STATEMENT FOR THE RECORD

BY THE

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO

BEFORE THE

FINANCIAL SERVICES AND GENERAL GOVERNMENT SUBCOMMITTEE

SENATE COMMITTEE ON APPROPRIATIONS

REGARDING

OPM INFORMATION TECHNOLOGY SPENDING AND DATA SECURITY

June 23, 2015

Chairman Boozman, Ranking Member Coons, the American Federation of Government Employees, AFL-CIO (AFGE) which represents more than 670,000 federal employees, would like to thank the Subcommittee for holding this important hearing on the recent data breaches to the Office of Personnel Management's electronic employee data systems. Unfortunately, in the days since the breach was originally announced, the number of individuals who are or have been employed by the federal government, and potentially had their personal data hacked continues to increase. Very little substantive information has been shared with federal employees, despite AFGE's numerous requests for specific information in an effort to help those affected by the data breach. All individuals affected by the OPM data breach deserve

nothing less than a clear path forward that allows them to take immediate action to protect themselves from the misuse of their stolen personal information, successfully monitor their credit, and continue their work as federal employees with confidence that the necessary precautions will finally be taken to protect their personal data.

OPM must commit to answering the most basic of questions regarding the breach. The fact that OPM continues to refuse to answer simple questions about the dimensions of the breach have made the federal and DC government employees and retirees that AFGE represents deeply skeptical of any information coming from OPM. AFGE understands the sensitive nature of the current criminal investigation that is underway, however, there are some questions and issues that the agency has a moral responsibility to answer. For example, one question that still has not been adequately addressed by OPM is whether or not the data that was stolen can be linked to federal employees' bank accounts or direct deposit information. Federal employees deserve answers to all of their questions so they can take appropriate action.

Based on the information that OPM has provided, AFGE believes that the Central Personnel Data File was the targeted database, and the hackers are now in possession of all personnel data for every federal employee, every federal retiree, up to one million former federal employees, as well as similar data for their family members. We believe that hackers have every affected person's Social Security number(s), military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance, and

pension information; age, gender, race, union status, and more. In fact, at the House of Representatives Oversight and Government Reform hearing held on June 16, 2015, OPM Director Katherine Archuleta testified that federal employees' Social Security numbers were not encrypted, and thus were compromised. This is a cyber-security failure that is absolutely indefensible and outrageous. While OPM has informed federal employees that they will provide 18 months of credit monitoring and $1 million in liability insurance, AFGE believes that a mere 18 months of credit monitoring is entirely inadequate, either as compensation or protection from harm. Federal employees will suffer the consequences of the OPM data breach far longer than 18 months. In order to protect the personal data of the millions of individuals affected by the data breach from this point forward, OPM owes employees and their family members free lifetime credit monitoring and liability insurance that covers the entirety of any loss attributable to the breach. With the personal information of millions of people stolen, we cannot underestimate the long-term threats to federal employees' personal finances, credit, and physical safety.

AFGE also requests that OPM reconsider the decision to enter into contact with Winvale/CSID, a contractor given responsibility for answering affected employees' questions involving their stolen personal information. Based on our membership feedback, federal employees have not been able to speak with an actual person when they have questions. At the very least, the terms of the contract should have included guaranteed access to points of contact that can answer specific, personal questions that affected federal employees may have regarding the data breach. Federal employees who have been victimized by this breach deserve more than a

website that is difficult to navigate and call center contractors who do not know the answers to questions that go beyond a Frequently Asked Questions (FAQ) template. Those affected should have access to OPM employees who can respond to questions that are unique to their individual situations.

AFGE has also received numerous complaints from federal employees who describe their horrendous experience trying to access assistance from the contractor hired to perform credit monitoring. These complaints range from reports of the website constantly crashing to the information the contractor produces being inaccurate and out of date. A recent report on Federal News Radio noted, CSID is "…thought of as a company that helps others get on the General Services Administration (GSA) schedules, prepare proposals and the like, and their GSA schedules are for things such as lab equipment and IT software services, but there is nothing about credit monitoring, insurance or similar offerings…interestingly enough Winvales's website now says they provide credit monitoring services, but their profile on Bloomberg does not mention it at all."[1]

Accuracy and accessibility are the entirety of the service that Winvale/CSID is supposed to be providing. Thus far, federal employees have not been able to rely on the accuracy and accessibility of the credit monitoring services that have been provided. Yet, OPM gave

[1] Federal News Radio, *OPM Contract for Credit Monitoring Services Called Into Question*; http://www.federalnewsradio.com/520/3875508/OPM-contract-for-credit-monitoring-services-called-into-question

Winvale/CSID what appears to be a sole-source $20 million contract with four one-year renewal options. These issues need to be addressed and federal employees must have reliable credit monitoring services immediately.

AFGE has received disturbing reports that agencies are denying federal employees the time to deal with the impact of the data breach. At numerous agencies, employees are forbidden to use their government computers for any purpose other than a work assignment. They are forbidden from using their government computers to access personal emails or any non-work related websites for any reason. Federal employees dealing with this breach need to be able to visit their banks, Social Security offices, mortgage holder's offices, the management offices of their apartment complexes, and other creditors in order to deal with the fallout of having to change credit card and bank account information. Many agencies' computer firewalls prevent employees from being able to handle these kids of transactions online. Therefore, agencies should grant employees time during normal business hours to take preventive measures such as contacting their financial institutions and businesses as notification of their current situation. Additionally, it is extremely important that OPM ensure that agencies are meeting all of their collective bargaining obligations on procedures for accommodating employees trying to deal with the breach.

Federal employees trusted OPM with their personal information and the agency failed them. Their personal information was not properly guarded, and as a result, federal government

workers and their families must now live with the threat of having the most intimate details of their lives exposed, and illegally used against them. The government must now earn back the trust of these employees and future public servants. AFGE thanks the Subcommittee for holding this hearing.