U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE EMPLOYEE BENEFITS SECURITY ADMINISTRATION

EBSA CAN PROVIDE GREATER OVERSIGHT OF THE THRIFT SAVINGS PLAN BY STRENGTHENING ITS AUDIT PROGRAM

DATE ISSUED: OCTOBER 11, 2018
REPORT NUMBER: 05-18-001-12-001

U.S. Department of Labor
Office of Inspector General
Audit

BRIEFLY...

EBSA CAN PROVIDE GREATER OVERSIGHT OF THE THRIFT SAVINGS PLAN BY STRENGTHENING ITS AUDIT PROGRAM

October 11, 2018

WHY OIG CONDUCTED THE AUDIT

Proper oversight of the world's largest retirement plan – the Federal Government's Thrift Savings Plan (TSP) – is vital to ensuring the security of the $510 billion in retirement assets it holds. The Employee Benefits Security Administration (EBSA) is charged with oversight of the TSP. In that capacity, EBSA has the authority to perform audits, civil investigations and take legal action against certain fiduciaries. However, the agency lacks certain critical aspects of oversight; for example, EBSA cannot perform criminal investigations or take legal action against the Federal Retirement Thrift Investment Board (Board) and Executive Director, arguably the most significant fiduciaries. Moreover, the Board is not required to implement audit recommendations EBSA makes.

By contrast, EBSA has full legal authority to bring legal action against private pension plans to force them to take action to correct issues it discovers in the course of its investigations. This ability is EBSA's most effective enforcement tool.

WHAT OIG DID

OIG conducted a performance audit to determine the following:

> Did EBSA conduct effective oversight of the TSP?

READ THE FULL REPORT

https://www.oig.dol.gov/public/reports/oa/2019/05-18-001-12-001.pdf

WHAT OIG FOUND

EBSA did not conduct effective oversight of the TSP for several reasons. First, EBSA lacked an ongoing process for assessing changes in risks to the TSP over time. EBSA had available relatively limited funds to expend on TSP audits, and a robust system to prioritize audits would ensure those resources were most effectively used.

Second, EBSA's oversight was not transparent. We found little information available to participants and beneficiaries about audits of the TSP because EBSA did not post its audit reports and recommendations to a forum such as its website. Transparency provides assurances of accountability to participants and beneficiaries.

Finally, EBSA lacks sufficient legal authority to require the Board to act on its recommendations. Although EBSA can conduct audits of the TSP and make recommendations for improvement, the Board is not required to implement them. Despite identifying significant IT security weaknesses, 73 percent of all recommendations made in the TSP audit reports EBSA issued from 2010 through 2017 are still open. The vast majority of those address IT security issues, an increasingly scrutinized area given the prevalence of cyberattacks against large institutions, including one in 2011 against a TSP contractor that compromised more than 120,000 accounts.

Notwithstanding the limits of its legal authority, EBSA needs to strengthen its oversight practices to provide greater assurance that plan assets and personal and financial information are safeguarded.

WHAT OIG RECOMMENDED

We recommended the Assistant Secretary for the Employee Benefits Security Administration implement a formal risk assessment system for prioritizing audits; post audit reports either redacted or only by title, and at least annually, post a listing of significant unimplemented non-sensitive audit recommendations; and seek amendments to the Federal Employees Retirement System Act granting EBSA additional statutory authority over the TSP.

TABLE OF CONTENTS

INSPECTOR GENERAL'S REPORT

Preston Rutledge
Assistant Secretary
for Employee Benefits Security Administration
U.S. Department of Labor
200 Constitution Ave, NW
Washington, DC 20210

The Thrift Savings Plan (TSP) is reportedly the largest defined contribution plan in the world, with 5.1 million participants and assets of $510 billion as of July 2017. The TSP is the federal equivalent of a private sector 401(k) plan, allowing federal employees to save pre-tax dollars toward their retirement.

The Federal Retirement Thrift Investment Board (FRTIB or Board) administers the TSP. As part of its oversight responsibilities, EBSA has the authority to perform civil investigations and audits directed at determining the Board's compliance with its fiduciary responsibilities and provisions relating to prohibited activities.

Due to concerns regarding EBSA's legal authority over the Board, coupled with the number of participants and the significant amount of money in the TSP, we performed an audit to determine the following:

Did EBSA conduct effective oversight of the TSP?

To answer this question, we reviewed federal laws and regulations related to EBSA's oversight of the TSP as well as reviewed various EBSA audit guides. We interviewed EBSA and met with Board officials to determine what oversight and communication practices existed relative to TSP monitoring. To assess EBSA's internal controls over the contractor it hired to audit the Board, we asked EBSA and its audit contractor to complete questionnaires. We also reviewed relevant supporting documentation.

RESULTS

EBSA was not able to conduct effective oversight of the TSP largely because it lacked certain internal processes, such as a systematic risk assessment process to determine its audit priorities, and a means to make important information readily available to external stakeholders, for example, by posting audit reports and recommendations to a public forum, such as its website. In addition, EBSA's oversight responsibilities with respect to the Board include performing audits and civil investigations of the TSP. To enforce any findings resulting from these audits and investigations, EBSA is empowered to take legal action against certain fiduciaries of the TSP, excluding, however, the Board or Executive Director. This limitation severely curtails EBSA's ability to enforce its findings because the Board and Executive Director are arguably the most important individuals in charge of administering the TSP. It is unclear if any other TSP employees qualify as fiduciaries and therefore subject to EBSA's authority. As a result, EBSA did not have sufficient enforcement authority over the TSP.

EBSA SHOULD IMPROVE ITS RISK ASSESSMENT PROCESS

EBSA lacked a documented formal analytic, systematic, and ongoing process for assessing the ever-changing threats and opportunities that could affect the achievement of its goal to safeguard the TSP. According to EBSA, its goal was to audit as many TSP program areas as possible every three years. EBSA said that its audits were based on programs EBSA considered high risk, when these programs were last reviewed, and the funds available to expend on audits. EBSA, however, did not demonstrate adequate evidence of a systematic, analytical process by which it assessed program risk.

OMB Circular A-123–*Management's Responsibility for Enterprise Risk Management and Internal Controls* sets forth required guidance to federal agencies for their risk assessment processes, such as the one EBSA prepared for its TSP audit program. We compared EBSA's risk assessment process with that described in the Circular and determined EBSA's process did not meet the criteria for risk assessments laid out in the Circular. For example, the Circular states risks are not static and must be assessed on a continuous and ongoing basis. The Circular also emphasizes that management must integrate risk management and an effective internal control system into its existing business activities. In this context, a proper risk assessment process should identify and document high-risk topic areas to ensure they receive audit priority. The Government Accountability Office's (GAO) *Internal Control Management and*

Evaluation Tool provides guidance regarding management's responsibility for identifying risks. In that document, GAO suggests that "[q]ualitative and quantitative methods [should be] used to identify risk and determine relative risk rankings on a scheduled and periodic basis." GAO continues by describing factors management should consider in preparing a risk assessment. Especially relevant in this case are, for example, "risks associated with technological advancements and developments" and "risks resulting from heavy reliance on contractors or other related parties to perform critical agency operations..." Although EBSA appears to consider these in an informal risk assessment, we found little evidence of a robust analytical process, outside of reviewing the results of previous audits, that would assign audit priority based on regular, documented assessments of the changing levels of risk. EBSA could not document that it had an ongoing, systematic process by which it calculated and assigned risk to the various audit areas.

Risk assessments can take many forms and include many inputs; for example, Circular A-123 notes that part of an audit risk assessment could include using past audit findings as a factor in the risk assessment. However, EBSA's practice has been to audit the same program areas using the same approach and audit objectives. In some cases, although those audits resulted in minimal findings or recommendations, the audits were repeated with the same minimal result. Following are some examples:

- Audits on "Investment Management Operations" issued in FYs 2012, 2014, 2016, and 2017 were repeated even though none of these reports contained any findings or recommendations;
- The "Investment Funds Operation Process" audit reports issued in FY 2012 and FY 2015 produced no new audit recommendations.

The fact that the repetition of audit topics resulted in few new recommendations suggests that EBSA may not have fully considered prior audit results as a factor in its risk assessment, and the lack of a documented process makes it difficult to determine what, if any impact prior audit results may have had on EBSA's risk assessment. That said, previous audits are one of many factors to consider, but not the only consideration in a comprehensive risk assessment. EBSA correctly points out that the extremely high dollar amounts involved in TSP operations greatly increase the risk involved. This fact however, argues even more strongly for a well-planned and executed risk assessment process, so that all relevant factors can be considered in making an audit plan for the TSP.

A well-documented assessment process that prioritizes and acknowledges the changing nature of risks will enhance management's ability to identify and

address high-risk areas and improve the use of audit resources. Without a transparent, effective, and well-documented risk assessment process, TSP participants have little assurance that plan assets and personal and financial information are being properly safeguarded and that the Board's actions are prudent. In the case of the TSP, 5.1 million TSP participants with holdings of $510 billion in retirement funds are subject to unnecessary risk.

EBSA AUDIT REPORTS WERE NOT READILY ACCESSIBLE TO EXTERNAL STAKEHOLDERS

Audits principally provide value when they are available to stakeholders of the audited entity. When audit reports are not freely available, stakeholders lack an important tool that helps guide their decision-making. The most important stakeholders of the TSP are its participants and beneficiaries. Only a limited number of audit reports EBSA has issued since FY 2010 were accessible to participants and beneficiaries. However, to find these audit reports, one would first have to locate the Board's website, then find and read through the Board's monthly meeting minutes, and look for meeting attachment links indicating an audit report had been released to the public that month, then click the link to access the actual audit report. Adding complexity to this endeavor is the fact that the Board's website (www.frtib.gov) is not the same as the TSP website (www.tsp.gov) familiar to participants. The TSP website allows participants to check balances and manage their accounts. As such, it seems that website would be the one most participants would tend to visit. The Board website, on the other hand, contains little content relevant to a participant's day-to-day management of their account, so it seems unlikely participants would visit that site. Since neither the Board nor EBSA publish audit reports or a list of open audit recommendations, the availability of information about TSP audits is unnecessarily limited. This makes it difficult for stakeholders such as participants and beneficiaries to access reports that might allow them to make better-informed decisions about their retirement funds, which, according to Board statistics, is substantial: the average account balance as of November 2017 was more than $130,000.[1]

Other oversight organizations such as federal offices of inspector general (OIG) are required to promptly and publicly post non-sensitive reports in such a way that they are easily and directly accessible on their websites. Federal OIGs are also required to periodically publish lists of significant unimplemented recommendations.

[1] Average civilian non-Roth balance.

GAO's *Standards for Internal Control in the Federal Government* require management to consider its entity's overall responsibilities to external stakeholders and establish reporting lines that allow the entity to both communicate to, and receive information from, external stakeholders. We consider the requirements placed on federal OIGs to represent a best practice for oversight organizations insofar as readily available audit reports increase transparency, promote accountability, and assist management in its responsibilities to establish reporting lines that facilitate communication. Failure to publish audit reports deprives stakeholders of important information needed to make decisions affecting their retirement savings.

DESPITE MULTIPLE EBSA AUDITS, LONGSTANDING IT SECURITY ISSUES CONTINUE TO PLAGUE THE TSP

The auditors who performed the TSP's first independent FISMA evaluation in 2016 found deficiencies across all IT security functions, which continued into 2017. Moreover, between FYs 2010 and 2017, EBSA issued 55 audit reports containing 180 recommendations, some dealing with internal TSP processes, but most with IT security issues (see Table 1). As of September 30, 2017, 131 – 73 percent – of those recommendations remained open, of which 114 related to "fundamental controls," as characterized by the auditors (see Table 4 on page 9). The Board has expressed a commitment to correcting the continuing deficiencies identified by the auditors; despite that, progress has been slow. EBSA's lack of authority under FERSA has left almost a half-trillion dollars in TSP assets potentially exposed to security risks, such as unauthorized access to personally identifiable information and other financial information.

Table 1: Audit Reports and Recommendations Issued by Fiscal Year[2]

		Recommendations Issued	
Year	**Reports**	**IT Security**	**Other**
2010	3	6	3
2011	5	0	8
2012	6	4	8
2013	4	7	11
2014	10	23	1
2015	7	17	1
2016	10	33	11
2017	10	40	7
Total	55	130	50

[2] These reports were provided to OIG by EBSA and the information contained within was not independently verified.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT DEFICIENCIES

Title Ill of the E-Government Act of 2002, commonly referred to as FISMA, focuses on improving oversight of federal information security programs and facilitating progress in correcting agency IT security weaknesses. FISMA requires federal agencies, including the FRTIB, to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Under FISMA, agency heads are responsible for, among other things, providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

Additionally, FISMA requires agencies to conduct an annual independent evaluation of their IT security programs and practices and to report its results to OMB. In general, these evaluations center around five information security functions and seven FISMA "metric domains" (see Table 2).

For FY 2016, the auditors who conducted the FRTIB's first FISMA evaluation found deficiencies in all five functions and seven domains. In their summary results, the auditors stated, in part:

Risk Management–FRTIB has not fully implemented a Risk Management strategy and has not established appropriate assessment procedures to continuously assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

Configuration Management–FRTIB's inventory of assets is not fully accurate and incomplete, security baselines required strengthening, a process that validates a list of changes from the

Table 2: FISMA Cybersecurity Functions and Metric Domains

Function	Domain
Identify	Risk management
Protect	Configuration management, Identity and access management, and Security training
Detect	Information security continuous monitoring
Respond	Incident response
Recover	Contingency planning

production environment has not been established, and known vulnerabilities have not been completely remediated.

Identity and Access Management–FRTIB has not fully implemented an Identity and Access Management program, which should include (but is not limited to), granting user access based on the least privilege principle, annual review of privileged users, establishment of a Personal Identification Verification … program for logical and physical access, controls that govern shared accounts, segregation of duties matrices, and enhancements regarding remote access configurations.

Security and Privacy Training–FRTIB has not provided a specialized security awareness and privacy training to [individuals] having significant security responsibilities.

Information Security Continuous Monitoring [ISCM]–FRTIB's ISCM program has not been fully developed and related policy and procedures have not been finalized. Furthermore, ISCM training has not been developed for key ISCM personnel.

Incident Response–Current policy does not include elements of an Incident Response program, such as training, designation of responsibilities for the Security Operations Center (SOC), collaboration procedures with DHS to respond to incidents to include utilization of DHS' Einstein program, and integration of IR requirements into FRTIB's other key business areas.

Contingency Planning–An overarching Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) have not been fully developed and implemented for the organization. Additionally, associated contingency planning tests have not been performed.

In addition to evaluating the five functions and seven domains, auditors assign a numerical grade between one and five to IT security programs based on their "maturity level," one being the least mature, and five the most (see Table 3).

In the FRTIB's 2017 FISMA evaluation, the auditors opined that:

- the TSP had not fully developed and implemented an effective organization-wide information security program;
- a number of control deficiencies related to people, process, and technology existed across all seven IG FISMA metric domains; and
- the appropriate maturity level for each of the seven FISMA domains was "Ad-Hoc."

Table 3: Maturity Model	
Level	**Description**
1: Ad-Hoc	Policies, procedures, and strategy are not formalized; activities are performed in an Ad-Hoc, reactive manner.
2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

In their 2017 report, the auditors also opined, among other things, the TSP "has not implemented an effective organization-wide information security program due to … [m]isaligned efforts to focus on addressing symptoms and not sufficiently analyzing root causes of previously-identified information security weaknesses." In short, the FTRIB suffers from IT security deficiencies that remain uncorrected, at least as of the 2017 FISMA evaluation.

THE BOARD HAS BEEN SLOW TO ACT ON EBSA AUDIT RECOMMENDATIONS

Since 2015, EBSA has spent an average of $2.5 million a year conducting performance audits of the TSP. These audits range in subject, some focusing on specific TSP processes, such as participant withdrawal operations, annuity operations, investment management operations, and participant account management operations; the majority of audits, however, are focused on IT security. EBSA auditors have identified significant, longstanding deficiencies in the TSP's IT security program. The auditors have issued many recommendations to the Board; ensuring they are implemented in a timely manner is critical to the security of the TSP. Some of these recommendations remain open since 2010 (see Table 4).

As Table 4 shows, 112 (85 percent) of the open recommendations related to IT security issues. EBSA auditors have pointed to several IT security areas as requiring prompt attention: in at least one report following up on previous recommendations, the auditors urged the Board to "…review and consider these [open] recommendations for timely implementation."

Moreover, 114 (87 percent) of the open recommendations, were categorized in audit reports as relating to fundamental controls, defined as "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" (see Table 4).

Table 4: Open Audit Recommendations by Type as of September 30, 2017[3]

	Open Recommendations		
Year Issued	**IT Security**	**Other**	**Addressing Fundamental Controls**
2010	2	0	2
2011	0	2	2
2012	3	1	4
2013	4	4	5
2014	18	0	16
2015	15	1	15
2016	30	4	29
2017	40	7	41
Total	112	19	114
Percent Open	**85%**	**15%**	**87%**

EBSA has consistently followed up with the Board regarding the lack of progress with repeated meetings and correspondence with the Board, and going as far as devoting resources to work with the Board on a short-term initiative begun in November 2016. In the "90 Day Security Sprint," the parties worked together to identify and correct high-risk audit findings reasonably prone to be addressed in the short-term window. EBSA followed up with the Board with frequent meetings; despite this effort, and as noted earlier in this report, the Board was unable to remediate many of the issues identified by the various audits. EBSA followed up by elevating the issue to the Secretary of Labor, who eventually wrote a letter to the Chairman of the Board urging him to address the TSP's security deficiencies. That said, progress has been slow, and the TSP remains at risk.

EBSA LACKS SUFFICIENT LEGAL AUTHORITY OVER THE TSP

EBSA, in its role as the TSP's federal regulator, lacks sufficient legal authority to conduct effective oversight.

EBSA is charged with oversight of both the TSP and private pension plans. The plans EBSA oversees are governed either by FERSA or the Employee Retirement Income Security Act of 1974 (ERISA). FERSA, among other things,

[3] These reports were provided to OIG by EBSA and the information contained within was not independently verified.

establishes standards for the federal Thrift Savings Plan. ERISA, on the other hand, establishes standards for private pension plans.

The two statutes have similarities: both allow EBSA to perform audits and investigations, and both require plan fiduciaries (in the TSP's case, the Board and Executive Director), to act "prudently" and in the best interest of their plan participants. The statutes, however, differ in a significant way when it comes to enforcement. ERISA allows EBSA to sue plan fiduciaries either to compel them to act in a certain way ("injunctive relief") and to collect monetary damages from them. FERSA, conversely, does not allow EBSA to sue the Board or Executive Director of the TSP, either to compel them to act or to collect monetary damages.

Personal liability is a powerful incentive for fiduciaries to act prudently and in their participants' best interests. Similarly, the ability to sue for injunctive relief is a powerful tool to compel organizations to act prudently and not contrary to the participants' best interests. These tools, however, are absent in FERSA. EBSA is limited to performing audits, but lacks effective tools to enforce findings that result from these audits.

Private pension plan fiduciaries can purchase liability insurance that helps cover the personal financial liability to which they are exposed by virtue of their positions. As originally passed in 1986, FERSA mirrored ERISA's personal liability and injunctive relief provisions. FERSA, however, was amended in 1988 to shield the Board from personal liability and remove EBSA's ability to sue for injunctive relief against the Board. According to the then-Executive Director of the Board, the 1988 amendments to the law were due in part to the potential difficulty in obtaining liability insurance for the Board and Executive Director. In a 1987 Committee hearing preceding the 1988 amendments to FERSA, the then-Executive Director of the Board testified that it would be difficult to find adequate insurance because of the unique nature and potential size of the TSP and lack of experience on which to base a premium.[4] It is unclear whether these challenges to obtaining liability insurance would still exist today. Congress subsequently amended FERSA to shield the Board, as well as the Executive Director, from personal liability for fiduciary breaches.

The 1988 amendments, in contrast to EBSA's authority with respect to private pension plans under ERISA, denied it the ability to sue for injunctive relief, thus taking away its ability to compel the Board to address audit recommendations, as well as denying it the only effective means of holding the Board accountable. As

[4] United States Congress, House Committee on Post Office and Civil Service. *Hearing on the Implementation of the Federal Employees' Retirement System,* March 24-25, 1987. 100th Congress, 1st Session. Washington: Government Printing Office, 1987 (statement of Francis X. Cavanaugh, Executive Director, Federal Retirement Thrift Investment Board).

a result, EBSA lost its most effective tools for compelling the Board to implement audit recommendations, rendering them effectively unenforceable.

In meetings with the OIG, the Board acknowledged the significance of the deficiencies reported by its 2016 and 2017 FISMA evaluations and the open audit recommendations. Board officials have stated the TSP is working toward resolving the underlying causes of each issue identified by an audit recommendation, and that once the most significant issues are resolved, the Board will work toward addressing the full recommendations. Board officials, in their response to the 2017 FISMA report, indicated that they were planning to move all IT security functions and domains to maturity level 2 in FY2018 and level 3 in FY2019. Nonetheless, because TSP systems are gateways to critical functions, such as participant applications for withdrawals, security vulnerabilities in those systems must be addressed.

OIG'S RECOMMENDATIONS

We recommend the Assistant Secretary for the Employee Benefits Security Administration:

1. Tailor EBSA's risk assessment process using criteria found in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.*

2. Timely and publicly post to its website all audit reports not considered "sensitive" in their entirety after the final release and post reports considered "sensitive" either redacted as appropriate or listed only by title along with a caption indicating the report contains sensitive information and will not be published.

3. On at least an annual basis, post to the EBSA public website a listing of all unimplemented, non-sensitive audit recommendations, including, at a minimum, the date of and text of the recommendations, a summary of the comments provided and any corrective actions proposed by the Board, and expected implementation dates (when available).

4. Seek amendments to FERSA granting EBSA injunctive authority similar to that EBSA has over private pension plans under ERISA.

SUMMARY OF EBSA'S RESPONSE

EBSA agreed to tailor its risk assessment process using criteria found in OMB Circular A- 123, *Management's Responsibility for Enterprise Risk Management and Internal Control* to better document the risk-related bases for its audit projects. Accordingly, as part of its planning for the FY 2019 audit cycle, the agency developed and implemented a "risk register" which included such factors as audit recommendations (both open and closed), the time span between audits, risk rankings, and other risk-related factors to develop an overall risk profile for each major audit area. The risk register will document the specific risk-related bases for the specific audit areas chosen for review in a unified comprehensive document.

EBSA also agreed, beginning in FY 2019, to post on its website non-sensitive audit reports and recommendations. Reports and recommendations critical or sensitive in nature will be redacted or listed by title only. EBSA will post information concerning all open, unresolved findings and recommendations. For non-sensitive items, proposed corrective actions and timeframes will be included.

In addition, EBSA agreed to explore possible legislative solutions that would provide the enhanced enforcement authority necessary to improve compliance with its audit findings.

SUMMARY OF FRTIB'S RESPONSE

In its response, the Board notes over the past several years leadership and staff at both the FRTIB and EBSA have worked together to improve the TSP's operations. While FRTIB believes they have made significant improvements in the daily operations of the TSP and their ability to handle cybersecurity threats, the agency acknowledges that their work is not complete and there is still progress that must be made.

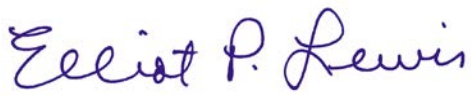
While the Agency acknowledges that its total number of open audit findings has grown and that addressing these findings is and will continue to be a priority, the Board and Executive Director do not agree with the statement that the Board "has been slow to act on EBSA audit recommendations." Instead, the FRTIB states the fact that the Agency's number of open audit findings has swelled is a matter the Board takes very seriously and monitors through regular reports. Also, FRTIB notes it is aggressively tackling audit findings and the underlying vulnerabilities using a risk prioritized approach to eliminate the vulnerability in the short run and implement fundamental controls to eliminate the root cause issues in the long run.

Additionally, the Board views EBSA's current authority as appropriate and effective, particularly when accounting for the unique status of the FRTIB and TSP. Further, the Agency contends that augmenting EBSA's authority to include injunctive relief may raise inherent conflicts for the Federal government (specifically the Department of Justice) and potentially negative consequences for the TSP.

FRTIB incorrectly states in their response that the OIG did not interview it during this audit. The OIG did in fact meet with FRTIB staff and officials to discuss this audit, share information, and obtain FRTIB's perspective in December 2015 and January and April 2018. We also considered the FRTIB's comments when drafting this report.

EBSA's full response can be found in Appendix B. FRTIB's full response can be found in Appendix C.

We appreciate the cooperation and courtesies EBSA and the Board extended us during this audit. OIG personnel who made major contributions to this report are listed in Appendix D.



Elliot P. Lewis
Assistant Inspector General for Audit

APPENDIX A: SCOPE, METHODOLOGY, & CRITERIA

SCOPE

OIG audited DOL's FY2014-FY2015 TSP audit programs and FY2010-FY2017 audit recommendations to the Federal Retirement Thrift Investment Board (FRTIB). We performed audit work at EBSA's National Office in Washington, D.C.

METHODOLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate 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 audit objectives.

To accomplish our objective, we: (1) reviewed federal laws and regulations and EBSA policies related to the agency's oversight of the TSP; 2) interviewed EBSA headquarters officials; Counsel for Regulation from DOL's Office of the Solicitor; and an Assistant Counselor in OIG's Office of Legal Services; 3) met with Board officials; and 4) reviewed various EBSA audit guides used to test IT operations, to include computer access and security controls. Additionally, to assess EBSA's internal controls related to overseeing the TSP, we asked the Agency to complete a 21- item questionnaire that included questions about the work of the contractor that audited the TSP.

We did not use data provided by EBSA or any computer processed data to develop our findings and conclusions related to the audit objective. Additionally, we did not use sampling. Therefore, we did not test data reliability.

In planning and performing our audit, we considered EBSA's internal controls that were relevant to our audit objective by obtaining an understanding of those controls and assessing control risks for the purposes of achieving our audit objective. The objective of our audit was not to provide assurance on the internal controls. Therefore, we did not express an opinion on the internal controls as a whole. Our consideration of EBSA's internal controls relevant to our audit objective would not necessarily disclose all matters that might be reportable conditions. Because of the inherent limitations on internal controls, noncompliance may nevertheless occur and not be detected.

CRITERIA

- ERISA Part IV
- Federal Employees' Retirement System Act (FERSA) of 1986 (Public Law 99-335), Title 5, Chapter 84 – Subchapter III, Sections 8439, Subchapter VII Sections 8472, and 8477
- Federal Information Security Management Act (FISMA) of 2002
- GAO Internal Control Management and Evaluation Tool, August 2001
- GAO Standards for Internal Control in the Federal Government
- OMB Circular A-123 Management's Responsibility for Internal Control
- OMB Circular A-123 Management's Responsibility for Enterprise Risk Management and Internal Control

APPENDIX B: EBSA'S RESPONSE TO THE REPORT

U.S. Department of Labor

Assistant Secretary for
Employee Benefits Security Administration
Washington, D.C. 20210

SEP 20 2018

MEMORANDUM FOR: ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: PRESTON RUTLEDGE
Assistant Secretary of Labor for Employee Benefits Security

SUBJECT: EBSA Response to OIG Performance Audit
Report No. 05-18-001-12-001

Thank you for the opportunity to review the September 2018 audit report regarding the Employee Benefits Security Administration's (EBSA) oversight of the Thrift Savings Plan (TSP). Below, EBSA outlines its plans to implement the report's recommendations and responds to some of the report's observations. As the report highlights, however, EBSA's robust audit program is currently hampered by the agency's lack of the enforcement authority necessary to compel compliance with audit recommendations.

OVERVIEW

The Federal Employees Retirement Systems Act (FERSA)[1] establishes standards for the TSP's fiduciaries, including the members of the Board and the Executive Director. It also describes prohibited transactions, outlines investigative and enforcement powers, and imposes fiduciary bonding requirements. FERSA gives the Secretary the authority and responsibility to conduct a program of audits of the TSP to ensure compliance with these standards and obligations. This administration is prioritizing TSP oversight and TSP compliance and risk management.

EBSA takes these responsibilities very seriously. The TSP is the world's largest employee contributory plan with over 5 million participants and $550 billion in assets. Given the substantial growth of the TSP in transaction volumes, as well as in numbers of participants and size of investments, EBSA conducts a rigorous audit program with a special focus on identified weaknesses that have not been adequately mitigated.

Risk Management

EBSA has a statutory obligation to carry out audits to "determine the level of compliance" with the fiduciary responsibility and prohibited transaction provisions of FERSA.[2] To that end, EBSA implements a risk-based audit program that identifies risks and vulnerabilities, assesses the likelihood of harm from these risks and vulnerabilities, and considers the magnitude of potential damage associated with the various risks. In recent years, as discussed in more detail below, this risk-based approach has resulted in a special focus on the security of the TSP's IT

[1] *See* 5 U.S.C. 8477, 8478 and 8478a.
[2] *See5* U.S.C. 8477(g)(1).

systems.[3] EBSA has devoted the majority of EBSA's audit funds to these IT systems based upon a quantitative and qualitative assessment of the security risks associated with the systems, as reflected and documented in EBSA's audit reports, penetration tests conducted at EBSA's request, FISMA reviews, and related activities, such as the 2017 "Security Sprint." The audit reports, penetration tests, FISMA audits, and correspondence and communications with the Board and TSP personnel demonstrate EBSA's careful focus on identifying risk, assessing the exploitability and potential impact of those risks, obtaining remedial actions, and reviewing the implementation of remedial actions. Thousands of pages of risk documentation support EBSA's focus on the TSP's IT systems, as well as its selection of specific IT vulnerabilities for review.

More generally, each component of the TSP Audit Oversight Manual reflects an area of operation that is susceptible to risk. For the non-IT operational portion of the audit program, EBSA broadly applies the same risk-based comprehensive approach discussed above. Regardless of whether OMB Circular A-123 literally applies to EBSA's audit work, the agency's audit program is always focused on risks, including their likelihood, potential resulting damages, and TSP's remediation and mitigation of identified risks. All the audit work is performed in accordance with Generally Accepted Governmental Auditing Standards (GAGAS), which also incorporates audit risk in both planning and performing the audit engagements. EBSA's aim with respect to these operational audits is not simply to do as many audits as funds permit, but rather – consistent with its obligation "to determine the [TSP's] level of compliance"—to comprehensively review TSP operations over a three-year cycle to ensure that the TSP is consistently operated in the best interests of participants and beneficiaries. EBSA believes that this cyclical aspect of the audit program is necessary to minimize the risks associated with not regularly reviewing all components of the TSP. Throughout this process, the agency ensures that priorities are established by careful, ongoing assessments of the risks facing the world's largest retirement plan.

Despite its careful and ongoing assessment of risks, however, and the thousands of pages documenting its work and risk-assessment, EBSA acknowledges that it does not routinely prepare a single formal document comprehensively setting forth its assessment of the risks that drive its selection of specific audit topics and activities. Accordingly, as EBSA moves forward with its audit program, it will routinely create such a risk register, which will document the risk-based assessments supporting the agency's actions. While EBSA does not believe this will result in a fundamental change in approach, it agrees that such formal documentation would increase transparency.

Transparency/Accountability

The report notes that EBSA's audit reports are not readily accessible to external stakeholders. Currently, EBSA does not post the reports or a list of open audit recommendations on its

[3] As the report notes on p.12: "Since 2015, EBSA has spent an average of $2.5 million a year conducting performance audits of the TSP. These audits range in subject, some focusing on specific TSP processes, such as participant withdrawal operations, annuity operations, investment management operations, and participant account management operations; the majority of audits, however, are focused on IT security. EBSA auditors have identified significant, longstanding deficiencies in the TSP's IT security program."

website. EBSA agrees that such posting could increase transparency, enhance accountability by increasing the TSP's incentives to work on the identified deficiencies, and facilitate communication. Accordingly, during FY 2019, EBSA will post non-sensitive audit reports and recommendations on the agency's website. Sensitive reports will remain non-public to maintain security just as OIG does not release its reports on sensitive issues. Reports and recommendations that are critical or sensitive in nature will be redacted or listed by title only.

Legal Authority

As originally enacted, FERSA placed no special limits on the liability of the Board Members and the Executive Directors.[4] They were subject to the same personal liability for fiduciary breaches as other Fund fiduciaries. Only the Secretary had authority to bring civil actions against Fund fiduciaries for monetary relief, but any participant, beneficiary, or fiduciary, as well as the Secretary, could bring an action to enjoin fiduciary breaches and for other appropriate equitable relief.

In 1988, however, Congress enacted technical corrections to protect the Board Members and the Executive Director from personal liability.[5] The Secretary's authority to enforce the fiduciary standards and transaction prohibitions now applies only to fiduciaries other than the Board members and the Executive Director.[6]

As the report explains, the effectiveness of EBSA's audit program is significantly reduced by its inability to compel the Executive Director and members of the Board to timely remedy audit findings. For example, between FY 2010 and FY 2017, the agency issued 55 audit reports containing 180 recommendations, some dealing with internal TSP processes, but most with IT security issues. As of September 30, 2017, 133 of these recommendations (74%) remained open. Moreover, these recommendations concern fundamental issues. Fully 86% of these open recommendations – 115 recommendations in total -- related to fundamental controls.[7] These recommendations remain open despite EBSA's expenditure of significant human and financial resources to identify the problems and promote their resolution. As the report notes, these efforts have included "repeated meetings and correspondence with the Board, going as far as devoting resources to work with the Board on a short-term initiative begun in November 2016" (the "90 Day Security Sprint" in which EBSA devoted IT personnel and contractors to work with the TSP to identify and correct high-risk and critical IT vulnerabilities).[8] The efforts also included the Department's advocacy in support of repeated IT penetration tests, an improved system of independent verification and validation of IT corrections, the elevation of audit issues to the Secretary, and involvement of other federal resources. Despite these efforts, as the report notes, "progress has been slow, and the TSP remains at risk."[9]

---

[4] *Id.* at p. 11. *See also* Pub. L. No. 99-335, sec. 101(a), 100 Stat. 514, 584-585 (1986).
[5] *Id. See also* Pub. L. No. 100-238, sec.133, 101 Stat. 1744, 1760-1761 (1988).
[6] 5 U.S.C. 8477(e)(3)(A).
[7] *Id.* "*EBSA Cannot Ensure the Effectiveness of it Audits of the Thrift Savings Plan,*" OIG Report No. 05-18-001-12-001, September 2018, p. at 5, 9.
[8] *Id.* at 10
[9] *Id.*

EBSA previously proposed amendments to FERSA that would enable the agency to seek injunctive relief from the Board and Executive Director in the same manner that it can currently seek such relief with respect to private pension plans. Alternatively, EBSA believes that such enforcement authority could be given to an independent Inspector General, as it has also suggested in the past.[10] EBSA agrees to continue to explore possible legislative solutions that would provide the enhanced enforcement authority necessary to ensure compliance with its audit finding.

RECOMMENDATIONS

1. **Tailor EBSA's risk assessment process using criteria found in OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control.***

As discussed above, EBSA agrees to implement the recommendation to better document the risk-related bases for its audit projects. Accordingly, as part of its planning for the FY 2019 audit cycle, the agency has developed and implemented a "risk register." The risk register includes such factors as audit recommendations (both open and closed), the time span between audits, risk rankings, and other risk-related factors to develop an overall risk profile for each major audit area. The risk register will document the specific risk-related bases for the specific audit areas chosen for review in a unified comprehensive document.

EBSA's risk-based audit program incorporates the criteria contained in OMB Circular A-123, and the risk register will document that approach. The planning and audit approach identifies risks and vulnerabilities, assesses the likelihood of harm from these risks and vulnerabilities, and considers the magnitude of potential damage. Additionally, EBSA reviews the Board and Executive Director's responsiveness to audit recommendations addressing vulnerabilities. The risk management process EBSA uses fully supports our underlying audit effort.

EBSA's audit program for the TSP's IT systems is illustrative of the agency's risk-based approach. Based on years of audit findings, independent penetration tests, FISMA compliance reviews, and direct interactions between EBSA staff, EBSA's contract auditor and TSP personnel, EBSA views the security of the TSP's IT system as a critical risk. Based upon these concerns, EBSA expended the majority of its TSP audit funds on IT audits, and EBSA worked with the FRTIB to obtain three independent penetration tests of the TSP's IT systems from 2015 through 2017, two conducted by Mandiant and one by the Department of Homeland Security. The purpose of these penetration tests was both to assess the current security posture of the IT systems and to assess the TSP's progress in resolving longstanding complaints. The resulting reports include hundreds of pages of detailed risk analyses and rankings of risk based on assessments of the exploitability of the vulnerabilities and the potential impact of successful exploitation of those vulnerabilities. Both the penetration tests and the FISMA reviews expressed specific ratings of the risk levels associated with identified vulnerabilities. EBSA's audit work was and is informed by these ratings and assessments – and they are used as a basis for determining future audit engagements.

[10] https://www.dol.gov/sites/dolgov/files/legacy-files/budget/2019/CBJ-2019-V2-01.pdf (page EBSA-11)

In addition, as a result of EBSA's ongoing concerns with the TSP's IT systems, in 2017, EBSA engaged in a "90 Day Security Sprint" with the TSP's IT personnel and contractors aimed specifically at remedying high-risk and critical vulnerabilities identified in both our audits and the penetration tests. These exercises focused on specified outstanding audit recommendations and independently verified EBSA's conclusions as to the vulnerabilities of the TSP's IT systems, as did the penetration tests. EBSA also expressed numerous specific concerns to the Board about the risks to which the TSP's IT systems were exposed, both at Board meetings and in repeated correspondence, both from EBSA's leadership and from the Secretary.

The audit reports, penetration tests, FISMA audits, correspondence and communications with the Board and TSP personnel demonstrate EBSA's careful focus on identifying risks, assessing the exploitability and potential impact of those risks, obtaining remedial actions, and reviewing the implementation of remedial actions. Thousands of pages of risk documentation support EBSA's focus on the TSP's IT systems, as well as its selection of specific IT vulnerabilities for review. EBSA cannot agree that there has been any deficiency in making and obtaining regular, documented assessments of risk on an ongoing basis, or that the TSP audits failed to consider these risks, their likelihood, magnitude, and remediation carefully. As noted above, however, EBSA does agree that the creation of a comprehensive risk register could increase transparency by setting out the agency's bases for choosing specific audit topics.

For the non-IT operational portion of the audit program, EBSA broadly applies the same risk-based comprehensive multi-year approach described above. The agency is always focused on risks, including their likelihood, potential resulting damages, and TSP's remediation and mitigation of identified risks. All of the audit work is performed in accordance with Generally Accepted Governmental Auditing Standards (GAGAS), which also incorporates audit risk in both planning and performing the audit engagements.

EBSA's aim with respect to these operational audits is not simply to do as many audits as funds permit, but rather to comprehensively review TSP operations over a three year cycle to ensure that the TSP is operated in the best interests of participants and beneficiaries. There is an important difference, however, between these operational audits and the IT audits: the operational audits have not found the sorts of high or critical risks that have plagued the IT program. While this is good news, it does not mean that EBSA need not conduct these audits or that it shouldn't conduct audits that are similar to prior year audits.

Nevertheless, the report appears to fault EBSA for continuing to conduct audits in risk areas for which it had previously made no or few findings. We disagree for at least three important reasons. First, any reasonable audit program must focus not only on the likelihood of harm, but also on the magnitude of potential harm. As the report notes, the TSP holds over $500 billion in assets for more than five million plan participants. Even if prior audits did not find deficiencies in the management or administration of these assets, the risk of loss is too great simply to dispense with important audit topics based on past findings. Second, it is very hard to assess the likelihood of loss based on past performance alone. Indeed, if EBSA were to consistently skip high-dollar audit areas based on past successes, it would effectively send a message to the TSP that one year's success means a free pass from oversight in future year(s). The dangers of such an approach should be obvious. Third, the environment in which the TSP is working is always

changing, as most recently demonstrated by recent changes in default investment options and default enrollment of military personnel. In other words, the context of the operational audits is always changing, meaning that even audits concerning the same broad topics are conducted in new contexts.

The report critically observes that audits on "Investment Management Operations" and "Investment Funds Operations Process" were repeated even though prior related reports did not contain any findings or recommendations. EBSA does not believe, however, that it could responsibly neglect to review investment management or funds operations on an ongoing basis, given the enormous size of the TSP's holdings and the number of participants potentially affected by poor investment management. Blackrock is the investment manager for the TSP and is responsible for all investment options other than the "G" Fund and currently manages more than 50% of the TSP's assets. When the "L" Funds became the default option for new TSP participants the audits in this area increased due to the greater likelihood and magnitude of harm. In EBSA's view, a decision not to audit investment management operations or Blackrock based on positive findings in past audits would increase the likelihood of violations and disregard the potentially large size of resulting injuries.

While EBSA believes the audit program responsibly balanced the well-documented and identified risks in the IT program with the clear and continuing importance of ensuring responsible management of the TSP's assets, it agrees that it can improve its documentation of the risk assessment process. Going forward, EBSA will use a risk register to document that process.

2. **Timely and publicly post all audit reports not considered "sensitive" in their entirety after the final release and post reports considered "sensitive" either redacted as appropriate or listed only by title along with a caption indicating the report contains sensitive information and will not be published.**

3. **On at least an annual basis, post to the EBSA public website a listing of all unimplemented, non-sensitive audit recommendations, including, at a minimum, the date of and text of the recommendations, a summary of the comments provided and any corrective actions proposed by the Board, and expected implementation dates (when available).**

EBSA agrees with these recommendations. During FY 2019, EBSA will post on its website non-sensitive audit reports and recommendations. Reports and recommendations critical or sensitive in nature will be redacted or listed by title only, just as OIG similarly does not post sensitive reports. We will post information concerning all open, unresolved findings and recommendations. For non-sensitive items, proposed corrective actions and timeframes will be included.

4. **Seek amendments to FERSA granting EBSA injunctive authority similar to that EBSA has over private pension plans under ERISA.**

As highlighted in the report, implementing audit recommendations in a timely manner is critical to the security of the TSP. Open recommendations date back to 2010 and 86% relate to

fundamental controls.[11] The TSP has been slow to act on EBSA's audit findings and recommendations. OIG recognizes EBSA's efforts to encourage and assist the Board and Director to remediate open recommendations:

> EBSA has consistently followed up with the Board regarding the lack of progress with repeated meetings and correspondence with the Board, and going as far as devoting resources to work with the Board on a short-term initiative begun in November 2016. In the "90 Day Security Sprint," the parties worked together to identify and correct high-risk audit findings reasonably prone to be addressed in the short-term window. EBSA followed up with the Board with frequent meetings; despite this effort, and as noted earlier in this report, the Board was unable to remediate many of the issues identified by the various audits. EBSA followed up by elevating the issue to the Secretary of Labor, who eventually wrote a letter to the Chairman of the Board urging him to address the TSP's security deficiencies. That said, progress has been slow, and the TSP remains at risk.[12]

As the OIG observed, "EBSA, in its role as the TSP's federal regulator, lacks sufficient legal authority to conduct effective oversight."[13] EBSA continues to explore ways to increase TSP compliance with audit recommendations. EBSA also agrees to explore possible legislative solutions that would provide the enhanced enforcement authority necessary to improve compliance with its audit findings.

[11] "*EBSA Cannot Ensure the Effectiveness of it Audits of the Thrift Savings Plan,*" OIG Report No. 05-18-001-12-001, September 2018, p. 9.
[12] *Id.* at 13.
[13] *Id.*

APPENDIX C: FRTIB'S RESPONSE TO THE REPORT

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

Office of Inspector General
Attn: Mr. Nicholas Christopher
U.S. Department of Labor
200 Constitution Ave., NW
Room S-5506
Washington, DC 20210

September 20, 2018

RE: FRTIB Response to Department of Labor, Office of Inspector General Audit Regarding the Effectiveness of the Oversight of the Thrift Savings Plan by the Employee Benefits Security Administration

Dear Mr. Christopher:

The FRTIB Board and Executive Director take seriously their legal mandate and mission to manage the Thrift Savings Plan (TSP) prudently and solely in the best interest of its participants and beneficiaries. To that end, FRTIB leadership, including the Board, the Executive Director, and senior management, has demonstrated an unwavering commitment to embrace input from stakeholders to ensure the TSP continues to be a world class defined contribution plan.

We thank the Department of Labor, Office of Inspector General (OIG) for its work and for allowing the FRTIB the opportunity to comment on its evaluation of the effectiveness of the oversight of the Thrift Savings Plan by the Department of Labor's Employee Benefits Security Administration (EBSA). We want to acknowledge that we view EBSA's audit program as much more than one simply required by law – we view EBSA as a critical partner in improving TSP operations and thank them for their ongoing support.

Over the past several years, as increasing cybersecurity risks have transformed the priorities of Federal agencies and private sector institutions, leadership and staff at both the FRTIB and EBSA have worked together to improve the TSP's operations, and we appreciate the support and counsel we have received from EBSA. While we believe that we have made significant improvements in the daily operations of the TSP and our ability to handle cybersecurity threats over the past few years, we acknowledge that our work is not complete and there is still progress that must be made.

1

Although the FRTIB was not interviewed as a part of this audit of EBSA, many of the conclusions drawn from and recommendations provided for in this report directly relate to the FRTIB and the Thrift Savings Plan. Consequently, as the fiduciaries of the TSP, we provide the following response.

Leadership of the TSP

The TSP is managed by five part-time Board members and a full-time Executive Director. In 2011, the composition of the FRTIB Board changed and, at this time, Mr. Michael Kennedy became Chairman. During Chairman Kennedy's tenure and that of his fellow Board members, the Board has consistently increased the resources available to the Agency to ensure that FRTIB staff and contractors can support the TSP's growing participant base and operational requirements. At the time that Chairman Kennedy assumed his role, the Federal Retirement Thrift Investment Board, which had been shrinking in size and budget over the previous several years, had a total staff of less than 100 employees and a budget of approximately $128 million. Since that time, while keeping expenses borne by participants relatively flat, in response to strategic priorities like cybersecurity, risk management, and audit remediation, the Board has nearly tripled the Agency's budget and increased the Agency's approved staffing level by approximately 250 percent.

These resources finally allowed the Agency to start to address significant technology and control issues. Specifically the Agency established an Office of Enterprise Risk Management including an Internal Audit Function and Anti-Fraud Division, established a division dedicated to cybersecurity, hired the Agency's first full-time Chief Information Security Officer, hired a Chief Operating Officer, established the FRTIB's first Security Operations Center (SOC), and rolled-out new programs such as Roth TSP accounts, L Fund default, and Blended Retirement for the Unformed Services.

As the TSP has grown in size and complexity, the skills required to manage the TSP have evolved. In April of 2017, the Board announced its selection of a new Executive Director. Additionally, over the past 18-24 months, the Agency has hired a new Chief Operating Officer, Chief Technology Officer, and Chief Information Security Officer. With the support of the Executive Director and FRTIB team, the Board will continue to provide the Agency with the resources and direction it requires to support the interest of the Thrift Savings Plan's participants and beneficiaries.

The State of TSP Cybersecurity and IT Operations

In part because of its ever evolving nature and environment-specific risk considerations, measuring cybersecurity is challenging. For example, the OIG report relies on one input (the IG assessment) of the Agency's 2017 FISMA assessment which found the Agency's FISMA maturity at an 'ad hoc' level. While the Agency agrees with the important feedback from this assessment and continues to work with its

independent FISMA auditor[1] to improve its FISMA compliance, the input from the IG is one of several factors which inform an agency's FISMA score. For example, there are additional assessments provided by the Chief Technology Officer and the Senior Agency Official for Privacy and commonly, conversations with the Office of Management and Budget and the Department of Homeland Security. Ultimately, as a result of these inputs, the FRTIB received an overall FISMA rating of 'at risk', the middle of three levels and the same as over 60% of rated Federal agencies.

Like most institutions, the FRTIB is constantly working to improve the state of its cybersecurity program and continues to dedicate resources and talent to harden its systems. Over the past five years, the Board has grown the FRTIB budget relating to cybersecurity 266% which has enabled FRTIB to make significant and tangible improvements in the IT environment, including:

- full encryption of all TSP data at rest, and all PII in transit,
- modernization and hardening of the TSP call center and data center infrastructure,
- implementation of security monitoring tools,
- two factor authentication for all FRTIB and contractor staff accessing the FRTIB environment,
- and complete integration of TSP contractors into the TSP environment, ensuring that FRTIB has full visibility into anyone with access to TSP data.

The Agency will implement the DHS's Trusted Internet Connection in early FY19, and is in the process of joining the DHS's Continuous Diagnostics and Mitigation (CDM) program, which will further fortify the Agency's networks and systems.

It often takes years to address many of the security issues that impact legacy systems as disparate and custom-built as the TSP's. However, over the past 12-18 months, as indicated by technical assessments of the TSP environment, the Agency's progress has been notable. For example, as reported at the Agency's April 2018 Board meeting, the FRTIB has been participating in the Department of Homeland Security's (DHS) National Cybersecurity Assessment and Technical Services (NCATS) program since 2014. This service provides an objective third party perspective on the current cybersecurity posture of external-facing Federal networks. In addition to noting that the FRTIB has never had any critical or high vulnerabilities, the most recent scans show that the FRTIB has had no open vulnerabilities (in any category) for the past several months and has reduced its time to mitigate vulnerabilities from a high of 200 days (for medium vulnerabilities) to nearly instantaneously.

[1] In addition to its FISMA auditor, the Agency has also retained the services of an independent firm with deep FISMA expertise. The firm is examining the Agency's performance in each FISMA domain, and is developing short-, medium- and long-term actions that will improve the Agency's performance in these domains.

The FRTIB is only one of four agencies that are currently fully compliant with all Department of Homeland Security-issued Binding Operational Directives (BODs), including BOD 18-01 relating to web and e-mail security mandates. It should also be noted that the agency was fully compliant with BOD 18-01 well before the October 2018 deadline.

Finally, the Agency has shown significant improvement in DHS assessments of social engineering vulnerability between 2015 and 2017.

In brief, hardening the TSP recordkeeping system and technology infrastructure has been and will continue to be the FRTIB's number one priority. Though the Agency must continue to improve in critical cyber and IT areas, it has made considerable progress and will leverage this progress to continue improvements.

How the FRTIB Addresses Audit Findings

As EBSA has significantly increased the number of annual TSP audits from 2 in 2012 to 18 in 2018, the Agency acknowledges that its total number of open audit findings has grown and that addressing these findings is and will continue to be a priority. However, the Board and Executive Director do not agree with the statement that the Board "has been slow to act on EBSA audit recommendations." The fact that the Agency's number of open audit findings has swelled is a matter the Board takes very seriously and monitors through regular reports. However, perhaps in part because Agency officials were not interviewed, critically omitted in the OIG's report's numerical summation of open audit findings is the fact that the Agency is aggressively tackling audit findings and the underlying vulnerabilities using a risk prioritized approach to eliminate the vulnerability in the short run and implement fundamental controls to eliminate the root cause issues in the long run.

As acknowledged by the National Institutes of Standards and Technology (NIST) in their special publications supporting FISMA compliance, the management of organizational risk is a key element in an organization's information security program. The FRTIB addresses vulnerabilities in its systems using a risk-based approach that directs FRTIB resources to address TSP systems' most critical vulnerabilities immediately. Specifically, in order to rank and address issues identified by sources such as external auditor partners which include EBSA, a FISMA auditor, and a financial statement auditor, the FRTIB utilizes a the CVSS (Common Vulnerability Scoring System) methodology, a framework used by both government and industry to objectively quantify the level of severity in an identified vulnerability. Those vulnerabilities rated the highest on the 10 point scale are designated critical or high vulnerabilities.

In addition to the CVSS rating, each finding is coded with the appropriate NIST control and the FISMA level that the finding addresses. For each critical and high finding, FRTIB immediately allocates resources toward responsive controls (e.g., patches) that mitigate the specific vulnerability and simultaneously FRTIB staff are

assigned longer-term projects to resolve broader, systematic issues (e.g., updating policies) that holistically address audit findings. The FRTIB began this process approximately a year ago; since then, the Agency reduced the severity of all 13 identified "critical" vulnerabilities, and reduced the severity of 27 of the 116 identified "high" vulnerabilities. As the process continues to mature and additional resources are deployed, the Agency expects the rate of reduction in operational vulnerabilities to accelerate—and thus further reduce overall operational risk.

Additionally, as the Board has been monitoring the nature of the Agency's open audit findings, the Board and FRTIB management designed a strategy to address the root cause of many of the Agency's struggles. Like many institutions, the Agency's legacy recordkeeping system developed over time in a piecemeal manner – meaning the system is not integrated, hardwired, and reliant on custom applications.

In consideration of the speed at which advancements relating to technology and security emerge, the ever evolving threat of bad actors, and the challenges the Agency has experienced maintaining and managing its recordkeeping system, two years ago, the Board and FRTIB launched the FRTIB's Plan Operations Modernization Portfolio (POMP). POMP will consolidate the FRTIB's support contracts and shift the FRTIB's role toward contract surveillance and out of the integration, ownership, and development roles. The first phase of this procurement is underway (a preliminary requirements document was posted on Fed Biz Ops in June 2018), and the Agency anticipates that the contract transforming the TSP's recordkeeping will be awarded in approximately 18 months.

Regarding EBSA's Legal Authority over the Board

The OIG suggests that the Department of Labor Employee Benefits Security Administration (EBSA) lacks sufficient legal authority over the Board, and, as a result, audit findings have not been addressed in a timely manner. As discussed above, the FRTIB has addressed risks associated with audit findings with both a short-term and long-term, strategic approach. Additionally, the Agency views EBSA's current authority as appropriate and effective, particularly when accounting for the unique status of the FRTIB and TSP. Further, the Agency contends that augmenting EBSA's authority to include injunctive relief may raise inherent conflicts for the Federal government (specifically the Department of Justice) and potentially negative consequences for the TSP.

When it created the TSP, Congress recognized that the plan would grow in size and become a potential magnet for external pressure. As noted in the conference report that accompanied the final version of FERSA:

> A great deal of concern was raised about the possibility of political manipulation of large pools of thrift plan money. This legislation was designed to preclude that possibility. Concerns over the specter of political involvement in the thrift plan management seem to focus on two distinct

> issues. One, the Board, composed of Presidential appointees, could be susceptible to pressure from an Administration. Two, the Congress might be tempted to use the large pool of thrift money for political purposes. Neither case would be likely to occur given present legal and constitutional constraints.

H.R. Conference Report No. 99-606, at 136 (1986), reprinted in 1986 U.S.C.C.A.N. 1508, 1519.

As a result of these concerns, Congress ensured that the fiduciaries of the FRTIB, which include the five Board members and the Executive Director, are subject to the same strict legal standards found in ERISA. 5 U.S.C. § 8477. Specifically, the fiduciaries are legally responsible for operating the TSP solely in the interest of its participants and beneficiaries, in accordance with stringent fiduciary principles, and may be sued for breach of these duties by participants, beneficiaries, and even co-fiduciaries. Moreover, to further illustrate its separation from the political process, Congress specified that the Agency's Executive Director could only be removed by a consensus of four of the five Board Members, and only for good cause shown.

Though Congress intentionally shielded the FRTIB from political interference, it also created a robust structure of oversight and accountability. Congress provided EBSA with a potentially limitless performance audit program (and EBSA has exercised that authority through a large increase in the number of TSP audits it conducts every year), it authorized DOL to bring suit against TSP fiduciaries, such as the investment manager, and it authorized DOL to promulgate certain TSP-related regulations, including those relating to the allocation of fiduciary duty. As has been the case from the Agency's inception, EBSA's audit reports are discussed at Board meetings and EBSA has frequent, direct access to both the Board and FRTIB management.

Additionally, FERSA requires that the Executive Director engage an independent qualified public accountant to perform an annual financial statement audit, which is also discussed publicly at the Agency's Board meetings. As mentioned, in 2014, the Agency took steps to develop its own mechanisms for internal oversight. It established an Office of Enterprise Risk Management, headed by one of the first Federal Chief Risk Officers. The Agency also added Internal Auditor-In-Charge, who conducts an annual internal audit program and reports directly to the Board. Most recently, the Board continued its efforts to enhance its oversight and insight into Agency operations by approving the creation of an Independent Verification and Validation (IV&V) function. Through the IV&V, the Board receives an independent (external) assessment as to the status of closed audit findings. Further, the FRTIB undergoes an annual FISMA audit, the results of which are provided to the Department of Homeland Security, Congress, the Office of Management and Budget, and are ultimately available to the public. Finally, the Agency is subject to audits and program reviews from entities such as the U.S. Government Accountability Office (GAO), Office of Government Ethics, the Internal Revenue Service, and the Office of Personnel Management.

What the OIG report suggests is that this framework of oversight is not enough. It suggests that DOL should have a role beyond that which it already has under FERSA. It states that it should have the authority to seek injunctive relief against the TSP fiduciaries, as it does with private sector plans. Though injunctive relief could take many possible forms, research indicates that EBSA has used this authority largely to remove trustees of private sector plans for violations of ERISA or for breach of fiduciary duties.

As a preliminary matter, the FRTIB believes that equating the regulation of a governmental/Federal plan to that of a private sector plan is misplaced. Some of the most basic challenges arising in private sector plans are simply not a possibility within TSP operations. For example, the TSP is not sponsored by an employer whose loyalty to plan participants inherently conflicts with an employer's profits. In addition, the investment line-up of the TSP is determined by Congress, not the fiduciaries, and FRTIB fiduciaries cannot shape the TSP's investment choices to benefit the FRTIB, themselves, or the Federal Government which is the plan sponsor. It should also be noted that state and local government plans are exempt from EBSA regulation.

Additionally, as DOL itself testified in 1987, fiduciaries in private sector plans who are subject to EBSA enforcement mechanisms are indemnified by the plan sponsor. Because of its size, it is impossible for the U.S. Government to provide for an analogous indemnification for the fiduciaries of the TSP. For this reason, in 1987, the Board of the FRTIB expressed concern about continuing in its role when provisions allowing for EBSA enforcement were originally included in FERSA.

Further, it is ultimately the Board's legal responsibility to ingest feedback from the multitude of bodies which support the oversight of the TSP and to act in accordance with its fiduciary obligation to address the issues identified. Suggesting that an agency outside the FRTIB should have the ability to compel or prevent Agency action both oversimplifies the root cause behind the audit findings at issue, and potentially compromises the fundamental principles established by Congress to insulate the FRTIB from the reach of agencies that are tied to political processes.

Finally, the Agency is concerned that this potential legislative proposal could create challenges for the Department of Justice and, by extension, the interest of the TSP participants and beneficiaries. Per FERSA, the Attorney General is responsible for handling litigation against the TSP. Should litigation arise regarding an EBSA-imposed injunction, the Attorney General would represent a Federal agency that is independent from the Executive Branch (FRTIB) against a Federal agency that falls squarely under the authority of the Executive Branch (DOL). As the Attorney General's mission is to represent the common interest of the Executive Branch, the Attorney General would have a conflict of interest which could potentially harm the interest of the TSP.

7

We appreciate the opportunity to comment and the interest of the Department of Labor, Office of Inspector General in the operations of the Thrift Savings Plan.

Sincerely,

Chairman Michael Kennedy,

Board Member Dana K. Bilyeu,

Board Member Ron McCray,

Board Member David A. Jones,

Board Member William Jasien,

and

Ravindra Deo, Executive Director

8

APPENDIX D: ACKNOWLEDGEMENTS

The audit team included:

Nicholas Christopher, Audit Director
Jason Jelen, Audit Manager
Fernando Paredes, Audit Manager
Richard Donna Jr., Auditor
Timothy Kerschen, Auditor
Lewis Leung, Auditor

REPORT FRAUD, WASTE, OR ABUSE
TO THE DEPARTMENT OF LABOR

Online
http://www.oig.dol.gov/hotline.htm

Email
hotline@oig.dol.gov

Telephone
(800) 347-3756 or (202) 693-6999

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Room S-5506
Washington, DC 20210