Federal Managers Association

June 23, 2015

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

The Honorable Tom Carper, Ranking Member
Senate Homeland Security and
Governmental Affairs
442 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member Carper:

On behalf of the managers and supervisors serving our nation in the federal government and whose interests are represented by the Federal Managers Association (FMA), I am deeply concerned about the recent data breach at the Office of Personnel Management (OPM) that compromised the personally identifying information (PII) of current, separated, retired, and perspective federal employees. This breach has impacted the financial security of an estimated 18 million individuals, leaving them vulnerable to identity theft, weakened credit, and potential financial difficulties for years to come.

FMA is concerned that this data breach first occurred in December 2014, was not discovered until April 2015, and was not announced to the public until June. Furthermore, when FMA was first notified of the breach, OPM announced it affected only four million current and retired federal employees. However, it seems the scope and severity of the impact continues to grow. Now, it appears at least four times as many employees' PII were compromised and include separated and perspective federal employees. Additionally, security clearance information was breached, which also includes sensitive information of an employee's spouse and family members. As this problem continues to grow, it is clear that OPM's response and assistance thus far is inadequate. FMA members expressed frustration with CSID, the identity theft protection company OPM contracted to assist federal employees. FMA members note long wait times while trying to reach CSID over the phone, as well as concern about handling the matter of identity theft protection with a private sector company whose initial emails went to some federal agency and department's spam folders. I am also concerned about the "Health Data Claims Workhouse." This was established in 2010 to track the costs of the Federal Employee Health Benefits Program. In a November 2014 memo, OPM auditors expressed concern of its security. While this database is not yet live, the health information of current and federal employees, along with their dependents, cannot also be jeopardized.

Because of the severity of these events and the implications, FMA calls upon the Homleand Security and Governmental Affairs Committee and Congress to ensure those responsible at OPM are held accountable. This situation will not only cause Americans to reconsider employment with the federal government, but to question the abilities of OPM and its Information Technology (IT) leadership. Because of the extent of the breach and the ever-growing number of those affected, OPM must provide lifetime credit monitoring and fraud protection to all active, separated, retired and perspective federal employees and their families. The PII obtained through the breach can be used at any time, well beyond the 18 months of protection initially offered by OPM. It is also necessary for OPM to offer guidance on the use of on-the-job time and government resources used to address the breach without penalizing the affected employee.

Those impacted should not face reprimand while they try to fix problems caused by OPM. Additionally, FMA calls upon members of Congress to work with OPM to continually evaluate the situation and develop responsible strategies that not only react to this event, but also manage possible risks. As IT is ever evolving, it is imperative OPM work quickly, yet carefully, on this matter. OPM must build a secure IT infrastructure for all personnel data. While FMA understands that OPM faces constricted IT funding, this is not an excuse to allow such a lapse in security. It is OPM's obligation to protect this information.

FMA is disappointed this needless breach took place. OPM has a duty to current, separated, retired, and perspective federal employees to protect their PII. The federal government's greatest asset is its workforce. This security breach alienates our dedicated workers. OPM needs to safeguard its cyber security systems and fix the damage caused.

Thank you for your time and consideration of our views. Should you have any questions or concerns, please contact FMA's Government Affairs Director Greg Stanford at gstanford@fedmanagers.org or (703) 683-8700.

Sincerely,

Patricia J. Niehaus
National President

Cc: Members of the Senate Homeland Security and Governmental Affairs Committee