optional partitioned dataset that contains the ACF/VTAM load modules, installation-coded logon exit routines, authorization and accounting exit routines, and unformatted system services (USS) definition tables.

Physical Security

The disaster recovery data center is staffed by two on-site managers from Switch and Data during business hours (i.e., 8:00am to 5:30pm). The perimeter is monitored by security guards who patrol at varied times during their shifts. Motion activated surveillance cameras are monitored remotely by Switch and Data's security operations center located in Tampa, FL. All visitors must sign in and out of a visitor log and be escorted at all times.

Access to the disaster recovery data center in Pittsburgh, PA, is controlled by key card access, also administered by Switch and Data security operations. Should an individual not have a key card badge when entering the facility's primary access point, he or she must produce a Federal government-issued identification to place inside of an inspection device for validation. Once inside the access point, a key card is again required for further access into the actual disaster recovery data center. Additional key card access points exist throughout the center to control access to critical components of the data center's operations (e.g., power closets, Universal Power Supply (UPS), electric switches, and telecommunication switches).

A 10-foot cage surrounds the disaster recovery mainframe, with access restricted by a locked entrance cage door. Only approved Agency and contractors have the lock's key. While the top of the cage is not covered and may allow for the locked cage door to be circumvented, the interior of the data center is monitored by the motion activated video surveillance cameras.

3. System Software

The CA-Top Secret software controls access to sensitive system utilities for the TSP system's hardware and system software (i.e., system utilities, jobs, and routines). The contractor's Operations Manager monitors system software and hardware vendors for releases of changes to system parameters, operating system (OS), and OS-related original equipment manufacturer products. All system software is required to be maintained by schedule, which identifies whether the software remains within one version of the current release. In addition, the Operations Manager is required to notify the Agency when new releases are available, communicate the features and impacts of the new release, and recommend a plan for implementation. The Operations Manager is required to obtain Agency agreement on the timeframe for performing the changes (i.e., scheduled outage time), any impact to operations up-time, and the budget for installing the new release. All changes made to system software are to be tested and executed in scheduled maintenance windows. All changes made to production are to be logged in the system modification program libraries.

The backup mainframe configurations remain consistent with the production mainframe, using the data replication tools to synchronize the system software volumes. For detail related to the data replication tools used, see Section II.C.c.6., Service Continuity.

4. Change Controls

The Agency notes that the TSP system is maintained by a large staff, which includes development and sustaining engineering teams comprised of computer programmers and developers; a group of telecommunications, network, and mainframe support technicians; a quality acceptance (QA) test team; and a software configuration management (CM) team. Changes to TSP software are made following QA and CM procedures, with updated versions of the TSP subsystems being identified, controlled, tracked, and moved to the development, test, and production environments in proper order. In similar fashion, the TSP data is identified, controlled, tracked, and backed up in stages based on the daily processing cycle.

The TSP system software development life cycle (SDLC) tracks the configuration of a software system through design, development, testing, production, and maintenance or sustaining engineering phases using six phases: (1) requirements definition, (2) system design, (3) system development, (4) testing, (5) production, and (6) sustaining engineering. The TSP system is currently in the maintenance-oriented sustaining engineering phase.

Within the sustaining engineering phase, changes in the TSP environment follow an application software change determination process under the guidance of the CM team. This process consists of two parts:

- The identification, documentation, and resolution of application software changes follows a high-level process which involves a cycle of (1) change identification, (2) Problem Report (PR) or Software Change Request (SCR) creation, (3) TSP software project and Configuration Control Board (CCB) notification, (4) CCB change disposition, (5) software development, and (6) bundling of the software into a new version or release.
- The promotion or deployment of application software releases follows a cycle of (1) release notes creation, (2) promotion notification, (3) testing, (4) acceptance, and (5) release promotion or deployment to the production environment, which constitutes a second high-level process. A product of this process is the migration of release source code into PVCS Version Manager (a repository of TSP subsystem release software and documentation).

Simultaneously, the software teams pursue maintenance of the TSP system, which includes support for the daily processing cycle, operation of several other TSP subsystems to support the TSP program (i.e., AdHoc Query Tool, AMI, CFIS, Tax, and TRIS) and support for related software (i.e., OTIS and Miscellaneous Adjustment).

The backup mainframe application changes remain consistent with the production mainframe due to the data replication tools that are used to synchronize the application file volumes. For detail related to the data replication tools used, see Section II.C.c.6., Service Continuity.

5. Segregation of Duties

The draft TSP security policies and procedures require that an individual's supervisor or manager request his/her access to the mainframe. Prior to approval of access, the Program Manager or SISO verifies that the access requested is restricted to a least-privilege basis and only approved to the level required to complete the individual's assigned job duties. Access authorization requires the Program Manager's or SISO's final approval.

The CA-Top Secret Access Control Software controls access to the TSP system resources and provides the technical control capabilities to enforce and govern segregation of duties. Security Administration access is controlled through the use of various administrative files settings. ACIDs are assigned to system resources and functions by their authorized security administrator, who typically works across teams or subcontracts. This separation of security administration duties provides a layer of protection in controlling access to TSP system resources and enforcing segregation of duties.

The security administration files that control security administration access and a description of their capabilities include:

- Master Security Control ACID (MSCA) – Can create all CA-Top Secret administrators, including Central Security Control ACIDs (SCAs), Limited Scope Security Control ACIDs (LSCAs), Department Security Control ACIDs (DCAs), Divisional Security Control ACIDs (VCAs), and auditors.
- SCA – A SCA's scope of authority depends on the administrative authorities that were granted to him. An SCA can create DCAs, VCAs, Profile, and User ACIDs, but not other SCAs.

- LSCA – Can have all of the authority of an SCA, but unlike the SCA, the LSCA must have the scope of authority assigned to it. The scope of authority can be one or more LSCAs and/or zones.
- VCA – A division security administrator can permit access to resources that are owned by his division, and all departments and users within that division, and can define profiles and perform maintenance for ACIDs that are within his scope. A VCA can permit ACIDs in other divisions to access his division's resources, but cannot perform maintenance for ACIDs in other divisions.
- DCA – A department administrator has the same scope over a department that a VCA has over a division.

It is not necessary to directly access the backup mainframe through the use of ACIDs; however, in limited cases, the Agency may warrant direct access to the backup mainframe to perform emergency maintenance. (See Section II.C.c.2., Access Controls, for additional discussion of the controls over logical security.)

6. Service Continuity

Service continuity involves the use of systems and tools for backup and recovery, as well as environmental controls to protect the systems performing these procedures. The TSP system is available 24 hours a day, 7 days a week, excluding any scheduled maintenance. The TSP mainframe production data files are backed up incrementally each day. Incremental backups occur hourly and capture only those changes that occurred since the last backup. A full backup is performed weekly. In addition, all backups performed at the RDC are written to tape and physically retrieved and stored off-site by a vendor in an access-controlled facility.

The disaster recovery data center in Pittsburgh, PA, provides TSP system business continuity for core processing and business-critical TSP systems. For data replication and system backups, the primary data center has a dedicated OC3 line and a dedicated DS3 line between the primary data center and the backup data center through CNT ultranet extenders (i.e., fiber optics). The sites mirror through asynchronous replication performed hourly for the online mainframe updates, nightly for the mainframe batch updates, and continuously for Windows updates. The primary data center only sends changed data to the backup site for the hourly updates to provide only one hour of difference in data updated between the production and backup site. The backup data center and corresponding business continuity procedures have been designed to resume operations within four hours following the declaration of a disaster at the primary data center (i.e., Reston, VA). For additional information regarding the continuity of operations planning, see Section II.C.b., Continuity of Operations Plan.

Several data replication tools ensure that the appropriate data is captured and restored at the backup data center (see Table 1 below). These tools are designed to capture data changes that occur during normal business hours, when system usage is at its highest point, or after the nightly cycle when system usage is minimal. Data changes are sent to the backup data center and will be applied when the site becomes operational. Snapshots of the OmniPlus and server applications data and the DB2 and Oracle databases changes are synchronized to establish a data baseline. When the backup data center is called into service, analysts should be able to determine the application data sync point and the amount of data to recover.

Table 1 Data Replication Tool Functions

Data Replication Tool	**Procedure Description**
DB2 Incremental	During normal business hours, the DB2 database is updated with Agency, FRB, and lockbox transactions, and any updated statement requests and requests for duplicate statements from PSR and IVR that were processed or entered during the day. Hourly, a DB2 incremental backup to DASD is taken, capturing only changes since the last backup. These incremental backups are transferred via file transfer protocol (FTP) to the backup data center and would be available to apply to the full backup if needed.
Rsync	This product is used to replicate the TSP Public Web logs.
FTP	FTP is used as a means of exchanging files between the production data center and the backup data center.
SnapCopy	The SnapCopy utility replicates mainframe files between the production data center and the backup data center. It copies full backups after the nightly unified batch processes and incremental changes that occur to OmniPlus files during normal business hours.
WANSync	This product synchronizes files for Oracle, structured query language (SQL) databases, Windows applications and databases between the production data center and the backup data center.

Data Replication Tool	Procedure Description
Nightly Backups	A nightly backup process copies all IBM mainframe production data files from the production data center mainframe to the backup data center mainframe. This process also copies mainframe data file changes at specific time intervals. The production site performs daily (Monday through Friday) incremental tape backups. Data files that were created and/or modified during the nightly batch processing are applied at the backup data center. This will enable quick startup in the event that the backup data center is called into service.
STK Peer-to-Peer	A backup of the underlying virtual storage access method (VSAM) datasets that contain the DB2 system and user databases is taken using STK's Peer-to-Peer Remote Copy utility after the nightly unified process is completed and DB2 has been stopped. The VSAM files are sent via FTP to the backup data center nightly, and overlay the prior night's VSAM files.

Tape backups of the TSP data are not performed at the backup data center but rather at the mainframe operations site at the RDC. As indicated in Table 1 above, in addition to creating backup tapes, other methods are used to replicate TSP production files from Reston to the mainframes at the backup data center. During our review of the mainframe operations at the RDC[6], we observed backup tapes in the backup tape silo during daily operation and also observed the scheduling of backups being performed via the CA Scheduler tool that corresponds to the backups being performed. The contract with SI provides for a minimum of 7 daily cycles, 6 weekly cycles, and 2 monthly cycles to be maintained with backup media verified being stored off-site within 12 hours of completion. This level of service is to be formally reported to the Agency on a quarterly basis, as written in the contract.[7]

Subsequently, we reported this as an exception in FY 2005 and issued recommendation 2005-1 (see Findings and Recommendations from prior engagements in Section III). In a disaster recovery scenario, as datasets and data volumes are copied via various data replication methods from the production mainframe to the backup data center at various times during the day, all

[6] FY 2005 report "Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005"

[7] We requested the Agency provide evidence supporting monitoring and reporting of SI International's performance against these service-levels to substantiate the completion and off-site storage of the backup media; however, we learned that the Agency has not required SI International to create or maintain such reports.

applications, including mainframe and servers, would synchronize data to a common and distinct point in time in order to determine the application data sync point and the amount of data to recover. Additionally, the Agency would request backup tapes from the off-site storage facility be sent to the backup data center in Pittsburgh, PA to address additional data recovery needs, although backup tapes are not required to address data recovery needs.

Table 2 below depicts the data replication and TSP subsystem component relationship.

Table 2 Data Replication Tools and TSP Subsystem Component Relationships

Application	**Data Replication Tools**					
	DB2 Incremental	**RSync**	**FTP**	**SnapCopy**	**WANSync**	**STK Peer-to-Peer**
TSP Web		X	X			
PSR					X	
CODIS					X	
PowerImage					X	
ThriftLine(IVR)	N/A - This application is not replicating data to the backup data center.					
AMI			X			
CFIS			X			
TRIS					X	
OTIS					X	
Lockbox				X		
API/FRBI	X					X
OmniPlus				X		
Reports, Notices, and Statements	N/A - These applications are not replicating data to the backup data center.					
Accounting					X	
Ad Hoc Database	X				X	

The backup data center is equipped with environmental control systems to protect the backup mainframe from fire, water, temperature, or electrical damage. The following environmental controls were observed throughout the data center:

- The facility's primary access point and data center are monitored through surveillance systems;

- Sensors and systems are set to detect humidity/temperature changes, fire and water;
- A dry-pipe and localized sprinkler system is used for fire suppression inside the data center;
- The mainframe is situated on raised flooring to reduce the risk of flood water damage;
- Fire extinguishers are situated throughout the data center;
- Water detection systems are placed throughout the data center flooring; and
- A UPS protects the mainframe from power surges and power spikes. A backup diesel generator protects the backup mainframe against power outages.

The disaster recovery data center environmental control systems undergo scheduled maintenance throughout the year. This maintenance includes monthly inspections of the generator; quarterly inspections of the power plants, generator, and heating, venting, and air conditioning (HVAC); semi-annual inspection of the UPS and fire protection systems; and annual inspections of the UPS, generator and cleaning of the equipment, and an integrated systems test.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We conducted procedures related to the Thrift Savings Plan (TSP) disaster recovery capabilities at SI International's subcontractor disaster recovery site in Pittsburgh, PA. This special project consisted of testing manual processes, which included interviewing key personnel (Appendix A), reviewing key reports and documentation (Appendix B), and observing selected procedures. Exhibit III-1 summarizes each open recommendation.

We also reviewed certain prior Employee Benefits Security Administration (EBSA) TSP recommendations, identified below, to determine their current status. Section III.B documents the status of prior EBSA recommendations. One prior year recommendation was reported in the "Post-Implementation Review of the New Thrift Savings Plan Recordkeeping System, December 12, 2003," specifically recommendation number 2004-3, related to disaster recovery capabilities and testing the disaster recovery plan. The other three recommendations were reported in "Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, October 7, 2005." Specifically, we reviewed prior year recommendation numbers 2005-1, related to security program policies and procedures, 2005-2, related to logical access to sensitive system datasets and system utilities, and 2005-3, related to configuration management policies and procedures. As discussed in subsection III.B, recommendation number 2004-3 has been partially implemented, closed, and incorporated into 2006 Disaster Recovery Capability recommendation number 2. Recommendation number 2005-1 is partially implemented but remains open, and recommendations 2005-2 and 2005-3 are not implemented and remain open.

The 2006 special project communicates two new fundamental control recommendations related to findings in disaster recovery site risk evaluation and sole source procurement justification, and business continuity planning and service continuity testing, presented in Section III.C. Fundamental control recommendations address significant procedures or processes that have been designed and operated to reduce, to a manageable level, the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Our new recommendations are based upon interviews, inquiries, observations and the data provided in response to our Provided by Client (PBC) documentation request list

Recommendations are numbered sequentially based on the fiscal year of related fieldwork and the name of the applicable report. For example, the first current year recommendation in this report is referred to as 2006 Disaster Recovery Capability Recommendation No. 1. The Federal Retirement Thrift Investment Board's Staff (Agency) should review and consider these recommendations for timely implementation.

Section III.B. documents the status of prior EBSA recommendations. Section III.C presents the current findings and recommendations. Exhibit III-1 (next page) summarizes each open recommendation.

EXHIBIT III-1

SUMMARY OF OPEN RECOMMENDATIONS

2005 Mainframe Operations Recommendations:

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

1. The Agency's Senior Information Security Officer (SISO) should:

   - Update and approve the TSP Security Plan to encompass the breadth of management, operational, and technical controls of the TSP System. This includes leveraging and incorporating the finalized data security standard elements, updated data classification rankings resulting from the most recent risk assessment, and updated incident handling procedures.
   - Update, approve and promulgate security awareness training requirements for contractors, verify that all contractor staff attends security awareness training and attendance is tracked consistent with federal criteria.
   - Perform or require background investigations, commensurate to the level of position sensitivity designated by the job role, for contractor staff that are exposed to Board information or information resources, and retain evidence of investigation completion.
   - Implement service level reporting for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management, consistent with contract requirements.

2. The Agency's SISO should:

   - Document the process for, and report the results of reviewing access rights to global security settings, administrative authorities and sensitive system datasets settings on a semi-annual basis and consistent with account recertification efforts for excessive or inappropriate access permissions. In addition, Accessor IDs (ACIDs) that have been inactive for 180 days must be reviewed and removed if no longer required in the process.
   - Update logical access control policies and procedures, including recertification of accounts on a semi-annual basis and requirements for obtaining, maintaining and controlling access to sensitive system utilities and functions.

EXHIBIT III-1, CONTINUED

SUMMARY OF OPEN RECOMMENDATIONS

2005 Mainframe Operations Recommendations (Continued):

3. The Agency's SISO should document and communicate configuration management procedures to capture and track scheduled or requested changes from authorization through testing and approval for use in the production environment.

2006 Disaster Recovery Capability Recommendations:

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

1. The Agency should conduct a formal recovery site evaluation of risk and strengthen its procurement practices related to sole source selections. A formal risk assessment would identify controls in operation, evaluate potential vulnerabilities with existing controls, and provide a documented basis to make the necessary business decisions either to mitigate or accept known risks, e.g., stacking of undetermined fertilizing agents and access to an underground delivery tunnel. Document vendor justification in accordance with Federal Acquisition Regulations (FAR) and ensure such documentation is produced and maintained in the future. Specifically, Agency management should:

   - Conduct and document a risk assessment of the present disaster recovery site location. The risk assessment should be conducted in accordance with Agency requirements and OMB guidance, including an evaluation of any weaknesses identified at the site. The Agency's assessment should include documentation of the effectiveness of controls and countermeasures in place to manage risk to an acceptable level.
   - Enforce controls over sole source procurement processes, including the retention of documentation that supports the Agency's vendor selection.

2. The Agency should improve its Disaster Recovery and Continuity of Operations Program by updating the required documentation to ensure clear communication and training for a timely recover of operations in an event of a business disruption or disaster. Specifically, we recommend that the Agency:

EXHIBIT III-1, CONTINUED

SUMMARY OF OPEN RECOMMENDATIONS

- Update, finalize, and disseminate all business continuity documentation, (i.e., Business Continuity Plan, Business Assurance Plan, Business Continuity Checklist, and Business Continuity Contact Information), and train the requisite personnel and stakeholders.
- Plan for and complete comprehensive service continuity testing exercising all relevant business continuity components with relevant stakeholders. Also consider administering periodic training and performing a tabletop exercises with the business assurance team members to ensure complete and accurate coverage of the business continuity processes.
- Perform periodic backup tape restoration procedures at the disaster recovery site.

B. Findings and Recommendations from Prior Reviews

Findings and recommendations from the EBSA's prior reviews that required follow-up are presented in this section. The discussion below includes the current status of each recommendation through March. In addition, we have also included Agency representations as of September 2006 that we have not verified.[8]

2004 Post-Implementation Review Recommendation No. 3:

Original Recommendation: To ensure that the new TSP System can be recovered, and that the capabilities and recovery time requirements are sufficient to meet the needs of a daily-valued recordkeeping system, the Agency should:

- Consider alternative recovery strategies and capabilities for a 24-hour recovery. Traditional recovery procedures, whereby a system is down for up to 48 hours while the back up tapes are shipped to an alternative recovery site for restoration, are no longer an acceptable length of time to restore operations. Alternatives should consider the cost versus benefit of parallel and/or mirrored processing in a replicated environment and the impact on traditional data back-ups and recovery procedures.
- Ensure that the disaster recovery procedures for the TSP mainframe and supporting infrastructure are developed, maintained, and updated periodically, based on routine testing.

Reason for Recommendation: As part of the United States Department of Agriculture National Finance Center's (NFC) Disaster Recovery Plan (DRP), procedures exist to recover only the TSP's mainframe system, which hosts the core OmniPlus application. The NFC tests the DRP twice a year with a 48-hour recovery goal. In August 2003, the recovery test was limited to restoring the TSP mainframe system. In addition, no end user testing was performed. Finally, the Agency has determined that a 24-hour recovery time is needed for the new system.

[8] Our assessment of certain information obtained through October 3, 2006, but related to the period of review has been incorporated into this report. In addition, certain management representations have been provided and are incorporated as necessary. Management's representations were not verified as part of our review.

March 2006 Status:

Partially Implemented.

The Agency has established a disaster recovery site location in Pittsburgh, PA. The disaster recovery site is considered the backup data center and provides recovery capability. To the extent tested by the Agency, the backup host and servers are available and ready to operate when communications are redirected to Pittsburgh as the primary site. Disaster recovery procedures have been designed to resume operations within a 24-hour period (i.e., a Recovery Time Objective (RTO) of 4 hours and a Recovery Point Objective (RPO) of 1 hour have been established). Also, while the most recent disaster recovery testing consisted of bringing up the disaster recovery mainframe, testing application interface, batch processing and reporting, all business continuity/disaster recovery planning documentation remains in draft status.

Disposition: **Recommendation Closed.** Although certain disaster recovery testing of the mainframe and application usage has occurred, comprehensive testing is planned but has not yet occurred. In addition, business continuity procedures have not been finalized and remain in draft status (see 2006 Disaster Recovery Capability Recommendation No. 2, related to Business Continuity Planning).

2005 Mainframe Operations Review Recommendation No. 1:

Original Recommendation: The Agency's Senior Information Security Officer (SISO) should:

- Update and approve the TSP Security Plan to encompass the breadth of management, operational, and technical controls of the TSP System. This includes leveraging and incorporating the finalized data security standard elements, updated data classification rankings resulting from the most recent risk assessment, and updated incident handling procedures.
- Update, approve and promulgate security awareness training requirements for contractors, verify that all contractor staff attends security awareness training and attendance is tracked consistent with federal criteria.

- Perform or require background investigations, commensurate to the level of position sensitivity designated by the job role, for contractor staff that are exposed to Agency information or information resources, and retain evidence of investigation completion.
- Implement service level reporting for mainframe system availability, online transaction response time, contractor software management, configuration management/quality assurance, backup and recovery, data recovery, security management and storage management, consistent with contract requirements.

Reason for Recommendation:

The Agency's prior SISO retired in July 2005 and a new SISO was appointed in August 2005. The TSP System has been in a state of change since June 2003. The new daily-valued TSP System was implemented, the OS/390 IBM mainframe was transitioned to a zOS IBM mainframe and the mainframe operations and disaster recovery locations were transferred to new sites. More recently, TSP operations at the NFC in New Orleans were severely impacted by Hurricane Katrina, requiring continuity of operations plans to be initiated and managed until operations had stabilized. This emergency required additional time and resource commitment by the Agency and its contractor staff.

March 2006 Status:

Partially Implemented.

The TSP Security Plan remains in draft status and does not contain a comprehensive list of management, technical and operational controls that are planned or in place, consistent with Office of Management and Budget (OMB) Circular No. A-130 requirements and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 guidance. Specifically, the plan does not contain controls related to Rules of the System, Authorize Processing, Environmental Controls, and Data Integrity/Validation. In addition, the TSP system's data classification risk rankings for confidentiality and integrity have not been updated from moderate to high based on the results of the most recent risk assessment performed in May 2005.

While contractor staff perform the majority of TSP mainframe hosting and operations functions, security awareness training is currently not administered to contractor staff. A security awareness training plan for contractors has been developed but remains in draft status.

Evidence of completed background investigations and non-disclosure agreements for two contractors selected was not provided.

In addition, we were not provided with evidence that mainframe service level reporting has been implemented.

September 2006 Status: With regard to security awareness training, the Agency communicated that it has procured an IT Security awareness training program in 2006, and all personnel accessing FRTIB systems are required to take, and pass (It is graded) the training. In fact, the Agency represented as of August 30, 2006, 81.01% (of 474 required) had taken and passed the training. The Agency has also represented that they now have a process in place to perform background investigations.

With regard to background investigations for the two selected contractors during this review, (i.e., one contractor from Switch and Data and one contractor from SI International), the Agency represented that they do not require Switch and Data employees to have background investigations performed. For the SI International employee, the investigation was handled by the prior incumbent contractor (i.e., NFC). However, during subsequent testing of this process during FY2006 at SI's call center in Clintwood VA, we selected and obtained evidence of 8 completed background investigations.

Disposition: **Recommendation Open.**

2005 Mainframe Operations Review Recommendation No. 2:

Original Recommendation:	The Agency's SISO should: • Document the process for and report the results of reviewing access rights to global security settings, administrative authorities and sensitive system datasets settings on a semi-annual basis and consistent with account recertification efforts for excessive or inappropriate access permissions. In addition, ACIDs that have been inactive for 180 days must be reviewed and removed if no longer required. • Update logical access control policies and procedures to include recertification of accounts on a semi-annual basis and requirements for obtaining, maintaining and controlling access to sensitive system utilities and functions.
Reason for Recommendation:	Mainframe operations and hosting were transferred from the NFC to SI International in September 2004. The current contractor has assumed the historical mainframe settings and configurations.
March 2006 Status:	**Not Implemented.** Because of the data replication process, the disaster recovery system inherits ACID logical access permission settings. In our 2005 post-implementation review of the production mainframe operations, we identified inappropriate ACID access to the CA-Top Secret security administration functions. During our current fieldwork, we identified an excessive number of ACIDs that had "ALL" or "UPDATE" access to the SYS1 sensitive datasets. According to the Agency, the ACID permissions were inherited from the NFC. Since SI International assumed the CA-Top Secret access control responsibilities, individuals are only granted the access needed to perform their work with approval. The Agency has communicated that a plan is being developed to identify and correct any excessive access and inappropriate privileges granted to individuals.

September 2006 Status:

The Agency represented that in recognition of the need to increase focus on security and business continuity, the Director of Automated Systems has reassigned a member of the staff to serve as the Agency's primary information technology security specialist and focus solely on those issues. In addition, the duties and responsibilities of this position encompass the breadth and depth of security and business continuity activities, training, documentation, and ensuring compliance with all applicable directives.

Disposition: **Recommendation Open.**

2005 Mainframe Operations Review Recommendation No. 3:

Original Recommendation:

The Agency's SISO should document and communicate configuration management procedures to capture and track scheduled or requested changes from authorization through testing and approval for use in the production environment.

Reason for Recommendation:

Mainframe operations were transferred from the NFC to SI International in June 2005. Since the transfer, Agency priorities have been focused on stabilizing system operations at the new contractor location.

March 2006 Status:

Not Implemented.

The Agency has not established a configuration management process to formally capture and track authorized changes and deviations from the baseline configuration, which include scheduled maintenance changes. In addition, during our current fieldwork, we requested a list of changes made to the OmniPlus recordkeeping software and the system software changes made to the backup system. A list of changes to the OmniPlus recordkeeping software was not provided, and the list of changes made to system software was incomplete as it only included informal change log notes through November 2005.

September 2006 Status: The Agency represented that e-mails have been used for scheduled outages to update system software and network changes. In addition, the Agency is in the process of implementing a comprehensive configuration management process utilizing Serena COTS products.

Disposition: **Recommendation Open.**

C. 2006 Findings and Recommendations

Our 2006 fieldwork identified two new findings and communicates related fundamental control recommendations. The EBSA requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

<u>Documentation Supporting the Evaluation of Risk and Cost to Justify the Selection of the Disaster Recovery Site</u>

Documents supporting a site evaluation of risk and the procurement basis for sole source selection do not exist. Although Agency management represents that a recovery site evaluation was performed, a documented and formal risk assessment over the TSP's disaster recovery facility does not exist. Based on our observations, we noted these site specific access weaknesses:

- A commercial truck delivery tunnel, serving multiple businesses, runs directly beneath the floor of the TSP disaster recovery site. A Switch and Data employee communicated that access to the tunnel should be controlled by the facility's management (Allegheny Center Associates) security guard and badge system, but the Switch and Data employee could not determine who was responsible for managing this access and to what degree security was maintained. Trucks can and do enter and unload freight in immediate proximity to the TSP disaster recovery site.

- We observed approximately *fifty* stacked bags of an undetermined fertilizing agent. These stacks abutted a wall of the disaster recovery site data center in a common hallway accessed and used by multiple businesses. During our on-site review at the Pittsburgh, PA disaster recovery site, no explanation was provided as to why the undetermined fertilizing agent was in such proximity to the TSP disaster recovery site, to whom it belonged, or how and when it arrived. Upon further discussion, the Agency's subcontractor, Switch and Data, confirmed that property manager uses the hallway as a make-shift trucked freight storage area. While we did not note the type of fertilizer in the bags cited above, the Agency has represented that urea, a fertilizing agent that the Chief Information officer (CIO) understands also has non-corrosive de-icing properties, would typically have been stored in the common hallway area against the wall of the disaster recovery data center. The Agency represents,, but we have not observed, that these bags have been subsequently removed.

As for the procurement basis for sole sourcing SI International to secure a disaster recovery site for TSP, we are unable to ascertain how Agency management evaluated the cost, value and capabilities to meet recovery requirements and sourcing alternatives that lead to supporting a decision to sole-source, based on the need to recover within 24 hours. Lastly, there is no formal contract in place between the Agency and SI International containing the add-on, sole-source work.

The Agency considered SI International to be the sole source provider of disaster recovery services as follow-on work to its existing data center operations contract (i.e., production operations in Reston, VA). However, the Agency made the decision to sole-source disaster recovery services to SI International without visiting the proposed disaster recovery site first and performing a formal risk assessment of that site and represents that a site risk inspection walkthrough, in lieu of a formal risk assessment, was performed. In addition, the Agency represented that contracting with another vendor for operation of the disaster recovery site would require additional staff and expenses that could be somewhat alleviated by using existing SI International operations; however, it performed no documented cost justification.

According to *Office of Management and Budget (OMB) Circular No. A-130 Appendix III, section B* states that the scope of a risk assessment "... should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." As for procuring services and documenting the basis, the *Federal Acquisition Regulation (FAR) 6.303-2 Content (a)* states that: "Each justification (for sole source contracting) shall contain sufficient facts and rationale to justify the use of the specific authority cited. As a minimum, each justification shall include the following information: (8) A description of the market research conducted and the results or a statement of the reason market research was not conducted; and (9) Any other facts supporting the use of other than full and open competition, such as: (ii) When 6.302-1 is cited for follow-on acquisitions as described in 6-302-1(a)(2)(ii), an estimate of the cost to the Government that would be duplicated and how the estimate was derived." Furthermore, *the FAR subpart 4.803 Contents of Contract Files* states that "... examples of records normally contained in contract files, if applicable...(b)(4) Cost or pricing data, Certificates of Current Cost of Pricing Data, or information other than cost or pricing data; cost or pricing analysis; and other documentation supporting contractual actions executed by the contract administration office."

1. **The Agency should conduct a formal recovery site evaluation of risk and strengthen its procurement practices related to sole source selections. A formal risk assessment would identify controls in operation, evaluate potential vulnerabilities with existing controls, and provide a documented basis to make the necessary business decisions either to mitigate or accept known risks, e.g., stacking of commercial fertilizing agents and access to an underground delivery tunnel. Document vendor justification in accordance with Federal Acquisition Regulations (FAR) and ensure such documentation is produced and maintained in the future. Specifically, Agency management should:**

    - **Conduct and document a risk assessment of the present disaster recovery site location. The risk assessment should be conducted in accordance with Agency requirements and OMB guidance, including an evaluation of any weaknesses identified at the site. The Agency's assessment should include documentation of the effectiveness of controls and countermeasures in place to manage risk to an acceptable level.**
    - **Enforce controls over sole source procurement processes, including the retention of documentation that supports the Agency's vendor selection.**

Without completing a thoroughly documented risk assessment of the TSP disaster recovery site, the Agency is not fully able to report to the TSP fiduciaries (i.e., Board members and the Agency's Executive Director) whether potential risks associated with establishing the TSP's disaster recovery site operations at its current location are acceptable. Also, without the Agency's performing adequate market research justifying the cost estimate used to sole source add-on services for the current disaster recovery site operations contract, the Agency is not fully able to report to the TSP fiduciaries the cost effectiveness of this use of TSP assets on behalf of TSP participants.

<u>Incomplete Documentation and Testing to Support a Comprehensive Continuity of Operations Program</u>

Although the Agency demonstrated its ability to recover operations resulting from Hurricane Katrina in 2004, improvements to its program and specifically to the supporting documentation is needed. Based on our review of TSP Business Assurance and Continuity Plan, the plan is incomplete and still requires finalizing as a base-lined, but living, document. For example, the plan does not clearly state the line of succession, outlining the decision-making responsibilities during contingency situations. In addition, the supporting checklists, listing of hardware and software vendor contacts, and referenced test plan are incomplete, or do not exist.

In addition, the following exceptions were noted:

- Due to competing priorities, the extent of management planned testing of TSP Business Assurance and Continuity Plan has not been fully completed.
- A process for recovering Omnicash daily entries is not documented. During the February 23 and 24, 2006, disaster recovery testing, Omnicash transactions were unaccounted for several days following the test.[9]
- Evidence that the Agency has been able to restore operations from back up tapes and that scheduled hardware maintenance at the back up site was performed in January 2006 could not be provided.

National Institute of Standards and Technology (NIST) Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, p. 5 states, "In order for contingency planning to be successful, agency management must ensure the following: 1) Understand the IT Contingency Planning Process and its place within the overall Continuity of Operations Plan and Business Continuity Plan process; 2) Develop or reexamine their contingency policy and planning process and apply the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection, and recovery strategies." In addition, p. 20 states, "The Contingency Planning Coordinator should test the backup tapes at the alternate site, to ensure that the site supports the same backup configuration that the organization has implemented."

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, p. 130 states, "The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities." In addition, "All

[9] In September 19, 2006, the Agency represented that this process was added to the documented procedures [See TSP Business Continuity Plan (Reston Data Center) TSP-PL008-c Version 1.3]. We have not verified this information.

personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills. Training is particularly important for effective employee response during emergencies. There is no time to check a manual to determine correct procedures if there is a fire. Depending on the nature of the emergency, there may or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved."

Agency personnel and contractor staff have been handling multiple, competing priorities. Thus the completion of business continuity planning activities has been delayed but continues to be refined. While the primary control for alternate site recovery is based on peer to peer replication, the Agency has represented that it will adopt a practice of periodically testing its ability to restore [illegible] its secondary back up tapes.

2. **The Agency should improve its Disaster Recovery and Continuity of Operations Program by updating the required documentation to ensure clear communication and training for a timely recover of operations in the event of business disruption or a disaster. Specifically, we recommend that the Agency:**

   - **Update, finalize, and disseminate all business continuity documentation, (i.e., Business Continuity Plan, Business Assurance Plan, Business Continuity Checklist, and Business Continuity Contact Information), and train the requisite personnel and stakeholders.**
   - **Plan for and complete comprehensive service continuity testing exercising all relevant business continuity components with relevant stakeholders. Also consider administering periodic training and performing a tabletop exercises with the business assurance team members to ensure complete and accurate coverage of the business continuity processes.**
   - **Perform periodic backup tape restoration procedures at the disaster recovery site.**

Without final, approved business continuity documentation and completed service continuity testing, the TSP's fiduciaries ability to safeguard TSP participants from lost data and disrupted service and to provide orderly and efficient resumption of operations in the event of an actual disaster may be at risk.

APPENDIX A

KEY PERSONNEL INTERVIEWED

While performing fieldwork, we inquired of the following personnel regarding disaster recovery capabilities and general control environment:

A. SI International

Patrick Rouse	CA-Top Secret Security Administrator
Glenn Meyers	Data Center Operations Manager
Merritt Poole	Assistant Program Manager
Bill Smithson	VP Financial Systems

B. Switch and Data

Sam Zurzola	Operations Manager

C. Jacob and Sundstrom

Doug Aronson	Computer Operator
Adrienne Stup	Computer Operator

D. Federal Retirement Thrift Investment Board - Agency Staff

Mark Hagerty	Chief Information Officer
Mark Allen	IT Specialist and Board Continuity of Operations Planning (COOP) Coordinator

KEY DOCUMENTATION REVIEWED

Post-Implementation Review of the New Thrift Savings Plan Recordkeeping System, Employee Benefits Security Administration, December 12, 2003

Post-Implementation Review of the Thrift Savings Plan Mainframe Operations, Employee Benefits Security Administration, October 7, 2005

Security policy and procedure documentation

- Disaster recovery operations memorandum
- TSP system security plan (draft)
- FRTIB background investigation review
- FRTIB non-disclosure agreement example

Logical access control documentation

- TSP security policies and procedures for disaster recovery
- Switch and Data facility sign-in log
- List of approved individuals with physical access to the backup mainframe
- System-generated list of personnel with access to the backup facility
- CA-Top Secret files for production mainframe (Reston)
- CA-Top Secret files for the backup mainframe (Pittsburgh), TSS MODIFY STATUS report for the backup mainframe)

System software documentation

- ZHIST list of changes to system software (excerpt)

Service continuity documentation

- Site maintenance schedule for 2006)
- Continuity of Operations Planning (COOP) documentation
- Business continuity test schedule
- Business continuity test support documentation for completion of tasks
- TSP business continuity plan (draft)
- TSP business continuity plan appendix A, TSP contact information
- TSP business continuity plan appendix B and related documents
- TSP business continuity plan appendix C
- TSP checklists
- TSP business assurance plan (draft)

ENTRANCE AND EXIT CONFERENCE ATTENDEES

An overall entrance conference was held at the Agency on January 12, 2006, to discuss the nature, scope, and timing of the fiscal year 2006 EBSA review of the Thrift Savings Plan, including the special project on disaster recovery capability at the disaster recovery site location.

Attendees were:

A. Federal Retirement Thrift Investment Board - Agency Staff

Mark Hagerty	Chief Information Officer
James Petrick	Chief Financial Officer
Pamela-Jeanne Moran	Director, Office of Participant Services

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance

C. KPMG LLP

Heather Flanagan	Partner
Felipe Alonso	Partner
Derek Thomas	Manager
Gregory Ruck	Computer Systems Analyst

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

An entrance conference was held at the Agency on January 31, 2006, to discuss the nature, scope, and timing of the fiscal year 2006 EBSA special project on disaster recovery capability at the disaster recovery site location.

Attendees were:

A. Federal Retirement Thrift Investment Board - Agency Staff

Mark Hagerty	Chief Information Officer
Mark Allen	IT Specialist and FRTIB COOP Coordinator
Leonard Dillard	Manager, ADP Systems

B. KPMG LLP

Gregory Ruck	Computer System Analyst
Mark Munster	Computer System Analyst
Kristine Saliendra	Junior Computer System Analyst
Evans Bannor	Junior Computer System Analyst

ENTRANCE AND EXIT CONFERENCE ATTENDEES, CONTINUED

An exit conference was held on October 3, 2006 with the Agency. Attendees were as follows:

A. Federal Retirement Thrift Investment Board – Agency Staff

Jim Petrick	Chief Financial Officer
Mark Hagerty	Chief Information Officer
Mark Allen	IT Security Specialist
Anne Beemer	Senior Financial Manager, Office of Benefit Services
Carla Steiger	Accountant

B. Department of Labor, Employee Benefits Security Administration

William Bailey	Senior Auditor, FERSA Compliance

C. KPMG LLP

Heather Flanagan	Partner
Don Farineau	Partner
Derek Thomas	Senior Manager
Mark Munster	Computer System Analyst