

JOSEPH I. LIEBERMAN, CONNECTICUT, CHAIRMAN

CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
THOMAS R. CARPER, DELAWARE
MARK L. PRYOR, ARKANSAS
MARY L. LANDRIEU, LOUISIANA
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
MARK BEGICH, ALASKA

SUSAN M. COLLINS, MAINE
TOM COBURN, OKLAHOMA
SCOTT P. BROWN, MASSACHUSETTS
JOHN MCCAIN, ARIZONA
RON JOHNSON, WISCONSIN
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JERRY MORAN, KANSAS

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510-6250

MICHAEL L. ALEXANDER, STAFF DIRECTOR
NICHOLAS A. ROSSI, MINORITY STAFF DIRECTOR

May 29, 2012

The Honorable Robert S. Mueller, III
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535

Dear Director Mueller:

On May 25, 2012, I was notified by the Federal Retirement Thrift Investment Board (FRTIB) of a sophisticated cyber attack on Serco, Inc., a third party service provider of the Thrift Savings Plan (TSP). As the Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, the committee of jurisdiction over federal workforce issues, including the FRTIB, and multi-agency efforts to prevent and respond to cybersecurity threats, I want to assess the process and timeframe whereby this attack was discovered and addressed.

According to the FRTIB, the attack occurred in July 2011 on a computer owned by Serco, Inc., a vendor used by FRTIB to support the TSP program. The breach resulted in the unauthorized access to personally identifiable information or financial information for approximately 123,000 TSP participants. The Federal Bureau of Investigation (FBI) reportedly only notified the FRTIB of the attack in April of this year, more than nine months after it occurred.

Please provide responses to the following questions by June 5, 2012:

- 1) When did the FBI first become aware of the attack?
- 2) Was the FBI the first federal entity to discover that an attack had occurred?
 - a. If so, how did the FBI discover the attack and the files of breached data?
 - b. If not, which agency was the first and under what circumstances?
- 3) What is the explanation for the delay, if any, between the time when the FBI became aware of the attack and its notification to the FRTIB?
- 4) Why did the FBI not simultaneously report the attack to Congress at the same time the FRTIB was notified?

The Honorable Robert S. Mueller, III
Page 2 of 2

For questions related to this matter, please have your staff contact [redacted] on my
staff at [redacted]

Sincerely,

A handwritten signature in black ink that reads "Susan M. Collins". The signature is written in a cursive, flowing style.

Susan M. Collins
Ranking Member

JOSEPH I. LIEBERMAN, CONNECTICUT, CHAIRMAN

CARL LEVIN, MICHIGAN
DANIEL K. AKAKA, HAWAII
THOMAS R. CARPER, DELAWARE
MARK L. PRYOR, ARKANSAS
MARY L. LANDRIEU, LOUISIANA
CLAIRE McCASKILL, MISSOURI
JON TESTER, MONTANA
MARK BEGICH, ALASKA

SUSAN M. COLLINS, MAINE
TOM COBURN, OKLAHOMA
SCOTT P. BROWN, MASSACHUSETTS
JOHN M. CAIN, ARIZONA
RON JOHNSON, WISCONSIN
ROB PORTMAN, OHIO
RAND PAUL, KENTUCKY
JERRY MORAN, KANSAS

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

MICHAEL L. ALEXANDER, STAFF DIRECTOR
NICHOLAS A. ROSSI, MINORITY STAFF DIRECTOR

May 29, 2012

Mr. Gregory T. Long
Executive Director
Federal Retirement Thrift Investment Board
77 K Street, NE
Washington, D.C. 20002

Dear Executive Director Long:

I appreciate your letter of May 25, 2012, on behalf of the Federal Retirement Thrift Investment Board (FRTIB), detailing the sophisticated cyber attack against Serco, Inc., a service provider of the Thrift Savings Plan (TSP). As the Ranking Member of the Senate Homeland Security and Governmental Affairs Committee, the Committee of jurisdiction over federal workforce issues, including the FRTIB, and multi-agency efforts to prevent and respond to cybersecurity threats, I want to assess the process and timeframe whereby this attack was discovered and addressed.

According to the details of your letter, the attack occurred in July 2011 on a computer owned by Serco, Inc., a vendor used by FRTIB to support the TSP program. The breach resulted in the unauthorized access to personally identifiable information or financial information for approximately 123,000 TSP participants. The Federal Bureau of Investigation (FBI) reportedly only notified the FRTIB of the attack in April of this year, more than nine months after it occurred.

Please provide responses to the following questions by June 5, 2012:

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

Mr. Gregory T. Long
Page 2 of 2

- 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?
- 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?

For questions related to this matter, please have your staff contact _____ ng on my

Sincerely,



Susan M. Collins
Ranking Member