KPMG

Employee Benefits Security Administration

Performance Audit of the Thrift Savings Plan Mobile Device Security and Governance Controls

May 8, 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

Michael Auerbach
Acting 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) mobile device security and governance controls. Our fieldwork was performed from September 19, 2016 through November 30, 2016, primarily at the Federal Retirement Thrift Investment Board's Staff's (Agency) headquarters in Washington, D.C. Our scope period for testing was October 1, 2015 through September 30, 2016.

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*. *Government Auditing 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 TSP mobile device security and governance controls were to determine whether (1) management developed a mobile device security and governance program; (2) management established controls for tracking and monitoring mobile devices; and (3) management established controls for configuring, updating, and removing mobile devices from the TSP network.

We present 11 new findings and recommendations related to TSP mobile device security and governance controls, all of which address fundamental controls. Fundamental control

recommendations address significant[1] 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. All recommendations are intended to strengthen TSP mobile device security and governance controls. The Agency should review and consider these recommendations for timely implementation. Section III.B 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 October 1, 2015 through September 30, 2016, (1) management had not developed a mobile device security and governance program; (2) management had not established controls for tracking and monitoring mobile devices; and (3) management had not established controls for configuring, updating, and removing mobile devices from the TSP network. As indicated above, we noted internal control weaknesses in all areas of the TSP mobile device security and governance controls within our audit objectives.

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 the recommendations.

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

[1] *Government Auditing Standards* section 6.04 defines significance in the context of a performance audit.

management. The report is not intended to be, and should not be, used by anyone other than these specified parties.

KPMG LLP

May 8, 2017

I. BACKGROUND OF THE TSP AND THE MOBILE DEVICE SECURITY AND GOVERNANCE PROCESS

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 September 30, 2016, had approximately $485 billion in assets and approximately 5.0 million participants[2].

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. Mobile Governance and Strategy[3]

The Agency developed its mobile device program to provide Federal employees and contractors with these devices and related applications to support limited telework and operational roles, including after-hours responsibilities. While the Agency had started a mobile device program in various forms since the early 2000s, the current program provides BlackBerry devices to Federal employees and contractors. These devices provide capabilities such as voice, mobile web, and TSP e-mail access. The Board members use iOS devices for voice, mobile web, TSP e-mail, and the BoardBook application and collaboration tool. Data plans for both BlackBerry and iOS devices are provided through a national telecommunications provider. To enroll in the program, an employee’s or contractor’s supervisor requests a mobile device for the individual through the Service Now portal, and the employee or contractor must meet certain required criteria.

---

[2] Source: Minutes of the October 31, 2016, Federal Retirement Thrift Investment Board meeting, posted on www.frtib.gov.

[3] Source: Multiple internally secured documents, procedures, and processes which pertain to the audit scope, dated from 2015 through 2016.

The Agency does not support bring-your-own-device (BYOD) for Federal and contract employees. Furthermore, Android devices are not supported by the program.

These offerings are considered an emerging technology for the Agency. Therefore, several related Agency policies and procedures are under development related to a mobile device governance and strategy program. During our scope period, mobile device governance relied on mobile-specific requirements defined in the Agency's Enterprise Information Security and Risk Management (EISRM) policies and the follow-on Baseline Security Requirements (BLSR) policy statement.

C. Mobile Device Management Solution[4]

During the scope of the audit, the Agency maintained two different mobile device management (MDM) tools used to administer the enrolled devices. An MDM tool allows the Agency to enroll devices for remote management, enforce security policies remotely, log user activity, monitor device compliance (with automated rules taking action to disable or wipe), and remotely decommission devices. One of the MDM tools active during the audit scope period was the BlackBerry Enterprise Server (BES), which administers BlackBerry devices. The Agency had also deployed a pilot implementation of IBM's MaaS360 to administer the iOS devices deployed in the infrastructure. In the spring of 2016, the Agency upgraded the BES to a newer version that supports iOS devices in addition to BlackBerry models. The Agency then re-enrolled all iOS devices into BES and decommissioned the MaaS360 service.

D. Tracking and Monitoring of Mobile Devices[5]

The BES performs limited tracking and monitoring of currently assigned mobile devices. In addition to the BES, the telecommunications company provides the Agency with data usage for all enrolled devices as part of the Agency' monthly billing process. The Agency is billed directly for Federal employee and contractor usage not otherwise covered under the TESS[6] contract. For support staff assigned through the TESS contract, contractor data plans are managed by a national telecommunications vendor, and costs are billed to the Agency under the TESS contract.

---

4 Source: Internally secured documents, dated August 26, 2016

5 Source: Office of Technology Services (OTS) Document Number OTS.100.01, EISRM: Baseline Security Requirements, dated May 31, 2015

6 Technology and Enterprise Support Services contract, awarded on October 1, 2014.

E. Configuration Management of Mobile Devices[5]

Configuration management of mobile devices begins with device enrollment. Once an enrollment request is approved in the Service Now workflow, including Agency approval, the mobile device is provisioned through the national telecommunications company for Federal employees and non-TESS contractors and through the TESS prime vendor for other non-Federal staff. Currently, TESS contractors and other Agency-approved contractors have the ability to obtain voice, mobile web, and TSP e-mail via the mobile device program.

After delivery of the new device, it is configured by the local desktop support team and enrolled into the BES. Once recognized, the BES pushes preconfigured policies, which include specific security configurations, to the managed mobile device.

In the event of a lost or stolen device, the BES has the capability to issue a wipe command. Upon termination, un-enrollment from the mobile program and removal of the device from BES are tasks in the overall de-provisioning process initiated by the Agency's information technology service desk (Service Desk).

F. Other Supporting Infrastructure[3]

In addition to the BES, the mobile device program relies on the Agency FRTIB network for e-mail access and does not access the externally-facing production network. The mobile device must be able to connect to the Agency's FRTIB network in order to provide the user with access to e-mail. Cellular and data services are provided by a national telecommunications company.

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) mobile device security and governance controls.

The objectives of this performance audit were to determine whether (1) management developed a mobile device security and governance program; (2) management established controls for tracking and monitoring mobile devices; and (3) management established controls for configuring, updating, and removing mobile devices from the TSP network.

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 October 1, 2015 through September 30, 2016. 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 mobile device security and governance process. Arranging the engagement included contacting the Agency and agreeing on the timing of detailed testing procedures.

During the testing and interviewing phase, we performed the following procedures to achieve our audit objectives:

- Conducted interviews;
- Collected and inspected auditee-provided documentation and evidence;
- Participated in process walk-throughs for mobile device administration activities and mobile device security and governance monitoring activities;
- Inspected applicable contracts and procedures for information technology support services;

- Inspected system documentation for evidence of implementation and ongoing monitoring of mobile devices;
- Inspected the population of mobile device users for evidence of baseline configuration actions, removal activities, and administrative monitoring;
- Inspected the population of mobile device administrators for evidence of least privilege access;
- Inspected a non-statistical sample of terminated employees and contractors for evidence of removal from the mobile device management tool;
- Inspected a non-statistical sample of new mobile device requests for evidence of appropriate approval; and
- Inspected a non-statistical sample of monthly vulnerability reports.

We conducted these test procedures primarily at the Agency's headquarters in Washington, DC. In Appendix B, we identify the key documentation provided by Agency personnel that we reviewed during our performance audit. Because we used non-statistically determined sample sizes in our sampling procedures, our results are applicable to the sample 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.

III. FINDINGS AND RECOMMENDATIONS

A. Introduction

We performed procedures related to mobile device security and governance controls over the Thrift Savings Plan (TSP) while conducting a performance audit at the Federal Retirement Thrift Investment Board's (Board) Staff's (Agency) headquarters. Our scope period for testing was October 1, 2015 through September 30, 2016. 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 October 1, 2015 through September 30, 2016 (1) management had not developed a mobile device security and governance program; (2) management had not established controls for tracking and monitoring mobile devices; and (3) management had not established controls for configuring, updating, and removing mobile devices from the TSP network. We noted internal control weaknesses in all areas of TSP mobile device security and governance controls within our audit objectives.

We present 11 new recommendations, presented in Section III.B, related to TSP mobile device security and governance controls, all of which address fundamental 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. 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 noted no prior recommendations requiring follow-up during our performance audit.

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

B. 2016 Findings and Recommendations

While conducting our performance audit over TSP mobile device security and governance controls, we identified 11 new findings and developed related recommendations. The U.S. Department of Labor Employee Benefits Security Administration requests appropriate and timely action for each recommendation.

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2016-01: Weaknesses in Mobile Device Governing Structure

During the scope period, we noted that a limited centralized governing structure existed to oversee mobile behavior and usage across the Agency, and the Agency lacked a central mobile device management office or similar organizational entity. We also noted that no formalized strategy had been documented to support and promulgate the Agency-wide mobile program, as evidenced by the following:

- Lack of formal, documented risk assessment prior to deploying either the Blackberry Enterprise Server (BES) or IBM's Mobile as a Service (MaaS) 360 mobile device management solution[7];
- Lack of formal, documented vendor selection process for the current and potential new mobile device management solutions; and
- Exclusion of relevant organization stakeholders from the mobile device and management solution selection process at the inception of the program, including the lack of a formalized roadmap developed by Agency stakeholders that would identify goals, objectives, and the anticipated future state of the program.

The Agency did not develop a formalized mobile strategy and governance program for mobile devices because of the lack of management and contractor oversight, competing priorities, and limited resources.

The Agency's Directive 12A, *Procurement Policy, Guidelines, and Procedures Manual*, Section XII – Competitive Proposal Evaluation, dated May 13, 1994 states:

2. Technical Evaluation Criteria. The Contracting Officer is responsible for directing the

[7] The Agency decommissioned the MaaS 360 mobile device management solution during the scope period.

activities of Board employees who have been appointed to a Technical Evaluation Panel (TEP) and are, therefore, responsible for the technical evaluation of proposals. The Contracting Officer ensures that the evaluation criteria are implemented in a consistent, fair, and practical manner throughout the evaluation process.

[…] For major acquisition contracting actions, a memorandum is inserted in the solicitation file detailing the evaluation method to be used. The Contracting Officer, however, may determine prior to the issuance of a solicitation, or prior to the receipt of proposals if the solicitation is appropriately amended, to employ any evaluation method logically determined to serve the best interests of the Board and the participants.

[…] Only Board employees who are familiar with the technical nature of the requirement […] may participate in a TEP.

The Agency's *Enterprise Information Security and Risk Management (EISRM): Baseline Security Requirements,* effective May 31, 2015, states:

RA-3 Risk Assessment

1. The Information System Security Officer SHALL:
   1.1. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits
   1.2. Document risk assessment results in a risk assessment report […]
   1.4 Update the risk assessment whenever there are significant changes to the information system or environment of operation that may impact the security state of the system […]

SA-4 Acquisition Process

2. The Division Chief of Contracting SHALL:
   2.1. Include the following requirements and/or specifications, explicitly or by reference, in any contracts related to Information System design, acquisition, or development based on an assessment of organizational risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:
      2.1.1. INFOSEC Contract Clauses may include the following, based on the complexity of the contract:
         ☐ Security functional requirements
         ☐ Security strength requirements

- ☐ Security assurance requirements
- ☐ Security-related documentation requirements
- ☐ Requirements for protecting security-related documentation
- ☐ Description of the information system development environment and environment in which the system is intended to operate
- ☐ Acceptance criteria

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

RA-3 Risk Assessment

Control: The organization: […]

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in [Selection: security plan; risk assessment report; [*Assignment: organization-defined document*]; […]
e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. […]

SA-4 Acquisition Process

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and

g. Acceptance criteria.

1. To strengthen mobile device security and governance, the Agency should:

a. Conduct and document a formal risk assessment of the deployed BES;

b. Develop and implement procedures to conduct and document a formal risk assessment prior to the deployment of any future mobile device management solutions;

c. Define and document a vendor selection process for the mobile device management solution, including detailed business and technical requirements; and

d. Identify and engage mobile device program organizational stakeholders to develop a program roadmap that includes the goals, objectives, and anticipated future state of the program.

Weaknesses in the mobile device program governance increase the likelihood the program is not meeting the Agency's business needs and that unknown risks may negatively impact Agency systems.

2016-02: Weaknesses in Mobile Device Requirements and Documentation

Security policies in place during the scope period did not comprehensively detail the Agency standards, procedures, and requirements for the mobile device program and were not readily available to Agency users. Specifically, policies and procedures did not exist over the following key areas:

- Definition and scope of mobile devices;
- Requirements to protect organization data on mobile devices, and procedures to follow when such requirements are not met or are broken;
- Definition of authentication and encryption control mechanisms required for mobile devices accessing the enterprise network (e.g., passcodes and lockout policy);
- Storing enterprise data and transmitting enterprise data;
- Sharing of data and other files using third party applications and personal email;
- Baseline configuration requirement(s) and common customization controls;
- Device compliance monitoring and remediation;
- User access review and recertifications;
- Number of devices allowed per user; and

- Mobile application testing.

The Agency did not develop mobile device standards, procedures, and requirements because of lack of management and contractor oversight and competing priorities.

The Agency's *EISRM: Baseline Security Requirements*, effective May 31, 2015, states:

> CM-1 Configuration Management Policy and Procedures
>
> 1. The Chief Information Security Officer SHALL:
>
> 1.1. Develop, document, and disseminate a configuration management standard that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
>
> 1.2. Review the configuration management standard annually and update as necessary
>
> 1.3. Develop, document, and disseminate procedures to facilitate the implementation of the configuration management standard for common controls
>
> 1.4. Review the configuration management procedures for common controls annually and update as necessary
>
> 2. The Security Configuration Management Manager SHALL:
>
> 2.1. Develop, document, and disseminate procedures to facilitate the implementation of the configuration management standard for system-specific controls
>
> 2.2. Review the configuration management procedures for system-specific controls annually and update as necessary […]

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

> AC-19 Access Control for Mobile Devices
>
> Control: The organization:
>
> a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
>
> b. Authorizes the connection of mobile devices to organizational information systems.
>
> Control Enhancement (5):
>
> Access Control for Mobile Devices | Full Device / Container-Based Encryption

The organization employs [*Selection: full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*Assignment: organization-defined mobile devices*] […]

CM-1 Configuration Management Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; […]

2. The Agency should develop and implement mobile device policies and procedures specific to the following key areas of security:

- **a. Definition and scope of mobile devices;**
- **b. Requirements to protect organization data on mobile devices, and procedures to follow when such requirements are not met or are broken;**
- **c. Definition of authentication and encryption control mechanisms required for mobile devices accessing the enterprise network (e.g., passcodes, lockout policy, "compromised root" or "jail broken" devices, operating system, and inactive devices);**
- **d. Storing enterprise data and transmitting enterprise data;**
- **e. Sharing of data and other files using third party applications and personal email;**
- **f. Baseline configuration requirement(s) and common customization controls;**
- **g. Device compliance monitoring and remediation;**
- **h. User access review and recertifications;**
- **i. Determination of the number of devices per user allowed to connect to Agency systems; and**
- **j. Mobile application testing.**

By not defining and implementing mobile device specific policies and procedures, Agency data residing on mobile devices is at risk of inadvertent or deliberate disclosure, modification, or destruction.

2016-03: Excessive Administrative Access to the Blackberry Enterprise Server

During our testing, we noted that the Blackberry Enterprise Server (BES) mobile device management application had two administrative type privileges, full and enterprise. Access to these privilege levels appeared inconsistent with "least privilege" requirements because 11 users were assigned the capability to manage the entire BlackBerry enterprise solution.

This condition occurred because of the lack of Agency oversight related to BES administrative access and the lack of a defined mobile strategy and governance program.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

> AC-6 Least Privilege
>
> 1. The System Owner SHALL:
>
> 1.1. Authorize access to the information system only for those processes and services necessary to accomplish assigned tasks and duties in accordance with FRTIB missions/business functions

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

> AC-6 Least Privilege
>
> Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

3. For the BES mobile device management application, the Agency should identify the minimum number of users required for full and enterprise administrative types, modify access accordingly, and develop and implement procedures to periodically review access permissions.

Failure to restrict access based on "least privilege" increases the risk that individuals may have inappropriate or excessive access to the BES console, which may result in unauthorized changes to the server and increases the risk of inappropriate disclosure, modification, or destruction of Agency data and systems.

2016-04: Lack of Removal of Non-Compliant Devices

During the scope period, the Agency did not actively monitor devices via the BES for compliance with Agency connection requirements. As such, the Agency had not taken actions to terminate or remove non-compliant devices, including personal devices connected to Agency systems.

The Agency was not actively monitoring mobile devices and removing non-compliant devices because of the lack of a defined strategy and governance program and the lack of management and contractor oversight.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

AU-2 Audit Events […]

2. The System Owner SHALL:
   - 2.1. Facilitate Collaboration on Audit Events with the Chief Information Security Officer
   - 2.2. Ensure the security audit function is coordinated with the network health and status monitoring function for monitored elements
   - 2.3. Ensure FRTIB-defined auditable events are audited within the information system
3. The Information System Security Officer SHALL:
   - 3.1. Maintain documentation (within the System Security Plan) that details which events are audited within the application, the format of event log entries, auditing frequency, and frequency of log reviews
   - 3.2. Ensure System Owners define system-specific auditable events which are adequate to support Incident Response and post-incident investigations […]

AU-6 Audit Review, Analysis, and Reporting […]

3. The System Owner SHALL:
   - 3.1. Increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to Agency operations, Agency assets, or individuals
     - 3.1.1. Upon identification
     - 3.1.2. Based on notification from the Chief Technology Officer, Chief Information Security Officer, or Security Operations Center
   - 3.2. Ensure the information system employs automated mechanisms to alert security personnel (i.e., the Information System Security Officer, Security

Operations Center, and the Chief Information Security Officer) of inappropriate or unusual activities with security implications including but not limited to:

3.2.1. Unauthorized privilege escalations
3.2.2. Unauthorized access
3.2.3. Inappropriate Usage (See the Incident Response and Limited Personal Use Policies for prohibited activities)
3.2.4. Denial of Service attacks
3.2.5. Malicious code detection

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

AU-2 Audit Events

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. […]

AU-6 Audit Review, Analysis, and Reporting

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and

b. Reports findings to [*Assignment: organization-defined personnel or roles*].

4. The Agency should develop and implement procedures to:

a. Conduct regular monitoring of devices managed by the BES for compliance with Agency connection requirements; and

b. Remove all non-compliant devices from the BES, including personal or unauthorized mobile devices connected to Agency resources.

Failure to monitor and remove non-compliant mobile devices, including personal mobile devices, connected to Agency resources increases the risk of unauthorized disclosure of Agency data.

2016-05: Weaknesses in Mobile Device Configuration Management Controls

The Agency had not developed and documented a unique process for mobile device configuration changes. In addition, the Agency's informal process deviated from its standard change configuration processes used for other systems; specifically, the Agency made multiple configuration changes during the scope period to the BES environment without proper documentation and approval prior to implementation.

Further, we noted the following instances in which Agency configuration management policies and processes were inconsistently enforced when updating the mobile devices' configuration baselines, an essential component for configuration management:

- For the most of the audit period, all 16 iOS devices used by TSP Board members were not governed by a configuration management baseline;
- The original configuration for Blackberry devices was not maintained in accordance with Agency policies; and
- iOS and Blackberry configuration baselines were not fully implemented during our scope period, although the Blackberry baseline was fully implemented during our fieldwork after our initial inquiries.

The Agency did not develop and document a process for managing mobile device configuration changes because of a lack of management and contractor oversight. We also noted that while Agency policy required configuration baselines for all systems, the Agency failed to follow this requirement because of lack of management enforcement of the requirement. Finally,

management indicated that the Agency was unable to consistently implement the mobile device baseline configuration requirements because of limited capabilities on the BES.

The Agency's *EISRM: Baseline Security Requirements*, effective May 31, 2015, states:

> CM-1 Configuration Management Policy and Procedures
>
> 1. The Chief Information Security Officer SHALL:
>
> 1.1. Develop, document, and disseminate a configuration management standard that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance […]
>
> 1.3. Develop, document, and disseminate procedures to facilitate the implementation of the configuration management standard for common controls […]
>
> 2. The Security Configuration Management Manager SHALL:
>
> 2.1. Develop, document, and disseminate procedures to facilitate the implementation of the configuration management standard for system-specific controls […]
>
> CM-2 Baseline Configuration […]
>
> 2. The System Owner SHALL:
>
> 2.1. Comply with the Baseline Security Requirements
>
> 2.2. Develop, document, and maintain under configuration control, a current baseline configuration of the information system and components […]
>
> CM-2 (3) Retention of Previous Configurations
>
> 1. The System Administrator SHALL: […]
>
> 1.2. Ensure FRTIB retains the previous configuration baselines as necessary to support rollback […]

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

> CM-1 Configuration Management Policy and Procedures
>
> Control: The organization:
>
> a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
>
> 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

b. Reviews and updates the current:

1. Configuration management policy [*Assignment: organization-defined frequency*]; and
2. Configuration management procedures [*Assignment: organization-defined frequency*].

CM-2 Baseline Configuration

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

CM-2 (1) Retention of Previous Configurations

Control: The organization retains [*Assignment: organization-defined previous versions of baseline configurations of the information system*] to support rollback.

5. The Agency should adhere to established configuration change management policies and procedures and update them to include mobile devices or develop and implement new procedures for the BES and mobile devices controlled through the BES.

Failure to follow established configuration change management policies and procedures increases the likelihood for unauthorized security configuration changes and the introduction of vulnerabilities to the BES.

2016-06: Security Weaknesses with the BoardBook Application

Certain security weaknesses existed with the BoardBook application used by the Agency to share and exchange Agency sensitive information with Board Members. Specifically, we noted that the Agency had not developed the security processes for the BoardBook application, including procedures for testing new versions prior to deployment.

These weaknesses related to the BoardBook application occurred because of the lack of management oversight and the lack of a formalized mobile strategy and governance program.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

SA-11 Developer Security Testing and Evaluation

1. The INFOSEC Contract Clauses SHALL:

1.1. Require the developer of the information system to:

1.1.1. Create and implement a security assessment plan
1.1.2. Perform unit, integration, system, and regression testing/evaluation
1.1.3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluations
1.1.4. Implement a verifiable flaw remediation process
1.1.5. Correct flaws identified during security testing/evaluation

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

> SA-11 Developer Security Testing and Evaluation
>
> Control: The organization requires the developer of the information system, system component, or information system service to: […]
>
> b. Perform [*Selection (one or more): unit; integration; system; regression*] testing/evaluation at [*Assignment: organization-defined depth and coverage*];
> c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; […]
> e. Correct flaws identified during security testing/evaluation.

NIST SP 800-124 Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, in Section 4.3 Implementation states:

> After the mobile device solution has been designed, the next step is to implement and test a pilot of the design, before putting the solution into production. Aspects of the solution that should be evaluated for each type of mobile device include the following: […]
>
> - **Protection.** Information stored on the mobile device and communications between the mobile device and the organization are protected in accordance with the established requirements. […]
> - **Applications.** The applications to be supported by the mobile device solution function properly. All restrictions on installing applications are enforced. All restrictions on uninstalling applications (such as enterprise mobile device management software) are enforced. […]

6. The Agency should develop and document the security processes for the BoardBook application, including procedures for testing new versions prior to deployment.

Lack of security processes for the deployment of the BoardBook application may reduce interoperability and increase the risk of inappropriate disclosure, modification, or destruction of Agency data and systems.

2016-07: Mobile Device Password Configuration Weaknesses

Although we noted that security personnel had configured the BES mobile device management application with password settings for both Blackberry and iOS devices, the settings were not in compliance with Agency policy, as follows:

- Password length was set to eight characters, while Agency policy requires 12;
- Password expiration was set to 90 days, while Agency policy requires 60 days for standard users;
- Password history was set to six (Blackberry) and ten (iOS), while Agency policy requires 24;
- Regarding password complexity, Blackberry devices were configured to support a minimum of only one letter and one number, and iOS devices were configured to support a minimum of four numbers. However, Agency policy requires least one each of upper-case letters, lower-case letters, numbers, and special characters; and
- The BES mobile device management application was not configured to restrict the number of failed password attempts.

These password configuration weaknesses existed because of the lack of management oversight and policy enforcement, competing priorities, and limited resources.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

> IA-5 Baseline Configuration (IA-5 + Enhancements #1) […]
>
> 1.2. Enforce minimum password complexity of 12 characters and at least one each of upper-case letters, lower-case letters, numbers, and special characters […]
>
> 1.4. Enforce password lifetime restrictions of one (1) day minimum and 60 days maximum for user accounts
>
> 1.5. Enforce password lifetime restrictions of one (1) day minimum and 90 days maximum for service accounts
>
> 1.6. Prohibit password reuse for at least 24 generations […]

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

IA-5 Authenticator Management

Control Enhancement (1):

Authenticator Management | Password Based Authentication

The information system, for password-based authentication:

a. Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];

d. Enforces password minimum and maximum lifetime restrictions of [*Assignment: organization-defined numbers for lifetime minimum, lifetime maximum*];

e. Prohibits password reuse for [Assignment: organization-defined number] generations; […]

7. The Agency should enforce password configuration requirements on mobile devices in accordance with Agency policy.

Failure to enforce a strong password policy on mobile devices increases the risk that mobile users may use weak passwords, thus placing Agency data at risk of unauthorized disclosure.

2016-08: Weaknesses over Compromised Devices

During our testing, we identified certain weaknesses over compromised device monitoring, reporting, and removal from Agency resources. Specifically, we noted:

- Although the BES mobile device management application had the capability to perform ad-hoc reporting of any devices that were compromised (a.k.a., jailbroken or rooted[8]) during the scope period, BES was not configured to automatically restrict those compromised Agency mobile devices from attempting to connect to Agency resources. Further, management did not have frequent monitoring in place to address the reporting and controlling of compromised devices; and
- The Agency did not have a procedure in place to confirm that a kill command, sent to mobile devices and used to disable lost or compromised phones, were received and performed as intended.

[8] "Compromised root" is the term used on iOS devices developed by Apple that indicate security of the mobile device was broken at the fundamental or root level. "Jail broken" is the term applied to Android devices when a similar security breach occurs on those devices.

This condition existed because of the lack of management oversight and the lack of defined procedures for compromised devices.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

AC-19 Access Control for Mobile Devices

1. The Chief Information Security Officer SHALL:
   1.1. Establish enterprise usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices
2. The System Owner SHALL:
   2.1. Authorize the connection of mobile devices to organizational information systems in accordance with the enterprise standard

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

AC-19 Access Control for Mobile Devices

Control: The organization:

a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

8. The Agency should develop and implement :

a. Procedures to automatically restrict compromised mobile devices from connecting to Agency resources;

b. Monitoring, reporting, and remediation procedures for compromised mobile devices enrolled in the program; and

c. A procedure to confirm that a kill command has been sent and executed by the targeted mobile device.

A compromised mobile device may bypass or disable vendor and Agency-implemented security policies on the device. This situation increases the risk that compromised devices may be exploited and, if allowed to connect to Agency network resources, may put Agency data at risk of unauthorized access and disclosure. Also, without confirmation that the kill command has been

successfully received and executed by the targeted mobile device, the Agency cannot have confidence that Agency data on a lost or compromised device has been successfully removed. This lack of confirmation places any Agency data on such devices at risk of unauthorized access and disclosure.

2016-09: Weaknesses in Mobile Device Incident Monitoring

During the scope period, the Agency did not send the BES application logs to the security incident and event monitoring tool, Splunk, for analysis and reporting. This weakness indicates that the Agency did not review BES-generated logs for mobile device management incidents, such as failed logins, lockouts, inactive devices, and administrative activity, as required by Agency policy.

The Agency did not develop procedures for reviewing mobile device incidents because of the lack of management and contractor oversight and an overreliance on contracted support.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

AU-2 Audit Events […]

2. The System Owner SHALL: […]
   2.3. Ensure FRTIB-defined auditable events are audited within the information system
3. The Information System Security Officer SHALL: […]
   3.2. Ensure System Owners define system-specific auditable events which are adequate to support Incident Response and post-incident investigations […]

AU-6 Audit Review, Analysis, and Reporting […]

3. The System Owner SHALL: […]
   3.2. Ensure the information system employs automated mechanisms to alert security personnel (i.e., the Information System Security Officer, Security Operations Center, and the Chief Information Security Officer) of inappropriate or unusual activities with security implications including but not limited to:
      3.2.1. Unauthorized privilege escalations
      3.2.2. Unauthorized access
      3.2.3. Inappropriate Usage (See the Incident Response and Limited Personal Use Policies for prohibited activities)
      3.2.4. Denial of Service attacks

3.2.5. Malicious code detection […]

IR-5 Incident Monitoring

1. The Security Operations Center SHALL:
   1.1. Record and track all reported incidents […]

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

AU-2 Audit Events

Control: The organization:

a. Determines that the information system is capable of auditing the following events: [*Assignment: organization-defined auditable events*];
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; […]
d. Determines that the following events are to be audited within the information system: [*Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event*].

   Supplemental Guidance: An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. […]

AU-6 Audit Review, Analysis, and Reporting

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*]; and
b. Reports findings to [*Assignment: organization-defined personnel or roles*].

IR-5 Incident Monitoring

Control: The organization tracks and documents information system security incidents.

9. The Agency should develop and implement BES-based audit logging procedures and integrate those logs with the Splunk security event and incident management software product for monitoring.

Failure to monitor BES audit logs and security incidents increases the risk of unauthorized access and disclosure of Agency data.

2016-10: Weaknesses in Mobile Device Approvals and Enrollment

Mobile devices were not appropriately approved in the mobile device program nor were consistent practices followed across platforms. Specifically, we noted the following:

- For all three newly enrolled devices tested on the pilot MaaS360 server and for three of eight newly enrolled devices tested on the BES, evidence of management approval was not provided;
- The Agency had not implemented a formal enrollment process for the pilot MaaS360 server, intended to replace the BES server, prior to its removal from the infrastructure[1];
- The Agency had not implemented a formal enrollment process requiring approvals for iOS devices given to Board members and senior Agency management; and
- While the Agency had defined a process in the Service Now workflow for new hires to request Blackberry devices as part of the onboarding process, the process for requesting Blackberry devices for existing employees did not require the level of documentation in the user tickets necessary to capture justification and management approval.

These enrollment process issues occurred because of the lack of a formalized mobile strategy and governance program, lack of Agency and contractor oversight, and overreliance on contracted support.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

AC-19 Access Control for Mobile Devices

1. The Chief Information Security Officer SHALL:
   1.1. Establish enterprise usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices […]
2. The System Owner SHALL:
   2.1. Authorize the connection of mobile devices to organizational information systems in accordance with the enterprise standard

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

> AC-19 Access Control for Mobile Devices
>
> Control: The organization:
>
> a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
> b. Authorizes the connection of mobile devices to organizational information systems.

10. The Agency should implement existing Agency account management approval requirements for all users when enrolling mobile devices and consistently document management justification and approval for all enrollment requests.

Failure to follow Agency account management approval requirements increases the risk that unauthorized devices and individuals may remotely connect to Agency resources and data.

2016-11: Weakness in Vulnerability Scanning of Mobile Device Server

During our scope period, the Agency had not developed and documented its mobile device vulnerability scanning procedures. Additionally, for one of three months tested during the scope period, the Agency did not maintain a detailed report of the vulnerabilities identified on the BES and did not provide evidence of remediation of any identified vulnerabilities. These issues occurred because of Agency resource constraints and lack of contractor oversight.

The Agency's *EISRM: Baseline Security Requirements,* effective May 31, 2015, states:

> RA-5 Vulnerability Scanning […]
>
> 3. The Security Operations Center SHALL:
>
> 3.1. Ensure all Agency information systems (i.e., databases, operating systems, web applications, and public-facing IP addresses, etc.) are scanned for vulnerabilities:
>
> 3.1.1. Monthly
>
> 3.1.2. When significant new vulnerabilities potentially affecting an FRTIB resource are identified and reported […]

3.3. Scan for vulnerabilities in the information system monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported

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

RA-5 Vulnerability Scanning

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; […]
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; […]

11. The Agency should:

a. Develop and implement procedures related to vulnerability management, including vulnerability scanning, remediation, and monitoring, for mobile device management solutions; and

b. Monitor for consistent implementation of the established vulnerability management procedures for the scanning, analysis, and remediation of mobile device management solutions.

Failure to monitor and remediate vulnerabilities places the BES, the mobile devices it monitors and controls, and other networked Agency resources at increased risk of unauthorized modification, disclosure, or destruction.

C. Summary of Open Recommendations

2016 RECOMMENDATIONS

RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

Weaknesses in Mobile Device Governing Structure

1. To strengthen mobile device security and governance, the Agency should:
    a. Conduct and document a formal risk assessment of the deployed BES;
    b. Develop and implement procedures to conduct and document a formal risk assessment prior to the deployment of any future mobile device management solutions;
    c. Define and document a vendor selection process for the mobile device management solution, including detailed business and technical requirements; and
    d. Identify and engage mobile device program organizational stakeholders to develop a program roadmap that includes the goals, objectives, and anticipated future state of the program.

Weaknesses in Mobile Device Requirements and Documentation

2. The Agency should develop and implement mobile device policies and procedures specific to the following key areas of security:
    a. Definition and scope of mobile devices;
    b. Requirements to protect organization data on mobile devices, and procedures to follow when such requirements are not met or are broken;
    c. Definition of authentication and encryption control mechanisms required for mobile devices accessing the enterprise network (e.g., passcodes, lockout policy, and "compromised root" or "jail broken" devices, operating system, and inactive devices);
    d. Storing enterprise data and transmitting enterprise data;
    e. Sharing of data and other files using third party applications and personal email;
    f. Baseline configuration requirement(s) and common customization controls;
    g. Device compliance monitoring and remediation;
    h. User access review and recertifications;
    i. Determination of the number of devices per user allowed to connect to Agency systems; and
    j. Mobile application testing.

Excessive Administrative Access to the Blackberry Enterprise Server

3. For the BES mobile device management application, the Agency should identify the minimum number of users required for full and enterprise administrative types, modify access accordingly, and develop and implement procedures to periodically review access permissions.

Lack of Removal of Non-Compliant Devices

4. The Agency should develop and implement procedures to:
    a. Conduct regular monitoring of devices managed by the BES for compliance with Agency connection requirements; and
    b. Remove all non-compliant devices from the BES, including personal or unauthorized mobile devices connected to Agency resources.

Weaknesses in Mobile Device Configuration Management Controls

5. The Agency should adhere to established configuration change management policies and procedures and update them to include mobile devices or develop and implement new procedures for the BES and mobile devices controlled through the BES.

Security Weaknesses with the BoardBook Application

6. The Agency should develop and document the security processes for the BoardBook application, including procedures for testing new versions prior to deployment.

Mobile Device Password Configuration Weaknesses

7. The Agency should enforce password configuration requirements on mobile devices in accordance with Agency policy.

Weaknesses over Compromised Devices

8. The Agency should develop and implement:
    a. Procedures to automatically restrict compromised mobile devices from connecting to Agency resources;
    b. Monitoring, reporting, and remediation procedures for compromised mobile devices enrolled in the program; and
    c. A procedure to confirm that a kill command has been sent and executed by the targeted mobile device.

Weaknesses in Mobile Device Incident Monitoring

9. The Agency should develop and implement BES-based audit logging procedures and integrate those logs with the Splunk security event and incident management software product for monitoring.

Weaknesses in Mobile Device Approvals and Enrollment

10. The Agency should implement existing Agency account management approval requirements for all users when enrolling mobile devices and consistently document management justification and approval for all enrollment requests.

Weakness in Vulnerability Scanning of Mobile Device Server

11. The Agency should:

    a. Develop and implement procedures related to vulnerability management, including vulnerability scanning, remediation, and monitoring, for mobile device management solutions; and
    b. Monitor for consistent implementation of the established vulnerability management procedures for the scanning, analysis, and remediation of mobile device management solutions.

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

May 8, 2017

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

Dear Michael.

This is in response to KPMG's email on April 18, 2017, transmitting the KPMG LLP report entitled Employee Benefit Security Administration Performance Audit of Mobile Device Security and Governance Controls, dated May 2017. 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,

Ravindra Deo

Ravindra Deo
Acting Executive Director

Enclosure

Executive Director's Staff Formal Comments on the
Employee Benefits Security Administration Performance Audit of the Thrift Savings Plan
Mobile Device Security and Governance Controls

2016 RECOMMENDATIONS TO ADDRESS FUNDAMENTAL CONTROLS

2016-1 Weaknesses in Mobile Device Governing Structure

To strengthen mobile device security and governance, the Agency should:

a. Conduct and document a formal risk assessment of the deployed BES;

b. Develop and implement procedures to conduct and document a formal risk assessment prior to the deployment of any future mobile device management solutions;

c. Define and document a vendor selection process for the mobile device management solution, including detailed business and technical requirements; and

d. Identify and engage mobile device program organizational stakeholders to develop a program roadmap that includes the goals, objectives, and anticipated future state of the program.

Agency Response:

a. The Agency concurs with the recommendation. A formal risk assessment of the deployed BES HA server will be performed and documented by November 30, 2017.

b. The Agency concurs with the recommendation. The Agency will develop and implement risk assessment as part of the Assessment and Authorization procedures by November 30, 2017.

c. The Agency concurs with the recommendation. The Agency will develop, document, and implement its mobile device strategy by December 31, 2017.

d. The Agency concurs with the recommendation. The Agency is in the process of developing the program roadmap that includes the goals, objectives and anticipated future state of the mobile device management program. The Agency expects to complete the program roadmap by December 31, 2017.

2016-2 Weaknesses in Mobile Device Requirements and Documentation

The Agency should develop and implement mobile device policies and procedures specific to the following key areas of security:

a. Definition and scope of mobile devices;

b. Requirements to protect organization data on mobile devices, and procedures to follow when such requirements are not met or are broken;

c. Definition of authentication and encryption control mechanisms required for mobile devices accessing the enterprise network (e.g., passcodes, lockout policy, "compromised root" or "jail broken" devices, operating system, and inactive devices);

d. Storing enterprise data and transmitting enterprise data;

e. Sharing of data and other files using third party applications and personal email;

f. Baseline configuration requirement(s) and common customization controls;

g. Device compliance monitoring and remediation;

h. User access review and recertifications;

i. Determination of the number of devices per user allowed to connect to Agency systems; and

j. Mobile application testing.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will define the scope of mobile devices in the BLSR by November 30, 2017.

b. The Agency concurs with the recommendation. The Agency will expand the BLSR to include requirements to protect organization data on mobile devices by February 28, 2018. The Agency will develop and implement procedures to protect organization data on mobile devices, to include when requirements are not met or are broken, by November 30, 2017.

c. The Agency concurs with the recommendation. The Agency will expand the BLSR to define authentication and encryption control mechanisms for mobile devices accessing the enterprise network in the BLSR by November 30, 2017.

d. The Agency concurs with the recommendation. The Agency will expand the BLSR to include storing and transmitting enterprise data by November 30, 2017.

e. The Agency concurs with the recommendation. The Agency will expand the BLSR to include sharing of data and files by November 30, 2017.

f. The Agency concurs with the recommendation. The Agency will expand the BLSR to include configuration change management policies for mobile devices by November 30, 2017.

g. The Agency concurs with the recommendation. The Agency will expand the BLSR for mobile device compliance monitoring and remediation by November 30, 2017.

h. The Agency concurs with the recommendation. The Agency will expand the BLSR and develop procedures for user access review and recertification by November 30, 2017.

i. The Agency concurs with the recommendation. The Agency will develop and implement the Mobile Device Issuance and Maintenance Procedure by December 31, 2017.

j. The Agency concurs with the recommendation. The Agency will develop and implement procedures for mobile application testing by December 31, 2017.

2016-3 Excessive Administrative Access to the Blackberry Enterprise Server

For the BES mobile device management application, the Agency should identify the minimum number of users required for full and enterprise administrative types, modify access accordingly, and develop and implement procedures to periodically review access permissions.

Agency Response:

The Agency concurs with the recommendation. The Agency identified and allows up to five privileged users with full and enterprise administrative access for the new BES HA mobile device management application. The BES 12 policies will remain unchanged since this server will be decommissioned. The Agency will develop a procedure to manage account access for mobile devices. The Agency will develop and implement procedures to conduct periodic reviews of the privileged users by November 30, 2017.

2016-4 Lack of Removal of Non-Compliant Devices

The Agency should develop and implement procedures to:

a. Conduct regular monitoring of devices managed by the BES for compliance with Agency connection requirements; and

b. Remove all non-compliant devices from the BES, including personal or unauthorized mobile devices connected to Agency resources.

Agency Response:

a. The Agency concurs with the recommendation. The Agency is currently implementing BES HA Compliance Policy for iOS devices. The BES 12 policies will remain unchanged since it will be decommissioned. The Agency will develop

procedures to conduct regular monitoring of devices managed by BES HA. The Agency will develop and implement procedures by October 31, 2017.

b. The Agency concurs with the recommendation. The Agency is currently implementing BES HA Compliance Policy for iOS devices. The BES 12 policies will remain unchanged since it will be decommissioned. The Agency will develop and implement procedures to remove non-compliant devices managed by BES HA server by October 31, 2017.

2016-5 Weaknesses in Mobile Device Configuration Management Controls

The Agency should adhere to established configuration change management policies and procedures and update them to include mobile devices or develop and implement new procedures for the BES and mobile devices controlled through the BES.

Agency Response:

The Agency concurs with the recommendation. The Agency will update its policies, including the BLSR, and develop applicable procedures for the BES HA server and mobile devices controlled through the BES HA server. The Agency will complete this update by November 30, 2017.

2016-6 Security Weaknesses with the BoardBook Application

The Agency should develop and document the security processes for the BoardBook application, including procedures for testing new versions prior to deployment.

Agency Response:

The Agency concurs with the recommendation. The Agency will develop and document the security processes for testing new versions to be included in the Assessment and Authorization procedures by December 31, 2017.

2016-7 Mobile Device Password Configuration Weaknesses

The Agency should enforce password configuration requirements on mobile devices in accordance with Agency policy.

Agency Response:

The Agency concurs with the recommendation. The Agency currently enforces password requirements through the configuration settings of the BES HA Server. The BES 12 policies will remain unchanged since it will be decommissioned. FRTIB policy on mobile device password complexity is stated in the BLSR under controls IA-5 and AC-3. The Agency will close this recommendation by November 30, 2017.

2016-8 Weaknesses over Compromised Devices

The Agency should develop and implement:

a. Procedures to automatically restrict compromised mobile devices from connecting to Agency resources;

b. Monitoring, reporting, and remediation procedures for compromised mobile devices enrolled in the program; and

c. A procedure to confirm that a kill command has been sent and executed by the targeted mobile device.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will develop procedures for usage restriction, configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices. The procedures will provide guidance to automatically restrict compromised mobile devices from connecting to the Agency resources. The Agency will develop and implement the procedures by November 30, 2017.

b. The Agency concurs with the recommendation. The Agency will develop procedures for usage restriction, configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices. The procedures will provide guidance for monitoring, reporting and remediating compromised mobile devices. The Agency will develop and implement the procedures by November 30, 2017.

c. The Agency concurs with the recommendation. The Agency will develop procedures for usage restriction, configuration requirements, connection requirements and implementation guidance for organization-controlled mobile devices. The procedures will ensure targeted mobile device received the wipe/kill command from BES server. The Agency will develop and implement the procedures by November 30, 2017.

2016-9 Weaknesses in Mobile Device Incident Monitoring

The Agency should develop and implement BES-based audit logging procedures and integrate those logs with the Splunk security event and incident management software product for monitoring.

Agency Response:

The Agency concurs with the recommendation. The Agency will develop and implement BES-based audit logging procedures and integrate those logs with the security event and incident management software. The Agency will develop a corrective action plan by November 30, 2017.

2016-10 Weaknesses in Mobile Device Approvals and Enrollment

The Agency should implement existing Agency account management approval requirements for all users when enrolling mobile devices and consistently document management justification and approval for all enrollment requests.

Agency Response:

The Agency concurs with the recommendation. The Agency will enforce procedures during the enrollment of all mobile devices, to document the management justification and approval of each newly enrolled device.

The Agency will enforce account management approval procedures to document the management justification and approvals of all mobile device replacement requests of existing VIP and standard government, and contractor employees, and all new employee enrollment requests for mobile devices. The Agency will close this recommendation by November 30, 2017.

2016-11 Weakness in Vulnerability Scanning of Mobile Device Server

The Agency should:

a. Develop and implement procedures related to vulnerability management, including vulnerability scanning, remediation, and monitoring, for mobile device management solutions; and

b. Monitor for consistent implementation of the established vulnerability management procedures for the scanning, analysis, and remediation of mobile device management solutions.

Agency Response:

a. The Agency concurs with the recommendation. The Agency will update and implement its vulnerability management procedures for scanning, analysis, and remediation of mobile device management solutions by December 31, 2017.

b. The Agency concurs with the recommendation. The Agency will monitor for consistent implementation of the established vulnerability management procedures for the scanning, analysis, and remediation of mobile device management solutions by December 31, 2017.

APPENDIX B

KEY DOCUMENTATION AND REPORTS REVIEWED

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

- *Enterprise Information System Risk Management (EISRM) Security Training and Awareness (AT) Policy*, dated June 21, 2012
- *EISRM Access Control (AC) Policy*, dated June 29, 2012
- *EISRM Audit and Accountability (AU) Policy*, dated June 20 2012
- *EISRM System Authorization (CA) Policy*, dated June 8, 2012
- *EISRM Configuration Management (CM) Policy*, dated June 20, 2012
- *EISRM Contingency Planning (CP) Policy*, dated June 26, 2010
- *EISRM Identification and Authentication (IA) Policy*, dated June 25, 2012
- *EISRM Incident Response (IR) Policy*, dated June 26, 2012
- *EISRM Maintenance (MA) Policy*, dated June 21, 2012
- *EISRM Media Protection (MP) Policy*, dated June 8, 2012
- *EISRM Physical and Environmental Protection (PE) Policy*, dated June 26, 2012
- *EISRM Planning (PL) Policy*, dated June 8, 2012
- *EISRM Program Management (PM) Policy*, dated June 8, 2012
- *EISRM Personnel Security (PS) Policy*, dated June 26, 2012
- *EISRM Risk Assessment (RA) Policy*, dated June 8, 2012
- *EISRM System and Service Acquisition (SA) Policy*, dated June 26, 2012
- *EISRM System and Communication Protection (SC) Policy*, dated June 26, 2012
- *EISRM Systems & Information Integrity (SI) Policy*, dated June 26, 2012
- *EISRM: Baseline Security Requirements*, dated May 31, 2015
- *How to Activate New Blackberry Device in BES12*, dated May 17, 2016
- *iOS Device and Email Setup Guide BES12*, dated August 17, 2016
- *Lost / Stolen BlackBerry and iPad Process*, as of August 26, 2016
- BlackBerry Enterprise Server (BES) Device Inventory List, generated on August, 24, 2016
- Screenshot of the BES dashboard, generated on August 24, 2016
- *Mobile Device Enrollment Qualification Requirements*, dated September 22, 2016
- BES Enrolled Mobile Devices, dated August 23, 2016
- BES Device Enrollment Approvals, varous dates
- MaaS360 Enrolled Mobile Devices, dated August 23, 2016
- MaaS360 Device Enrollment Approvals, various dates
- TESS Program Contractor New Hire Listing, dated August 26, 2016
- Federal Employee New Hire Listing, dated August 31, 2016

KEY DOCUMENTATION AND REPORTS REVIEWED, CONTINUED

- BES - Active User List, generated August 24, 2016
- Termination List- Federal Employees, generated August 31, 2016
- Termination List- Contractors, generated August 31, 2016
- Screenshot of Set Number of Devices Per User, obtained on August 24, 2016
- BES Blackberry Password Configuration, generated August 28, 2016
- BES iOS Password Configuration, generated August 28, 2016
- Login Attempts (Blackberry and iOS), generated August 24, 2016
- Screenshot of BES Compromised Device Monitoring, generated August 23, 2016
- BES Allowed Mobile OS Listing, generated August 24, 2016
- BES Device Inventory List (OS Versions), as of August 24, 2016
- BES Administrators- User List(s), as of August 24, 2016
- BES Administrators- Rights by Role, as of August 24, 2016