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

GREGORY T. LONG
Executive Director

June 4, 2012

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
Washington, D.C. 20510-6250

Dear Senator Collins:

This is in response to your letter of May 29 regarding the cyber attack suffered by Serco Inc., a service provider to the Thrift Savings Plan (TSP). I appreciate your interest in this event. Below are the answers to your questions.

1. I understand that your initial step upon notification of the breach was to analyze the breached data files in order to identify affected TSP participants and the specific data exposed for those participants. On what date was the identity of the affected TSP participants first assessed?

On April 10, 2012, Serco Inc. notified the Federal Retirement Thrift Investment Board (FRTIB) of a cyber attack. In that notification, Serco explained that its system had been compromised, but that it did not yet have knowledge of whether any data belonging to FRTIB was accessed. The FRTIB and Serco immediately acted to isolate and contain the suspected source of the data. After a combined investigation, on April 13, the FRTIB and Serco determined that data belonging to FRTIB, including personally identifiable information of TSP participants, had been compromised. Within one hour of the discovery, the FRTIB notified US CERT as required by the Federal Information Security Management Act. At that time, however, the FRTIB did not yet know which participants were affected by the incident.

The FRTIB and Serco worked together to analyze the various files to determine what types of information they contained. As a result of this extensive analysis, by May 4, FRTIB and Serco had compiled an unverified list of Social Security numbers and, in some instances, other information (e.g., TSP account number) that had been compromised. There were no names associated with the majority of these Social Security numbers. On May 8, the FRTIB produced a file that was verified against our TSP participant database. On May 20, the FRTIB received an independent verification and validation (IV&V) confirming that the

various files that had been accessed had been completely and correctly analyzed to accurately capture the affected population.

2. Please provide samples of the notification letters sent to TSP participants and other affected individuals.

The letters sent to affected individuals are attached. There are two versions of the letter, reflecting the two groups of affected individuals. The first letter went to group A, whose members' names, addresses, and Social Security numbers were accessed. In less than half of this group, financial account numbers and routing numbers were also accessed. The second letter went to group B, whose members' had their Social Security number and some TSP-related information, such as a payment amount, accessed. The information accessed in group B did not include any names or addresses of TSP participants or payees.

We would respectfully request that these letters not be made public. They are intended for the affected participants. We are trying to avoid having the more than four million unaffected individuals contact the outside vendor selected to provide a suite of services to support the affected individuals. The letters contain information pertinent to assisting the affected individuals and any wider distribution could affect the level of service available to them. If the unaffected individuals have questions, they can contact our regular call centers, as they are already doing.

3. I understand that FRTIB was notified of the attack on April 11, 2012 by the FBI, yet the Senate Committee of jurisdiction was not notified until May 25, 2012. Why was Congress not immediately notified in April, when FRTIB learned of the attack, and then subsequently kept apprised as more details of the incident became available?

The FRTIB was notified of the attack on April 10. (On a phone call on May 25, we provided your staff with the April 11 date. We misspoke and I apologize for that error.) At that time, however, the FRTIB was notified only that an incident had occurred; it did not have knowledge as to what data was accessed and which individuals were affected. It was critical that the FRTIB understand the scope of the incident prior to briefing Congress, such that it could provide a full and comprehensive explanation of the incident.

4. Will FRTIB be modifying its Congressional notification process so as to prevent in the future the type of delay in briefing Congress that occurred in this case?

We will review our incident handling procedures to determine when Congressional notifications should be made.

I hope this information is helpful to you. If your staff has any additional questions, they may call Kim Weaver at 202-942-1641.

Sincerely,

Gregory T. Long