Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Participant Website

May 12, 2016

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Members of the Federal Retirement Thrift Investment Board
Washington, D.C.

Ian Dingwall
Chief Accountant
U.S. Department of Labor, Employee Benefit Security Administration
Washington, D.C.

As part of the U.S. Department of Labor Employee Benefits Security Administration (EBSA) Fiduciary Oversight Program, we conducted a performance audit of the Thrift Savings Plan (TSP) participant website. Our fieldwork was performed from December 1, 2015 through January 29, 2016 primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was January 1, 2015 through December 31, 2015.

We conducted this performance audit in accordance with the performance audit standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and the American Institute of Certified Public Accountants *Standards for Consulting Services*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate audit evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives. Criteria used for this audit is defined in the EBSA's *Thrift Savings Plan Fiduciary Oversight Program*, which includes the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

The objectives of our audit over the Agency's TSP participant website were to:

- Determine whether the Agency implemented certain procedures related to (1) altering and resetting TSP participant passwords; (2) monitoring threats on participant data from external sources; and (3) securing participant communications and transactions.

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of Thrift Savings Plan Participant Website as of March 20, 2014*.

We present seven new recommendations, six addressing fundamental controls and one addressing other controls. Fundamental control recommendations address significant procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Other control recommendations address procedures or processes that are less significant than fundamental controls. All recommendations are intended to strengthen the TSP participant website process. The Agency should review and consider these recommendations for timely implementation. Section III.C presents the details that support the current year findings and recommendations.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2015 through December 31, 2015, the Agency implemented certain procedures related to (1) altering and resetting TSP participant passwords; (2) monitoring threats on participant data from external sources; and (3) securing participant communications and transactions. However, during the scope period, an outage occurred on the TSP.gov website impacting availability, and as of the date of this report, the Agency had not completed a comprehensive root cause analysis. Additionally, as indicated above, we noted other internal control weaknesses in certain areas that could adversely affect the TSP participant website process.

We also reviewed three prior EBSA recommendations related to the TSP participant website to determine their current status. Section III.B documents the status of these prior recommendations. In summary, all three of the recommendations have been implemented and closed.

The Agency's responses to the recommendations, including the Executive Director's formal reply, are included as an appendix within the report (Appendix A). The Agency concurred with all recommendations, except for the use of ten character temporary passwords on the MyAccount website discussed in Recommendation No. 2015-5a. We noted that the use of an eight-character password does not comply with the Agency's website password requirements. Additionally, although the Agency indicated compensating controls exist, evidence of them was not provided.

This performance audit did not constitute an audit of the TSP's financial statements in accordance with *Government Auditing Standards.* KPMG was not engaged to, and did not render an opinion on the Agency's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of this audit to future periods is subject to the risks that

controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

While we understand that this report may be used to make the results of our performance audit available to the public in accordance with *Government Auditing Standards*, this report is intended for the information and use of the U.S. Department of Labor Employee Benefit Security Administration, Members of the Federal Retirement Thrift Investment Board, and Agency management. The report is not intended to be, and should not be, used by anyone other than these specified parties.

KPMG LLP

May 12, 2016

I. BACKGROUND OF THE TSP AND PARTICIPANT WEBSITE

A. The Thrift Savings Plan

Public Law 99-335, the Federal Employees' Retirement System Act of 1986 (FERSA), as amended, established the Thrift Savings Plan (TSP). The TSP is the basic component of the Federal Employees' Retirement System (FERS) and provides a Federal (and, in certain cases, State) income tax deferral on employee contributions and related earnings. The TSP is available to Federal and Postal employees, members of the uniformed services, and members of Congress and certain Congressional employees. The TSP began accepting contributions on April 1, 1987, and as of November 30 2015, had approximately $463 billion in assets and approximately 4.8 million participants[1].

The FERSA established the Federal Retirement Thrift Investment Board (FRTIB or the Board) and the position of Executive Director. The Executive Director manages the TSP for its participants and beneficiaries. The Board's Staff (Agency) is responsible for administering TSP operations.

B. Overview of the TSP Participant Website

The Agency utilizes the FRTIB website (FRTIB.gov) to publish general information about the Board and the Agency and the TSP website (TSP.gov) to support participant communication, participant account management, and participant transactions processed by payroll offices.

1. FRTIB.gov Website – Functional Design[2]

The FRTIB.gov website publishes general information about the Board's fiduciary activities, the Agency, and the TSP itself. This website resides on the Linux operating system.

At the perimeter of the TSP architecture, firewall devices provide initial security measures and control access to the public-facing network elements while routers are in place to control the flow of information to web-available network services. The FRTIB.gov website resides inside the TSP

[1] Source: Minutes of the December 14, 2015, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

[2] Source: Various internal Agency policies and procedures developed or modified in 2014 and 2015 related to the subject matter of the audit.

perimeter (i.e., behind firewall devices) and is available to web sessions and users through a proxy server, which provides additional security measures. Internal network services run anti-virus and other software protection checks to reduce the risk of threats to the TSP system.

2. TSP.gov Website – Functional Design[3]

a. TSP.gov - Public Website

The TSP public website provides the main entry point for the TSP web system to participants. The public site maintains a repository of TSP forms, publications, and retirement planning information for each of the funds in the TSP fund portfolio as well as information and links for federal agency and uniformed services payroll representatives. The TSP.gov public website utilizes a MySQL-High Availability (HA) database for share price history and performance metrics of the TSP funds, factor tables for TSP retirement planning tools, and storage of participant feedback comments.

b. TSP.gov Secure Website – "My Account" Link

The "My Account" link of the TSP.gov website allows active, separated, and beneficiary participants to log into their TSP account using their account number or unique user ID and associated password to view account information and perform transactions. Participants can view balances, review recent activity, review statements, update contribution allocations, request interfund transfers, request loans and withdrawals, and update profile preferences. To establish account access, participants initially log into "My Account" by entering their account number using a temporary password, which previously was mailed to their mailing address on file; once logged into the site, the participant is required to create a ten-character password that meets certain complexity rules. The participant also has the option to create a user ID for all subsequent logins.

Each "My Account" session is established within an encrypted connection. To secure transmissions, the Agency uses a current web-based security protocol. For each request, the session key is checked and validated to determine if the request was sent from valid source.

Web requests from the "My Account" link are received by the web proxy server application and forwarded to the web application server for request processing. Each request from login to logout is expected to be analyzed and validated by the web proxy server prior to forwarding to the web

[3] Source: Functional Design Document, dated January 23, 2014

application server. The system is designed so that financial participant transactions are recorded by the proxy application in an audit log and that these audit logs are stored in the MySQL-HA database maintained in the production data center in Virginia.

c. TSP.gov-Secure Website "Web-Based Data Submission (DSUB)" Link and System

The DSUB link of the TSP.gov website allows authorized Federal and uniformed services payroll agencies (payroll agencies) to submit secured payroll information to the TSP. To access and perform specific tasks in DSUB, Federal and uniformed services officers (payroll officers) must request a digital identification certificate from the TSP. Payroll agencies can submit TSP applications (TSP Form OC05-6 and TSP Form OC06-06) on behalf of payroll officers for three types of digital identification certificates:

- Data entry certificates – these allow authorized payroll officers to submit traditional and Roth payroll contributions and request and receive associated reports;
- Certify only certificates - these allow the authorized certifying official at the agency to submit traditional and Roth journal vouchers and request and receive reports; and
- Certify entry certificates – these allow authorized payroll officers to submit traditional and Roth file data and associated journal vouchers and request and receive reports.

Payroll agencies are responsible for assigning and controlling payroll certificates in their payroll offices. The payroll agency must submit the appropriate TSP application form, including signatures and a copy of two forms of identification to TSP for review, approval, and processing. Once the TSP reviews the application for correct information and signatures, the application is approved and sent to the TSP applications security team for processing by the contracted digital credential provider. The TSP applications security team establishes the payroll officer's initial profile at the contracted digital credential provider. The provider then sends to the payroll officer a PIN and instructions on completing and obtaining the web certificate.

Once authorized and enrolled, payroll representatives can use that digital signing certificate to submit electronic journal vouchers, participant transactions, and account updates to the TSP via the DSUB link on the TSP.gov website. The journal vouchers authorize specific events such as contributions, withdrawals, loan payments, and indicative data record updates (e.g., name, address, age, and bank information) for associated TSP participant accounts.

d. TSP.gov-Secure Website – Agency Payroll Interface (API)

Once journal vouchers are submitted via the DSUB link, the transactions are sent to the Agency Payroll Interface (API) system. The API system serves as the interface between the Federal government's agency payroll systems and TSP. Journal vouchers submitted are placed in a "wait" status until the system receives a corresponding participant data file. The API system receives data files from payroll agencies via DSUB's electronic submission process, web entry, or file transfer protocol. The API system validates the transactions from payroll offices by matching submitted journal vouchers with summary information from the received data files, which may include participant transactions. The system rejects a transaction when participant data submissions cannot be matched with participant journal vouchers. Successfully matched transactions are then sent to the OmniPlus recordkeeping system for the nightly processing and updating of the participants' accounts.

II. OBJECTIVE, SCOPE AND METHODOLOGY

A. Objectives

The U.S. Department of Labor Employee Benefits Security Administration (EBSA) engaged KPMG LLP (KPMG) to conduct a performance audit of the Thrift Savings Plan (TSP) participant website.

The objectives of our performance audit were to:

- Determine whether the Federal Retirement Thrift Investment Board's Staff (Agency) implemented certain procedures related to (1) altering and resetting TSP passwords; (2) monitoring threats on participant data from external sources; and (3) securing participant communications and transactions.

- Determine the status of the prior EBSA TSP open recommendations reported in *Performance Audit of Thrift Savings Plan Participant Website as of March 20, 2014*.

B. Scope and Methodology

We conducted this performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and the American Institute of Certified Public Accountants *Standards for Consulting Services*, using EBSA's *Thrift Savings Plan Fiduciary Oversight Program*. Our scope period for testing was January 1, 2015 through December 31, 2015. We performed the audit in four phases: (1) planning, (2) arranging for the engagement with the Agency, (3) testing and interviewing, and (4) report writing.

The planning phase was designed to assist team members to develop a collective understanding of the activities and controls associated with the applications, processes, and personnel involved with the TSP participant website. 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 auditee-provided documentation and evidence, participated in process walk-throughs, and

designed and performed tests of controls and compliance[4]. These procedures included the following:

- Inspected and tested procedures that established the participant website access control process;
- Inspected and tested process for participant communications via the TSP.gov and FRTIB.gov websites;
- Inspected and tested process for monitoring unauthorized attempts on the TSP.gov website;
- Inspected the policies that documented TSP.gov and FRTIB.gov website browser and Federal website requirements and settings, and inquired of and observed activities based on those policies and requirements;
- Inspected applicable contracts and procedures for acquisitions with third-party applications;
- Inspected and tested a non-statistical sample of system edit checks on the TSP.gov website for evidence of configuration and access controls; and
- Inspected and tested a non-statistical sample of web content change on the TSP.gov and FRTIB.gov websites for evidence of approval prior to migration into production.

We conducted these test procedures at the Agency's headquarters in Washington D.C. In Appendix B, we identify the key documentation provided by Agency and contractor personnel that we reviewed during the performance audit.

Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the sample items we tested and were not extrapolated to the population.

The report writing phase entailed drafting a preliminary report, conducting an exit conference, providing a formal draft report to the Agency for comment, and preparing and issuing the final report.

[4] We obtained and utilized certain information technology system settings related to the participant website process subsequent to the scope period and in a test environment due to timing and availability. While we could not validate independently that the MyAccount password controls tested were in place during the entire audit period, the Agency represented that such edit checks and settings were functionally and technically the same as those designed and operating in production environment from January 1, 2015 through December 31, 2015.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We performed procedures related to the Thrift Savings Plan (TSP) participant website controls while conducting a performance audit at the Federal Retirement Thrift Investment Board's (FRTIB) Staff (Agency) headquarters. Our scope period for testing was January 1, 2015 through December 31, 2015. This performance audit consisted of reviewing applicable policies and procedures and testing manual and automated processes and controls, which included interviewing key personnel, reviewing key reports and documentation (Appendix B), and observing selected procedures.

Based upon the performance audit procedures conducted and the results obtained, we have met our audit objectives. We conclude that for the period January 1, 2015 through December 31, 2015, the Agency implemented certain procedures related to (1) altering and resetting TSP participant passwords; (2) monitoring threats on participant data from external sources; and (3) securing participant communications and transactions. However, we noted internal control weaknesses in certain areas that could adversely affect the TSP participant website controls.

We present seven new recommendations, presented in Section III.C, related to TSP participant website controls, six addressing fundamental controls and one addressing other controls. Fundamental control recommendations address significant procedures or processes that have been designed and operate to reduce the risk that material intentional or unintentional processing errors could occur without timely detection or that assets are inadequately safeguarded against loss. Other control recommendations address procedures or processes that are less significant than fundamental controls. The Agency should review and consider these recommendations for timely implementation. The Agency's responses to these recommendations are included as an appendix within this report (Appendix A).

We also reviewed three prior U.S. Department of Labor Employee Benefits Security Administration (EBSA) recommendations related to the TSP participant website controls to determine their current status. Section III.B documents the status of these prior recommendations. In summary, all three recommendations have been implemented and closed.

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

B. Findings and Recommendations from Prior Reports

The findings and recommendations from prior reports that required follow-up are presented in this section. The discussion below includes the current status of each recommendation.

2013 Participant Website Recommendation No. 1:

Title:	Weaknesses in Website Incident and Monitoring Procedures
Original Recommendation:	To strengthen website incident and monitoring activities, the Agency should fully develop, document, and enforce procedures for website monitoring activities in accordance with Agency policy requirements.
Reason for Recommendation:	The Security Operation Center (SOC) became operational in June 2013, and the Agency developed SOC User Guides in late July 2013 and an ad hoc process for recording and mitigating actions on website alerts. However, the Agency lacked written procedures that define roles, responsibilities, and extent of website monitoring required.
Status:	**Implemented.** We obtained and inspected the *Technology Enterprise Support Services (TESS) Security Operations Analyst Runbook*, dated September 25, 2015, and noted that the document included procedures for addressing web monitoring investigations. Additionally, we obtained and inspected the *TESS Computer Security Incident Response Team (CSIRT) Incident Response Plan*, dated May 28, 2015, and noted the plan included responsibilities and monitoring activities to be performed by Intrusion Analysts. These activities consisted of analyzing alerts/reports generated by Agency-owned security sensors (e.g., Intrusion Detection System/Intrusion Prevention System, anti-virus, firewalls, and web gateways). To determine if website monitoring activities were being enforced, we obtained the *TSP Websites and Web Server Daily Monitoring Report* for December 15, 2015, and noted the report included monitoring details for TSP and FRTIB public sites and My Account (secure site).

Disposition: **Recommendation Closed.**

2013 Participant Website Recommendation No. 2:

Title: Security Weaknesses in Participant Electronic Communications

Original Recommendation: To strengthen controls over participant electronic communications, the Agency should:

a) Fully develop, document, and enforce procedures for protecting and transmitting sensitive data in electronic communications; and

b) Properly test Secure Message Center[5] email configurations prior to implementation to validate that participant electronic inquiries and responses are securely maintained.

Reason for Recommendation: The Agency had not developed written procedures to address the protection of sensitive participant information contained in participant electronic communications. Additionally, we noted through observation that participant communications could contain the participant's original message, which potentially could include unsecured, sensitive participant information, in instances where participants elected delivery notification of Agency responses from the Secure Message Center.

Status: **Implemented.**

a) In November 2013, the Agency developed and documented e-messaging procedures related to transmitting electronic communications in the Secure Message Center (SMC) within My Account. Agency management indicated that e-messaging procedures are enforced via Participant Service Representative (PSR) quality reports, which are conducted for each PSR ten times a month and allow PSR supervisors to review messages sent via SMC. We inspected *E-messaging Procedures*, dated November 1, 2013, and noted that procedures were documented for receiving electronic messages, responding to electronic messages, and reviewing electronic messages.

[5] The Secure Message Center is used by participants to send secure messages to the Agency regarding their TSP participant accounts.

b) Agency management indicated that its former contractor conducted testing to identify the root cause of the issue but evidence of detailed testing could not be provided. Prior to the change being deployed to production, the Agency's Supervisory Call Center Specialist tested the updated solution in development and verified that messages sent via SMC did not contain the contents of the message within the e-mail received by the participant.

Because evidence of testing SMC email configurations could not be provided, we determined an alternate approach to test if SMC email configurations were established to ensure that participant inquiries and responses are securely maintained. During our scope period, we observed that an Agency representative responded to a participant message sent using SMC with a custom reply and a message to the participant's personal e-mail address. When viewing the response in the participant's personal e-mail address, we noted that only a generic notification was sent and that the participant's original email was no longer appended to the Agency reply, prompting the participant to view the specific response to the inquiry in the SMC. As such, potentially sensitive information in the participant's SMC inquiry and the Agency representative's response was no longer sent to the participant's personal e-mail address, sufficiently resolving the condition noted during our 2013 audit.

Disposition: **Recommendation Closed.**

2013 Participant Website Recommendation No. 3:

Title: Lack of Guidance for Applicable Website Content

Original Recommendation: To strengthen conformance with Federal requirements, the Agency should develop and implement a process to determine and enforce applicability of relevant Federal website requirements for the TSP.gov and FRTIB.gov websites.

Reason for Recommendation: The Agency had not developed internal guidance regarding applicability of conformance to various Federal website laws and regulations.

Status: **Implemented.**

Late in our scope period, the Agency implemented policies and procedures to address this prior year recommendation. We inspected the Agency's *Compliance Program Policy*, dated September 30, 2015, and noted that the Office of General Counsel Compliance Team is responsible for analyzing inquiries or material received from external parties and information gathered through the use of automated tools, such as a content aggregator, to determine if material is applicable to the Agency. We also inspected the Agency's *Compliance Program Procedures*, dated November 30, 2015, and noted that the Agency uses a governance, risk, and compliance tool to develop two workflows. These workflows provide the Agency information that helps them determine the applicability of relevant Federal website requirements for the TSP.gov and FRTIB.gov websites. The first workflow, referenced as the Client-Requested Workflow, is used when an external party inquires of the Agency how or if a piece of legislation or other material affects the Agency. The second workflow, referenced as the Proactive Workflow, is used when the Compliance Team receives materials and information through subscriptions, alerts, and other tools.

Disposition: **Recommendation Closed.**

C. 2015 Findings and Recommendations

While conducting our performance audit over TSP participant website, we identified seven new findings and developed related recommendations. EBSA requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in My Account Functional Design Documentation

Although the Agency's primary system of record for business requirements is Serena Dimensions Requirements Manager (RM), the functional design document for the My Account portion of the

TSP website is also used for documenting website requirements. However, we noted that the *My Account - Functional Design Document*, dated January 23, 2014, did not include security-related information, including user ID requirements or password lockout settings, for end users. Additionally, the *My Account - Functional Design Document* had not been updated to include the business requirement for a ten character password, which was implemented on May 10, 2014.

The Agency had not updated the *My Account - Functional Design Document* to include requirements of the current state environment because of the lack of management oversight.

The Agency's Enterprise Information Security Risk Management (EISRM) *Configuration (CM) Policy*, dated June 29, 2012, states:

> (e) CONFIGURATION SETTINGS (CM-6 + Enhancement #1, 2, & 3) […]
>
> (2) Information System Owners, in cooperation with the Information System Security Manager [i.e., the CISO or a designated representative thereof, acting as the Certification Agent] SHALL establish mandatory configuration settings to provide a secure baseline for all systems, and SHALL ensure that authorized system engineers, administrators, and the Information System Security Officer:
>
> (A) Document all configuration settings as those settings are implemented.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Configuration Management (CM), Control CM-6 states:

> Control: The organization:
>
> a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; […]

1. The Agency should:

a. Update the *My Account - Functional Design Document* to capture the current environment and include all currently implemented security requirements and settings, including user ID, password lockout, and minimum password character requirements; and

b. Develop, document, and implement procedures to periodically update the *My Account - Functional Design Document* in the future for consistency with the Serena Dimensions RM.

Without properly documenting and updating business requirements based on business needs, the Agency may not track and address all requirements of the system; may not be able to integrate My Account with other inter-related systems; and may not be able to recreate logical, programmatic, or security requirements in the unexpected event of a system failure or loss.

Least Privilege Weaknesses in Content Change Management

During our audit procedures, we noted that a review was not conducted of user access permissions to the Cascade Server, a content management solution that enables content posting and modifications to the TSP.gov and FRTIB.gov websites. For all 5 users sampled with access to the Cascade Server, Agency management did not provide evidence of approvals. Additionally, we noted that all 29 Cascade Server users were granted administrative privileges, which were not required for their ongoing job functions.

During the conversion from Serena Collage to the Cascade Server, users were granted administrative privileges to allow for enhanced functionality; however, excessive access was not revoked after the conversion was completed. Additionally, Agency management had not developed, documented, and implemented access administration procedures and processes for the Cascade Server or defined related roles and responsibilities.

The Agency's EISRM *Access Control (AC) Policy*, dated June 26, 2012, states:

> (a) Account Management (CM-2 + Enhancements 1, 2, 3, and 4)
>
> Each Information System Owner, in cooperation with, and subject to the approval of, the Information Owners having information contained, or processes within each Information System, SHALL assign Information System Custodians to be responsible for the daily administration of all Information System access, including creating, activating, modifying, disabling, and removing accounts. […]
>
> (2) Information System Custodians/Account Managers and Security Administrators SHALL follow designated procedures for creating, activating, modifying, disabling, and removing user accounts and authentication credentials, including, but not limited to: […]
>
> (C) Reviewing account access privileges for appropriateness based on type of account and current requirements, including reviewing:
>
> (i) All in-active permanent accounts for appropriateness of assigned access rights no less than annually […]

(e) Least Privilege (AC-6) […]

(2) Information System SHALL employ the concept of least privilege when assigning rights related to specific duties and Information System access (as necessary to adequately mitigate risk to organization operations, organizational assets, and individuals) in accordance with:

(A) Job descriptions,

(B) Risk assessments,

(C) Audit findings, and

(D) IA Best Practices.

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Configuration Management (CM), Control CM-5 states:

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Access Control (AC), Control AC-2 states:

Control: The organization: […]

b. Establishes conditions for group and role membership;

c. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; […]

j. Reviews accounts for compliance with account management requirements [*Assignment: organization-defined frequency*] […]

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC, Control AC-6 states:

Control: The organization employs the principal of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2. The Agency should:

a. Develop, document, and implement access administration procedures, including role definitions and responsibilities, for systems that support Agency websites, including the Cascade Server; and

b. Develop, document, and implement an annual review of user and system accounts for systems that support Agency websites, including the Cascade Server, for ongoing appropriateness.

Not reviewing account access permissions increases the risk that individuals may have unnecessary or inappropriate access to make content changes to the TSP.gov and FRTIB.gov websites, which puts Agency systems at risk of inadvertent or deliberate disclosure, modification, or destruction.

Procedural Weaknesses in My Account Data Transfer

Nightly, a critical process transfers data from OmniPlus[6] to MySQL for participant data accessibility on the My Account portion of the TSP.gov website. However, Agency management had not documented the process and procedures for the information flow of data between these two systems, including the use of a File Transfer Protocol (FTP) and related security controls.

Management had not documented data transfer and FTP procedures for the nightly data transfer between OmniPlus and MySQL because the Agency did not identify a need to document such procedures.

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

> Control: The information system enforces approved authorizations for controlling the flow of information within the systems and between interconnected systems based on [*Assignment: organization-defined information flow control policies*].

3. The Agency should document data transfer and FTP procedures for the transfer of data between OmniPlus and MySQL.

[6] OmniPlus is the recordkeeping system that contains all TSP account records and stores transaction records made in My Account. Source: *My Account – Functional Design Document*, dated January 23, 2014.

By not documenting the data transfer and FTP process and procedures, the Agency cannot ensure that the complete and accurate transfer of data between OmniPlus and MySQL would occur nightly in the event of key personnel loss.

Content Change Management Approval Weaknesses

During our scope period, content change management weaknesses existed for the TSP.gov and FRTIB.gov websites. Specifically, we noted the following:

- For 14 of 15 FRTIB.gov content changes made using the Cascade Server selected for testing, proper evidence of initial approval was not provided, and for 7 of 15 FRTIB.gov content changes, evidence of testing approval was not provided;
- For 15 of 15 TSP.gov content changes made using the Cascade Server selected for testing, proper evidence of initial approval was not provided, and for 3 of 15 TSP.gov content changes, evidence of testing approval was not provided;
- For all 15 TSP.gov content changes made using Serena Collage selected for testing, proper evidence of initial approval and testing approval was not provided;
- The Agency had not developed, documented, and implemented procedures for requesting, approving, and migrating changes to the TSP.gov and FRTIB.gov websites into production; and
- One Cascade Server procedure document for updating meeting minutes to FRTIB.gov was created in response to our initial request.

These content change management weaknesses existed because of a lack of a configuration change management board or similar governing body to review and approve content changes prior to migration to production.

The Agency's EISRM *Configuration Management (CM) Policy,* dated June 29, 2012, states:

> (b) CONFIGURATION CHANGE CONTROL (CM-3 + Enhancements #1 & #2)
>
> (1) The Authorizing Official [i.e. the Chief Technology Officer or a designated representative thereof] SHALL ensure that:
>
> (A) All Information System Configuration Changes are authorized, documented, and controlled through the Agency Change Control procedures, in order to:
>
> (i) Prevent unauthorized changes;
>
> (ii) Provide an audit trail of all change events (see AU policy for more information on Audit trail requirements); and

(iii) Provide accountability for authorized system changes.

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CM, Control CM-3 states:

Control: The organization: […]

a. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
b. Documents configuration change decisions associated with the information system; […]

4. The Agency should:

a. Develop, document, and implement formal procedures for requesting, approving, and migrating changes to the TSP.gov and FRTIB.gov websites; and

b. Develop and implement a Configuration Change Board or similar governing body to approve all web content changes prior to migration.

Without formal procedures for requesting, approving, and migrating changes to its websites prior to implementation, the Agency may inadvertently implement a change that has an adverse effect on the TSP.gov and FRTIB.gov websites and Agency systems.

My Account Configuration Weaknesses

During our scope period, certain My Account configuration weaknesses existed. Specifically, we noted the following:

- Temporary user passwords issued to participants, and used for initial login, are only eight characters in length and do not meet the Agency's ten character requirement;
- Participants were not required to re-enter their current password prior to modifying their password on-line; and
- Separated participants were able to update their user profiles to include an invalid mailing address.

Configuration settings for temporary passwords and updating mailing addresses and re-authenticating prior to resetting passwords in My Account had not been documented or included in Serena Dimensions Requirements Manager software or the *My Account - Functional Design*

Document. Therefore, these security controls were not implemented on the My Account portion of the website.

The Agency's TSP.gov MyAccount website requires that "Passwords must contain: 10characters."

The Open Web Application Security Project *Session Management Cheat Sheet*, dated January 8, 2016, states:

> The session ID must be renewed or regenerated by the web application after any privilege level change within the associated user session. […] Other common scenarios must also be considered, such as password changes, permission changes or switching from a regular user role to an administrator role within the web application.

As a leading practice, *Postal Addressing Standards*, dated May 2015, Section 12-122, states:

> The Postal Service defines a complete address as one that has all the address elements necessary to allow an exact match with the current Postal Service ZIP+4 and City State files to obtain the finest level of ZIP+4 and delivery point codes for the delivery address.

5. The Agency should develop, document, and implement system edit checks that:

- **a. Require that temporary passwords are ten characters in length, in accordance with Agency requirements;**
- **b. Require users to re-enter their current password prior to modifying their password on-line; and**
- **c. Validate participant addresses entered in My Account against the United States Postal Service's Address Information System.**

Not requiring participants to re-authenticate prior to resetting their password may increase the likelihood of an unauthorized individual accessing an account. Further, failure to implement system edit checks that restrict participants from inputting invalid mailing addresses increases the likelihood that participants may not be notified of unauthorized My Account transactions.

Infrastructure Weaknesses

We were informed that an incident occurred in December 2015, with the TSP.gov website that negatively affected the network availability of TSP.gov and other Agency applications. As of the date of this report, the root cause of this incident had not been determined.

The Agency's EISRM *Incident Response (IR) Policy*, dated June 29, 2012, states:

> (d) INCIDENT HANDLING (IR-4)
>
> (2) The Incident Response Team Manager, in cooperation with the Chief Technology Officer (CTO) and the Chief Information Security Officer (CISO), SHALL implement an incident handling process for security incidents that includes:
>
> (D) Post-Incident Analysis and After Action Reporting, including: […]
>
> (iv) Creating and disseminating an After-action report […]

The Agency's EISRM *System and Communications Protection (SC) Policy*, dated June 29, 2012, states:

> The Confidentiality, Integrity, and Availability of Information is dependent on the Integrity and Availability of its host system and transmission media and may be compromised if the Integrity of Availability of the Information System it is stored in, transmitted through, or processed by, is compromised. Preserving the Integrity and Availability of Information Systems and their communication links is therefore paramount to the effort of preserving the Confidentiality, Integrity, and Availability of Information.

NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Incident Response (IR), Control IR-4, states:

> Control: The organization:
>
> a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; […]
>
> c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

6. The Agency should:

a. Complete a root cause analysis for the December 2015 website outage and subsequent unavailability of applications caused by this outage; and

b. Implement proposed solutions identified to address the cause of the December 2015 website outage as reported in the root cause analysis.

Without determining a root cause of this incident, the Agency may not be able to prevent future network outages. Further, failure to implement any fixes or solutions as a result of conclusions from the root cause analysis increases the likelihood that a similar incident and the unavailability of the www.TSP.gov and Agency applications may occur again.

RECOMMENDATION TO ADDRESS OTHER CONTROLS

Lack of Brand Monitoring Policies and Procedures

To monitor for unauthorized use of the TSP and FRTIB logos and brand names, the Agency implemented brand monitoring activities on July 1, 2014. However, brand monitoring policies and procedures had not been documented by the end of our scope period. Agency management had not documented these policies and procedures because of resource constraints.

The United States Government Accountability Office's *Standards for Internal Control in the Federal Government*, dated September 2014, Principle 12.01, states, "Management should implement control activities through policies."

7. The Agency should develop, document, and implement policies and procedures for TSP and FRTIB brand monitoring activities.

The lack of formal brand monitoring policies and procedures may result in processes to monitor and protect the TSP and FRTIB brand not being followed consistently or at all.

D. Summary of Open Recommendations

2015 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in My Account Functional Design Documentation

1. The Agency should:
    a. Update the *My Account - Functional Design Document* to capture the current environment and include all currently implemented security requirements and settings, including user ID, password lockout, and minimum password character requirements; and
    b. Develop, document, and implement procedures to periodically update the *My Account - Functional Design Document* in the future for consistency with the Serena Dimensions RM.

Least Privilege Weaknesses in Content Change Management

2. The Agency should:
    a. Develop, document, and implement access administration procedures, including role definitions and responsibilities, for systems that support Agency websites, including the Cascade Server; and
    b. Develop, document, and implement an annual review of user and system accounts for systems that support Agency websites, including the Cascade Server, for ongoing appropriateness.

Procedural Weaknesses in My Account Data Transfer

3. The Agency should document data transfer and FTP procedures for the transfer of data between OmniPlus and MySQL.

Content Change Management Approval Weaknesses

4. The Agency should:
    a. Develop, document, and implement formal procedures for requesting, approving, and migrating changes to the TSP.gov and FRTIB.gov websites; and
    b. Develop and implement a Configuration Change Board or similar governing body to approve all web content changes prior to migration.

My Account Configuration Weaknesses

5. The Agency should develop, document, and implement system edit checks that:
    a. Require that temporary passwords are ten characters in length, in accordance with Agency requirements;
    b. Require users to re-enter their current password prior to modifying their password on-line; and
    c. Validate participant addresses entered in My Account against the United States Postal Service's Address Information System.

Infrastructure Weaknesses

6. The Agency should:
    a. Complete a root cause analysis for the December 2015 website outage and subsequent unavailability of applications caused by this outage; and
    b. Implement proposed solutions identified to address the cause of the December 2015 website outage as reported in the root cause analysis.

RECOMMENDATION TO ADDRESS OTHER CONTROLS

Lack of Brand Monitoring Policies and Procedures

7. The Agency should develop, document, and implement policies and procedures for TSP and FRTIB brand monitoring activities.

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

May 12, 2016

Mr. Ian Dingwall
Chief Accountant
Employee Benefits
Security Administration
United States Department of Labor
Suite 400
122 C Street, N.W.
Washington, D.C. 20001-2109

Dear Ian:

This is in response to KPMG's email of May 5, 2016, transmitting the KPMG LLP report entitled Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan Participant Website, dated May 2016. My comments with respect to this report are enclosed.

Thank you once again for the constructive approach that the Department of Labor and its contractors are taking in conducting the various audits of the TSP. The information and recommendations that are developed as a result of your reviews are useful to the continued improvement of the Thrift Savings Plan.

Very truly yours,

Gregory T. Long

Enclosure

RECOMMENDATION TO ADDRESS FUNDAMENTAL CONTROLS

2015-1 Weaknesses in My Account Functional Design Documentation

Corrective Action Recommendation: The Agency should:

a. Update the My Account - Functional Design Document to capture the current environment and include all currently implemented security requirements and settings, including user ID, password lockout, and minimum password character requirements; and

b. Develop, document, and implement procedures to periodically update the My Account - Functional Design Document in the future.

Audit Response:

a. The Agency concurs with the recommendation regarding the Functional Design Document (FDD) for MyAccount. While the Agency's system of record for business requirements is Serena Dimensions Requirements Manager (RM), the MyAccount Functional Design Document should also include all currently implemented requirements. The Agency will have the My Account FDD updated by July 29, 2016.

b. The Agency concurs with this recommendation. The procedure for updating Serena Dimensions RM as requirements change is documented within the TESS Requirements Management Plan. The Agency will have this plan updated to incorporate the maintenance of the My Account FDD by July 29, 2016.

2015-2 Least Privilege Weaknesses in Content Change Management

Corrective Action Recommendation: The Agency should:

a. Develop, document, and implement access administration procedures, including role definitions and responsibilities, for systems that support Agency websites, including the Cascade Server; and

b. Develop, document, and implement an annual review of user and system accounts for systems that support Agency websites, including the Cascade Server, for ongoing appropriateness.

Audit Response:

a. The Agency concurs with the recommendation. Formal review of the current users of Cascade Server CMS is underway collaboratively between the Office of Communications and Education and the Office of Technology Services web teams. Purging of users who no longer require access to the CMS will be performed. A process and procedure will be developed to accomplish the review, purge, and addition of users. Creation of roles and definitions, in addition to or in place of the five pre-defined global roles, which more accurately describe the functions will be developed, documented and implemented by September 30, 2016.

b. The Agency concurs with this recommendation. An annual process to review user and system accounts for continued appropriateness will be developed, documented and implemented by December 30, 2016.

2015-3 Procedural Weaknesses in My Account Data Transfer

Corrective Action Recommendation:

The Agency should document data transfer and FTP procedures for the transfer of data between OmniPlus and MySQL.

Audit Response:

The Agency concurs with the recommendation. The current process for the data transfer to include the schedules from CA Scheduler that manage the transfer in addition to any oversight activities has been documented and was approved on April 30, 2016.

2015-4 Content Change Management Approval Weaknesses

Corrective Action Recommendation: The Agency should:

a. Develop, document, and implement formal procedures for requesting, approving, and migrating changes to the TSP.gov and FRTIB.gov websites; and

b. Develop and implement a Configuration Change Board or similar governing body to approve all web content changes prior to migration.

Audit Response:

a. The Agency concurs with the recommendation. FRTIB has a process in place for this function. Concurrently, formal procedures are currently being drafted collaboratively by the Office of Communications and Education, Office of External Affairs, and the Office of Technology Services web teams to address all components (requesting, approving, and migrating) of this recommendation. As the teams share the same Content Management System (CMS), the procedures will be materially similar, but because the two teams maintain different websites (TSP.gov and FRTIB.gov) and answer to different stakeholders, some procedural variances should be expected. These procedures will be developed, documented, and implemented by October 31, 2016.

b. The Agency concurs with the recommendation. The Agency will develop and implement a governing body to review and approve content changes prior to migration within the TSP.gov and FRTIB.gov websites by October 31, 2016.

2015-5 My Account Configuration Weaknesses

Recommendation: The Agency should develop, document, and implement system edit checks that:

a. Require that temporary passwords are ten characters in length, in accordance with Agency requirements;

b. Require users to re-authenticate prior to resetting their passwords; and

c. Validate participant addresses entered in My Account against the United States Postal Service's Address Information System.

Audit Response:

a. The Agency does not concur with the recommendation. The fact that Agency-issued temporary passwords are 8 randomized characters, whereas participant passwords may be no less than 10 characters in length, has no bearing on participant password security. Currently, the process is:

   i. Agency issues participant a temporary, 8-character password.
   ii. Participant logs in with temporary password and is immediately prompted to create a new password in accordance with Agency requirements. Participant cannot proceed further into My Account without changing the password.
   iii. If participant declines to change the password, they are returned to the Log In page.
   iv. Participant can reuse the temporary password an unlimited amount of times until a new password is created, but the temporary password will never take them further than the password change screen described in step ii.
   v. Once the participant successfully changes the password in accordance with Agency requirements, the temporary password is no longer valid.

   Changing the temporary password to satisfy the strong password requirement in My Account would require a complete redesign of the password function. A cost benefit analysis would be required, and at this time it is believed the cost benefit would not provide enough return on investment for this change to be feasible.

b. The Agency concurs with this recommendation. The Agency will implement a new requirement to force end users to re-enter their current password, as part of the on-line change password function. This requirement will reduce the risk of an unauthorized individual assuming control of a participant's account. This initiative is scheduled to be completed by December 31, 2016.

c. Agency concurs with the recommendation and considers this recommendation to be closed due to a compensating control. While My Account does not validate participant mailing addresses, an alternate process is in place. The Agency securely provides Broadridge Financial Solutions, the Agency's print and mail handling contractor, a quarterly United States Postal Service (USPS) National Change-of-Address (NCOA) formatted file, to validate participant mailing addresses. The NCOA formatted file contains the names and addresses of all TSP participants. On behalf of the Agency, the contractor processes the file against the USPS NCOA address information system's database. The contractor sends TSP change-of-address postcards to participants with address discrepancies. Additionally, the Agency receives a secure file from the contractor of the participants, with forwarding addresses for Agency corrections.

2015-6 Infrastructure Weaknesses

Corrective Action Recommendation: The Agency should:

a. Complete a root cause analysis for the December 2015 website outage and subsequent unavailability of applications caused by this outage; and

b. Implement proposed solutions identified to address the cause of the December 2015 website outage as reported in the root cause analysis.

Audit Response:

a. The Agency concurs with this recommendation and considers it to be closed. A Root Cause Analysis (RCA) was performed immediately following the website outage that occurred in December 2015. The RCA process determined that the SAN was flooded with Input Output requests from hosts exceeding its capacity to respond. The Problem Tickets and Incident Tickets related to this RCA (and provided to KPMG) provide additional detail of the analysis of the outage and the remediation efforts taken by the Agency.

   According to ITIL best practices and Agency procedures, Problem Records can only be formally closed when a root cause has been determined and steps have been taken to prevent future occurrences of the problem. The RCA has been completed to the extent possible at this point in time. This problem record will remain open and moved into the pending / recurrence state. The state of the problem record will be adjudicated on the anniversary of the incident if it has not occurred again.

b. The Agency concurs with this recommendation and considers it to be closed. Given the results of the RCA, the Agency has implemented three proposed solutions identified in the RCA (Problem Record PRB0040230). Agency management decided to not implement the remaining four proposed solutions in the RCA due to an ongoing refresh of the host environment.

RECOMMENDATION TO ADDRESS OTHER CONTROLS

2015-7 Lack of Brand Monitoring Policies and Procedures

Corrective Action Recommendation:

The Agency should develop, document, and implement policies and procedures for TSP and FRTIB brand monitoring activities.

Audit Response:

The Agency concurs with the recommendation and will develop, document, and implement policies and procedures for TSP and FRTIB brand monitoring activities by July 31, 2016.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

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

- My Account Password Business Requirements, dated December 16, 2015
- My Account Password Lockout Business Requirements, dated December 16, 2015
- My Account Business Requirements, dated January 8, 2016
- Enterprise Information Security and Risk Management (EISRM) Access Control (AC) Policy, dated June 29, 2012
- EISRM Configuration Management (CM) Policy, dated June 29, 2012
- EISRM System and Communications Protection (SC) Policy, dated June 29, 2012
- EISRM Audit and Accountability (AU) Policy, dated June 29, 2012
- Office of General Counsel (OGC) Compliance Program Policy, dated September 30, 2015
- OGC Compliance Program Procedures, dated November 30, 2015
- Draft Compliance Program Flowcharts, dated September 14, 2015
- OGC Memo: Applicability of Certain Laws, Memoranda, and Other Guidance Relating to Website Development and Maintenance, dated November 21, 2013
- OGC Memo: Applicability of OMB Circular No. A-130, dated March 17, 2009
- OGC Memo: OMB Memorandum Regarding Breach Notification Policy, dated June 18, 2007
- OGC Memo: Compliance re: OMB's 30 Day Cybersecurity Sprint, dated June 23, 2015
- OGC Memo: Compliance re: Department of Homeland Security Binding Operational Directive 15-01, dated June 30, 2015
- My Account E-messaging Procedures, dated November 1, 2013
- Federal Employees' Retirement System Act (FERSA) Regulation, dated January 18, 2016
- Office of Technology Services (OTS)-Webteam's Desk Procedures & Program Notes, dated March 27, 2014
- Standard Operating Procedure (SOP) – Adding Job Announcements to FRTIB.gov in Cascade Server, dated December 22, 2015
- SOP – Updating Meeting Minutes and Attachments, dated December 18, 2015
- Cascade Server Modify Access List, dated December 22, 2015
- FRTIB.gov Cascade Changes, dated January 12, 2016
- TSP.gov Cascade Changes, dated January 12, 2016
- TSP.gov Collage Changes, dated December 22, 2015
- TSP.gov Certificate Details, dated September 9, 2015
- Symantec Trust Network (STN) Certification Practice Statement, dated December 9, 2015
- Secure Socket Layer (SSL) Checker Symantec CryptoReport, dated January, 26, 2016
- TSP Browser Requirements (Browsers Website Plugin), dated January 24, 2016

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- TSP Browser Requirements (Recommended Browsers), dated January 24, 2016
- TSP Browser Requirements (Browsing Tips), dated January 24, 2016
- TSP Browser Requirements (Clearing Browser Cache), dated January 24, 2016
- TSP Browser Requirements (Java Script Settings), dated January 24, 2016
- File Transfer Protocol (FTP) hash for file transfer from OmniPlus to the My Account, dated January 29, 2016
- Computer Security Incident Response Team (CSIRT) Analyst Runbook, dated September 25, 2015
- Technology Enterprise Security Services (TESS) Security Operation Center (SOC) Incident Response Plan, dated May 28, 2015
- Brand Monitoring Request for Quotation (RFQ) Technical Evaluation, dated June 9, 2014
- Winvale Brand Monitoring Contract, dated June 27, 2014
- FRTIB Paid Search Report, dated February 12, 2015
- FRTIB Social Media Report, dated February 12, 2015
- FRTIB Websites Report, dated February 12, 2015
- FRTIB TSP Trademark Infringement Notices, dated August 2015
- TSP.gov Website Outage Incident Ticket, dated December 30, 2015
- TSP.gov Website Outage Problem Ticket, dated December 31, 2015
- TSP.gov Website Outage Root-cause Analysis report, dated December 30, 2015
- TSP.gov Site Scope Report/Alerts, dated December 30, 2015