



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

The Director

October 27, 2015

Ms. Barbara Oswald
President
Federal Probation and Pretrial Officers Association (FPPOA)
United States Court House
75 Spring Street, S.W.
Atlanta GA, 30303

Dear Ms. Oswald:

Thank you for your letter regarding the discovery of intrusions on Office of Personnel Management (OPM) cyber systems which have affected the security of Federal employees' personal data. I have made addressing the cybersecurity incidents a top priority. I believe the security of Federal employees' personal data is of paramount importance, and I will do all I can to see it protected.

The root causes of the cyber incidents are subject to ongoing investigation by the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and our agency partners. During this investigation, we have and will continue to work diligently to determine exactly how these cyber intrusions happened and what additional steps are necessary to further our efforts to minimize the risk of future incursions. For example, through an ongoing review of the security of our IT systems, we have been able to make important security enhancements. OPM has identified 15 new steps to improve security and modernize its systems, including completing deployment of two-factor Strong Authentication for all users, expanding continuous monitoring of its systems, and hiring a new cybersecurity advisor.

At this time, there is no information to suggest misuse of the information that was taken from OPM's systems. However, we are continuing to work with our interagency partners to investigate and monitor this.

I encourage you to share with your members the resources available on OPM's cyber web site at <https://www.opm.gov/cybersecurity/>. All available information on the cybersecurity incidents can be found on this site. Any individual may subscribe to cybersecurity updates through an RSS feed or by signing up for email updates. In addition, we make available widgets and badges to embed on your website which allow you to direct individuals from your website to the OPM cybersecurity homepage. While individuals may sign up for cybersecurity updates directly on our website, I've directed my staff to add the FPPOA to email communications that are directed to national level employee groups providing notice of when updated information is posted on the cybersecurity website.

As you know, a vendor was recently selected for the background investigation cyber incident. Notifications to affected individuals began at the end of September and will continue on a rolling basis. As new information becomes available on the notification process, we will share this with you and other employee groups. In addition, the government has stated that it will continue to assess and evaluate whether additional coverage associated with this incident is appropriate.

Finally, I understand that peace of mind regarding information security is of the utmost importance. Considering the current global environment and overall increase in cybersecurity incidents in both the government and private sector, OPM is working with other agencies to develop longer-term recommendations regarding Federal employee identity protection regardless of whether they have been affected by these incidents.

Thank you for your letter. We appreciate your letter and are always receptive to input from our stakeholders.

Sincerely,

A handwritten signature in black ink, appearing to read "Beth F. Cobert", with a long horizontal line extending to the right.

Beth F. Cobert
Acting Director