**STATEMENT OF GREGORY T. LONG EXECUTIVE DIRECTOR FEDERAL RETIREMENT THRIFT INVESTMENT BOARD BEFORE THE SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE AND THE DISTRICT OF COLUMBIA JULY 31, 2012**

Good morning, Chairman Akaka and members of the Subcommittee, my name is Greg Long and I am the Executive Director of the Federal Retirement Thrift Investment Board (FRTIB). The five members of the Board and I serve as the fiduciaries of the Thrift Saving Plan (TSP). As fiduciaries, the law directs that we act solely in the interest of the TSP's participants and beneficiaries and exclusively for the purpose of providing them with benefits. Because of this fiduciary duty, in the Federal Employees' Retirement System Act (FERSA), Congress afforded the FRTIB significant independence. The FRTIB does not receive appropriated funds for its operations. We are funded through participant monies and our budget is not subject to review or approval by Congress or the President.

The TSP is the largest defined contribution retirement plan in the world. Individual accounts are maintained for more than 4.5 million Federal and Postal employees, members of the uniformed services, retirees, and spousal beneficiaries. As of June 30, 2012, the TSP held approximately $313 billion in retirement savings.

I have been asked to discuss a number of issues, including the cyber attack that resulted in the unauthorized access of the personally identifiable information of roughly 123,000 TSP participants and payees. In July of 2011, a desktop computer used by an employee of Serco, Inc. was subjected to a sophisticated cyber attack. Serco is a contractor which assists with TSP record keeping – keeping track of participant accounts and funds. Neither Serco nor the FRTIB was aware of the attack at the time it occurred.

In April 2012, the Federal Bureau of Investigation (FBI) notified Serco that the FBI had discovered data that appeared to be stolen from Serco. On April 10, 2012, Serco notified the FRTIB of the cyber attack. On that day, Serco told the FRTIB that Serco's system had been compromised, but Serco did not yet have knowledge of whether any data belonging to FRTIB had been accessed. The FRTIB and Serco immediately acted to isolate and contain the personal computer that was the suspected source of the data.

On April 13, after a combined investigation, the FRTIB and Serco determined that data belonging to FRTIB, including personally identifiable information of TSP participants and payees, had been compromised. As required by the Federal Information Security Management Act (FISMA), within one hour of the discovery, the FRTIB notified US CERT at the Department of Homeland Security. At that time, however, the FRTIB did not yet know which participants and payees were affected by the incident.

The FRTIB and Serco worked together to analyze numerous files and, by May 4, had compiled an unverified list of Social Security numbers and, in some instances, other information (e.g., TSP account numbers) that had been compromised. No names were associated with the majority of these Social Security numbers. On May 8, the FRTIB produced a file that had been verified against the TSP participant database.

On May 20, an independent verification and validation (IV&V) concluded that the various files that had been accessed from the Serco computer had been completely and correctly analyzed to accurately capture the affected population.

On May 25, five days after the final, complete list was produced, the FRTIB notified affected participants and other stakeholders about the cyber attack. The FRTIB sent letters to every affected participant notifying them of the cyber attack, the fact that certain personally identifiable information had been accessed, and offering them one year of free identity theft consultation, restoration, and continuous credit monitoring.

I would like to emphasize the fact that this cyber attack was made on our contractor's network. Neither the FRTIB's network nor the TSP participant website www.tsp.gov was affected. I would also like to emphasize that we have no reason to believe that this data has been misused.

Nonetheless, we undertook a comprehensive review of our systems to ensure that they had not been affected. Serco also took a variety of steps to address the cyber attack. The immediate response included initiating scans and sweeps of devices, deploying additional event detection devices, and delivering awareness training to Serco employees. Serco then conducted a forensic analysis on the target hard drive to determine whether malware was present, coordinated a review and feedback from the FBI on the hard drive, and had an external forensics review of the hard drive. Serco next completed an information technology assessment and completed its scanning of its computer systems.

Operationally, we have over a long period of time provided specific guidance to Serco and worked with them to implement controls and processes to protect FRTIB enterprise-wide hardware, software, and information assets. Examples of these controls and processes include standard security configurations for server, database, and network platforms, defining and implementing requirements for firewall security practices, and implementing requirements for the control of ports on devices at our call centers.

As the fiduciary for a plan charged with protecting the retirement savings of more than 4.5 million participants and beneficiaries, data security and privacy protection are priorities for me and the employees of the FRTIB. Over the past decade, the FRTIB has undertaken a significant number of changes in both its infrastructure and the features offered through the TSP. The FRTIB transitioned from the Department of Agriculture's National Finance Center to private contractor support for its record keeping operations. That transition was completed in 2006. From 2008 through 2011, the FRTIB engaged in a substantial information technology (IT) modernization effort, which included a change in data centers. The FRTIB has been keenly focused on upgrading its infrastructure and security during this time. We have created new call centers, instituted a back-up data center to ensure continuity of operations, updated our record keeping software, purchased a new mainframe, developed disaster recovery plans and testing for those recovery plans, mainframe and distributed systems, modernized the network, including full redundancy and high availability, initiated a virtual infrastructure, and deployed a new www.tsp.gov website. These efforts speak to major IT or IT support activities that provided technical controls to improve our IT security posture.

In addition to these infrastructure enhancements, over the past decade, in many cases in response to legislation, the FRTIB has successfully added new services for its participants and beneficiaries: daily valuation of participant accounts; catch-up contributions for participants 50 years of age and older; life cycle funds; immediate contributions for newly-hired Federal employees; auto-enrollment for newly hired Federal employees; beneficiary accounts for spouses of deceased TSP participants; annual participant statements; accounts for uniformed services; and, most recently in May of 2012, a Roth TSP option, allowing for after-tax contributions to the TSP.

Many of these changes added significant complexity to the Plan. The infrastructure changes listed above were necessary, in many cases, to allow the FRTIB to offer these new services to TSP participants. The need to implement these new funds and services, in large part, mandated how we assigned our personnel and allocated funding. For example, rolling out the Roth TSP initiative was a two-year project that required staffing from every office within the Agency. The complexity of the programming necessitated that we delay other programming changes to ensure a stable platform to allow for the success of Roth. We also had to revise virtually every form, notice, and brochure that we have – more than 145 – to reflect the new Roth option. As a result of this careful planning and prioritization of effort, the Roth TSP rollout was successful.

I was also asked to address the Agency's compliance with the Privacy Act and the E-Government Act. The FRTIB complies with the Privacy Act and has implemented the security controls and incident prevention processes, consistent with the data and systems held by our agency, as spelled out in FISMA. Because we are not covered by the Transportation, Treasury, Independent Agencies, & General Appropriations Act of 2005, the FRTIB is not required to appoint a Chief Privacy Officer, and, therefore, has not. The Agency's Office of General Counsel is responsible for ensuring compliance with the Privacy Act.

While the FRTIB has security controls in place, completing all of the documentation and accreditation that FISMA requires is an on-going area of focus for our Agency. I recognize that a comprehensive IT security management program is of paramount importance to the Board and we are making strides toward that goal. In September 2011, the FRTIB issued an Enterprise Information Security and Risk Management **(**EISRM**)** directive. Its purpose is to ensure that the FRTIB information systems operate with an acceptable level of risk. Its scope is all information resources used or operated by the Agency, an Agency contractor or any other organization on behalf of the Agency to access, collect, create, record, process, transmit, store, retrieve, display, print, or otherwise disseminate information owned or maintained by the Agency. The EISRM program has four major components: 1) key roles and responsibilities; 2) a risk management framework; 3) policies and controls; and 4) standards, procedures, and guidance.

As part of the continued implementation of the EISRM program, on June 29, 2012, I approved policies covering 18 families of management, operational, and technical security controls. To ensure that our privacy and data security policies are appropriate, I have commissioned a "Tiger Team" to develop a plan to improve the security posture of information systems that contain Agency information. The Tiger Team has four main objectives:

- Assess the current state of implementation of information security controls against FRTIB Enterprise Information Security and Risk Management (EISRM) requirements;
- Assess the current state of FRTIB's application and infrastructure security architecture and data;
- Assess the current state of outstanding findings; and then
- Develop a plan to address any identified gaps. Where practical, the team will address gaps within their respective areas in compliance with the EISRM requirements.

I regret to say that the FRTIB did not have a breach notification plan in place prior to 2012. This was due to a lack of resources to develop the plan. As noted above, the past decade has been a time of dramatic expansion for the Agency, in the number of participants, the dollars invested in the TSP and the services provided to our participants and beneficiaries. This growth taxed the Agency's ability to complete all that needed to be done. During the FRTIB response to the cyber attack, I placed our General Counsel, in charge of the breach response team. In turn, the General Counsel instructed the team to use the May 22, 2007 OMB guidance as a roadmap for the team working to respond to the cyber attack. The team found the OMB guidance very useful and information in the guidance helped expedite the FRTIB response to the attack. I have since signed the FRTIB's breach notification plan on June 14, 2012.

As for instances of inter-agency sharing of knowledge, the FRTIB shares security and privacy materials with other agencies on an ad hoc basis. It also participates in groups like the Small Agency General Counsel consortium, the CIO Small Agency Council and the Chief Information Security Official (CISO) Advisory Council. We also participate in non-Federal associations, such as the National Association of Public Pension Plan Attorneys, in order to learn about other government retirement plans' best practices in areas like security and privacy.

I was asked whether the FRTIB has any recommendations to improve privacy laws. My suggestion is not directed at the Privacy Act, per se, but at a problem specific to the FRTIB. Currently, FERSA does not contain a statute of limitations for judicial review of a claim for benefits brought by a TSP participant or beneficiary. This indefinite exposure to potential litigation over benefits forces the TSP to retain records of benefits paid for an unlimited period of time, even after a participant's account balance has been completely disbursed and he or she is no longer a participant. The absence of a statute of limitations, therefore, results in an extraordinary record retention burden, which increases the data potentially available to be accessed through a cyber attack or other data breach.

We, therefore, suggest that FERSA be amended to create a five year statute of limitations on judicial review of a claim for benefits. This would be longer than the statute of limitations available to virtually all plans covered by the Employee Retirement Income Security Act of 1974 (ERISA). Under ERISA, courts have ruled that as little as 90 days, 3 years and 39 months were reasonable statutes of limitations for private sector employee benefit plans.

Mr. Chairman and members of the Subcommittee, helping people retire with dignity is what drives the employees of the FRTIB. Congress made it clear that we are a unique agency with the mission of administering the TSP solely in the interest of the participants and beneficiaries. We take this very seriously. I deeply regret the cyber attack and the concern that it caused our participants. I want to take this opportunity to assure all of our participants and beneficiaries that we will continue to pursue all new avenues of data and computer security to ensure the safety and security of their personal data and their retirement funds.