AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO

J. David Cox, Sr.
National President

Eugene Hudson Jr.
National Secretary-Treasurer

Augusta Y. Thomas
National Vice President for
Women and Fair Practices

1j/00347559

June 18, 2015

The Honorable Katherine Archuleta
Director, U.S. Office of Personnel Management
1900 E Street, NW
Washington, DC

Dear Director Archuleta:

In the week since I last wrote to you, the impact of the breach of electronic files containing personal information of federal workers and retirees has only worsened. The number of people affected has risen to an estimated 14 million, a figure that must include some combination of contractors, military, postal employees and retirees, legislative and judicial branch employees and retirees, in addition to the active federal workforce. We also now know that information provided in the course of applying for security clearances and other background checks, information that cannot be changed the way a Social Security number or account number can be changed, was also hacked. Our members are bearing the brunt of the consequences, and they are angry and scared.

The fact that OPM continues to refuse to answer simple questions about the dimensions of the breach has made the federal and DC government employees and retirees our union represents deeply skeptical of any information coming out of your agency.
The most frequent complaint I have received – one which is well within your power to address – is the horrendous experience people have had trying to access assistance from the contractor you hired to perform credit monitoring, CSID. It appears that OPM spent a grand total of 36 hours in considering which contractor to hire. The decision to hire Winvale/CSID so quickly might not be raising such questions if it were known as an expert in credit monitoring. But, as a recent report on Federal News Radio noted:

> "[CSID is] thought of as a company that helps others get on the 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 Winvale's website now says they provide credit monitoring services, but their profile on Bloomberg doesn't mention it at all."

I cite this because I cannot count the number of AFGE members who have reported an abysmal experience with CSID. The website reportedly crashes constantly.

The "information" they produce is of the lowest quality; one member's report told him he was on a sex offenders list and he definitely is not, another received information using her maiden name even though she has been married 18 years and never worked for the executive branch under her maiden name, others have received various pieces of information they know for certain is false. Needless to say, the quality of their monitoring is low and federal employees cannot rely on its accuracy. Accuracy and accessibility are the entirety of the service CSID is supposed to be providing and they have failed miserably. Yet OPM gave them what appears to be a sole-source $20 million contract with four one-year renewal options.

This contractor is clearly incapable, and apparently unqualified for the task of monitoring the credit of the 14 million people affected by the government's failure to protect their personal data. They are making a disastrous situation worse, and their contract should be terminated for the failures that have already come to light. Their continued involvement is adding to the impact of the breach itself, and making those affected by the breach even less trustful that the government is capable of protecting their data or remediating the breach.

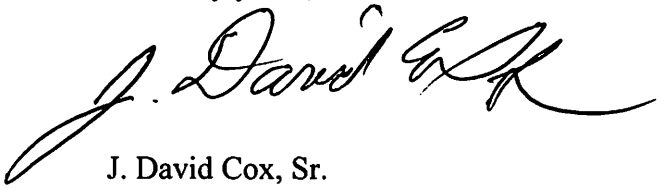
Our members are also disturbed by reports that agencies are denying federal employees time to deal with the impact of the breach. Employees need to be able to visit their banks, Social Security offices, mortgage holder's offices, the management office of their apartment complexes, and other creditors in order to deal with the fallout of having to change credit card and bank account information. Many agencies' computer firewalls – more secure than OPM's – prevent employees from being able to handle these kinds of transactions online. Thus, they need to be able to bargain over the right to spend duty time attending to these matters. I asked you to make sure that agencies were meeting all of their collective bargaining obligations on procedures for accommodating employees trying to deal with the breach. Yet, OPM has not responded. I ask you again to communicate with Human Resources representatives in all agencies to remind them of their bargaining obligations on this matter.

OPM has been invoking the criminal investigation as its explanation for why it has been so evasive in the face of questions about what databases were affected in the breach. But, there is one question weighing heavily on everyone's minds, and it's a question you have an absolute moral responsibility to answer right away. That question is: was direct deposit payroll information breached? Federal employees deserve to know the answer to that question and they deserve it immediately. It may be too late for some if this is something that is reluctantly acknowledged in a Hill hearing next week or next month.

Finally, I find it despicable that while OPM has been unwilling to address legitimate questions in the aftermath of the breach, your lawyers made sure that you immediately issued a disclaimer attempting to insulate the agency from liability. In the initial letter that went to many of those whose data the government failed to protect, OPM gave the impression that its primary concern was that those affected not sue the government. "[N]othing in this letter should be construed as OPM or the U.S. Government accepting liability for any of the matters covered by this letter or for any other purpose," the letter reads. "Any alleged issues of liability concerning OPM or the United States for the matters covered by this letter or for any other purpose are determined solely in conformance with appropriate Federal law." OPM should have admitted liability and accepted the consequences. That would have been the right thing to do.

I hope to hear from you soon on all of these issues relating to the data breach. I cannot emphasize enough how urgent these questions are to the 670,000 federal and DC government employees AFGE represents. They want information, and they want action. I look forward to your prompt response.

Sincerely yours,



J. David Cox, Sr.
National President