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

May 15, 2015

The Honorable Ronald Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson:

This letter is in response to your letter of May 6, 2015, regarding the information security program at the Federal Retirement Thrift Investment Board (FRTIB), the agency charged with administering the Thrift Savings Plan (TSP). I appreciate this opportunity to share with you information about the FRTIB's efforts to continually improve in this area.

The TSP is a retirement savings plan for Federal employees; it is similar to the 401(k) plans offered by many private employers. As of April 2015, TSP assets totaled approximately $454.0 billion and retirement savings accounts were being maintained for more than 4.7 million TSP participants. The Board members and the Executive Director are fiduciaries, charged by law with acting solely in the interest of the participants and beneficiaries. As such, we take our responsibilities to establish and maintain an information security program very seriously.

As you note in your letter, in April of 2012, a cyber attack on a former FRTIB contractor was discovered. While the Agency had undertaken a significant number of changes in our information technology infrastructure in the years prior, we have accelerated our pace of enhancements over the past three years.

I will start with a high level overview of our most significant organization developments in this area. In 2012, we established Office of Enterprise Risk Management (OERM), which consists of the internal controls group, the anti-fraud group, the risk management group, and the internal audit group. This Office of 15 people did not previously exist and each of these employees is now dedicated to helping the FRTIB measure and manage risk. Also in 2012, within the Office of the Chief Technology Officer, we established a separate Information Assurance Division, led by a CISO and supported by 6 Information System Security Officers (ISSO). Working with our current contractor, the FRTIB has deployed a Security Operations Center (SOC) and a Network Operations Center (NOC) to monitor and assess IT security risks to the organization. In total, our staff that is full-time dedicated to risk management or information security increased significantly.

These new personnel, and activities that they undertake, have significantly improved our IT security capabilities and compliance with FISMA. In furtherance of our activities under FISMA, we defined and implemented an Enterprise Information Security & Risk Management (EISRM) program and nineteen associated information security policies. In accordance with these new EIRSM policies we reviewed and updated our system boundary delineation, which led us to designate 19 separate systems. We initiated assessment and authorization (A&A) activities of each system and, as of today, 14 of these 19 A&As are completed. We will conclude A&A work on the remaining 5 systems by December 2015.

I would note that the concerns that you cite in your letter are largely drawn from an article about our April 20, 2015, Board meeting. As can happen with press articles, the entirety of information that was discussed during the meeting was not referenced. I would like to provide you with a more complete picture of the conversation at our April Board meeting, which is when we regularly hear from our auditors. The Board has two statutory audit requirements: an annual audit of the TSP financial statements, as well as performance audits performed by the Employee Benefits Security Administration (EBSA) at the Department of Labor (DoL). EBSA contracts with KPMG to perform these audits.

Our financial auditor is a qualified public accountant and is currently CliftonLarsonAllen (CLA). CLA provided its unmodified (clean) audit opinion regarding the TSP calendar year 2014 financial statements at our April meeting. CLA also audits internal controls that could impact our financial statements. As such, CLA found one significant deficiency and three other management letter comments. The significant deficiency was in system authorizations, which was a carry-over from the previous year. CLA's engagement partner on the audit made these comments:

> When we were engaged, and obviously through today, we had several deficiencies in terms of internal control. Many related to IT. And I'll just say that as progress forward, it's been really impressive to see…So, you know, great job from both the Board making it a priority and then obviously management for addressing those. So I did want to at least point that out, significant progress.

After a general discussion of audit findings and DoL's desire to perform credentialed penetration testing, Mr. Dingwall, the Chief Accountant at EBSA, commented, "We know the Board is committed to resolving all of this. We have never, ever questioned the Board's views on any of this." In addition, Mr. Dingwall reiterated several times his desire to move forward quickly with the penetration testing. Those comments gave rise to the article you cite.

It is worth clarifying that the FRTIB has never taken the position that DoL auditors were not permitted to conduct network penetration testing. The comments made at our April Board meeting were made as we were working with DoL and KPMG to ensure that the FRTIB had the proper legal and other safeguards in place prior to allowing anyone such sensitive access to its systems, as that is the obligation the FRTIB has to our participants. These "rules of engagement" are standard practice before engaging in

penetration testing. A potential scenario that must be addressed with extreme caution and forethought is when the tester, having gained access to a TSP information system, may be able to alter data about our participants in our live production environment, which is used nightly to update account values and information. It is essential, therefore, that we fully understand any impact that the penetration testing could have on participant account data and not permit that data to be compromised.

Mr. Dingwall also commented that the DoL performance audit program is a "money-driven" audit program. He pointed out that "(w)e can only plan to do audits based on the money that we have." I then commented:

> So I'll start with the idea and start from the comments that Ian made, is there is no disagreement. We absolutely – we run the largest defined contribution plan in the world. We fully embrace a robust audit program, which is exactly what we have. What we—the issue here is scheduling, as Ian mentioned they typically run through an audit schedule over a three-year cycle. This year we're doing a three-year audit cycle in one year. It's simply about resources.

To illustrate the scheduling challenges being faced this year by the FRTIB in responding the DoL's audit program, below is a chart outlining the last ten years of DoL audits of the FRTIB. As you can see, we are experiencing a significant increase in audits. While we welcome the audits, which will yield benefits for our participants, the very uneven nature of the number of audits makes it extremely difficult for FRTIB staff to respond. We are staffed to respond to four to five audits per year, not sixteen per year. However, due to the uncertainty of the budget process, EBSA unable to assure us that they will be able to maintain higher number of audits, which makes it imprudent for FRTIB to hire additional staff to support that level of audits.

Year	Number of TSP Performance Audits Performed by EBSA
2015	16
2014	2
2013	9
2012	2
2011	5
2010	2
2009	4
2008	4
2007	4
2006	4

I hope I have provided a more complete picture of the discussion at our April Board meeting. The responses to your specific questions are below. Per your request, we will be providing the referenced audits and reports in electronic format. We are providing two disks. The first contains this letter and information that is otherwise publicly available. The second disk contains information that is sensitive and should be treated

with appropriate care and controls. The second disk is encrypted and we will provide your staff with the key in a separate communication.

1. Has your agency undergone any assessments, audits, or independent reviews of its cybersecurity posture, including the assessments required under FISMA? If so, please include any reports associated with those assessments, audits, and reviews with your response.

Yes. Fifteen audits involving the FRTIB's cybersecurity posture have been conducted by CLA, EBSA/KPMG and GAO. Since 2012, FRTIB has committed substantial resources, people and technology to establishing and implementing an Enterprise-wide Information Security/Information Assurance Program. The initiative has both tactical and strategic components resulting in capabilities that address a range of requirements and issues, including addressing and closing open audit findings. For example:

- Third party commercial scanning commenced in November 2013.
- Cyber hygiene scanning commenced through the Department of Homeland Security (DHS)/ National Protection and Programs Directorate (NPPD) Federal Network Resiliency Team in January of 2015.
- Fourteen Assessments and Authorizations (A&As) have been completed on FRTIB Systems that followed National Institute of Standards and Technology (NIST) 300-37 Rev. 1.; five additional A&As are underway and will be completed by December 31, 2015.

2. What are your plans to work with auditors at the Department of Labor to ensure the Board is building an effective and robust security program?

The FRTIB has an excellent long-standing working relationship with DoL/EBSA and their auditors (KPMG). We will continue our efforts to maintain this strong relationship and in light of the increased audit activity in FY 2015 have implemented additional measures to strengthen the audit coordination activities:

- Increase the frequency of status calls from a monthly to a weekly basis to discuss any issues related to ongoing audits and the scheduled audit activity. The weekly meetings are attended by senior staff from all offices that are subject to these audits. To give you a sense of our involvement, during January through March, we have responded to over 350 requests for information and held over 60 meetings for just two recently completed Information Technology (IT) audits.
- OERM has dedicated staff members who act as the primary liaison with DoL/EBSA. In addition, our Office of Technology Services (OTS) has also allocated staff to support OERM given that the majority of audits in FY 2015 are in the IT arena.
- We have also recently established an Internal Audit Division in OERM and it is our intent to have our internal auditors work closely with the DoL/EBSA team to complement and augment the audit activities that will result in streamlining the scope of the overall annual audit effort.

3. Why didn't the Board comply with the reporting requirements under FISMA?

The FRTIB did report as required. The FRTIB submitted an FY 2014 Report to OMB, which was accepted and approved by OMB in January 2015.

4. How do you plan to work with OMB to come into compliance with FISMA?

The Agency follows FISMA. As noted above, the FRTIB duly filed its FISMA report with OMB for 2014, which OMB acknowledged. That report contained our responses to all of the questions required in the report. In some cases, the questions did not pertain to the FRTIB, as they were only applicable to particular categories of Executive Branch agencies. In other cases, they related to matters concerning OMB budgetary or management requirements from which the Agency is exempt by statute for the reasons explained below. In all of these cases, the Agency responded "Not Applicable." We note that the Agency has received no communication from OMB to indicate that OMB believes it is not in compliance. The Agency is audited against the NIST standards and guidance under FISMA.

We note that the FRTIB is funded solely by participant money and does not receive appropriated funds; therefore, as provided for in our statute, our budget is not subject to review or approval by either Congress or the President – but only by the named fiduciaries, who have a statutory obligation to make decisions solely in the interest of the participants and beneficiaries of the Thrift Saving Plan. Congress therefore determined in enacting our authorizing statute, the Federal Employees Retirement System Act of 1986 (FERSA), that it would be inappropriate for the President or Congress to tell the FRTIB fiduciaries how to spend participant money. For that reason, all guidance issued by OMB must be reviewed by the Agency's Executive Director to ensure that following it would further the interest of the TSP's participants and beneficiaries.

5. How does the Board work with the Department of Homeland Security to take advantage of its resources, including the Continuous Diagnostics and Mitigation program, the protections of the EINSTEIN program, and services at the United States Computer Emergency Readiness Team? What other programs and services has the Board utilized to assess and improve its information security, such as those offered by other Federal agencies of private sector firms, if any?

Currently, the FRTIB collaborates with the DHS in the area of cyber hygiene scanning through the DHS/NPPD Federal Network Resiliency Team and US-CERT through the G-FIRST Portal to share cyber security information. With regard to DHS's specific Continuous Diagnostics and Mitigation (CDM) Program, we do not subscribe to CDM's centralized monitoring methods. However, we have deployed several commercial tools with similar network monitoring and intrusion detection capabilities. These tools have capabilities that are similar to DHS's Einstein capabilities and have been used to operationalize the SOC and NOC referenced earlier. Finally, the FRTIB Chief Information Security Officer is a member of the Federal Small Agency CISO Advisory

Council, and also the Financial Services Information Sharing and Analysis Center (FS-ISAC) from whom the CISO receives information and threat notifications.

I hope this information is helpful to you. As requested in your letter, we have scheduled the meeting with your staff and will be happy to answer any other questions they might have. I thank you for your interest in the Thrift Savings Plan.

Sincerely,

Greg Long

Enclosure