UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

SEP 04 2015

Mr. Anthony M. Reardon
National President
National Treasury Employees Union (NTEU)
1750 H Street, N.W.
Washington, DC 20006

Dear Mr. Reardon:

Thank you for NTEU's letter regarding the incidents involving Office of Personnel Management (OPM) cyber systems which have affected the security of Federal employees' personal data. I share the concerns expressed in your letter and 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 undertake comprehensive efforts to see it protected.

I appreciate the questions that you and your members submitted and the challenges your members experienced in communicating with CSID, the company working with OPM to provide credit monitoring and theft identity insurance on the personnel records cybersecurity incident. As you and other stakeholders brought these challenges to our attention, my team worked with CSID to address and resolve them as soon as possible. NTEU's feedback was tremendously helpful in assisting us in not only responding to and improving our response to the personnel records cybersecurity incident, but in planning our response to the background investigation cybersecurity incident. I encourage you and other unions to continue providing us input as we move forward in addressing the background investigation cybersecurity incident.

In addition, NTEU has provided critical support to help us communicate to everybody affected by these incidents. We are always looking for opportunities to improve, so I appreciate NTEU's participation and great suggestions in a focus group that has assisted us in improving OPM's cyber web site at https://www.opm.gov/cybersecurity/. I look forward to working with you to continually enhance our communications with those affected. As you know, a vendor has recently been selected for the background investigation cybersecurity incident. Notifications to individuals impacted will begin by the end of September and continue on a rolling basis. Your assistance in keeping your members updated with current information in the coming weeks is valued.

I understand that peace of mind is of the utmost importance to all affected by these incidents. We appreciate and are reviewing all of your recommendations along with recommendations received from other impacted stakeholders and are exploring possible

implementation of ideas generated by those recommendations. For example, based on stakeholder feedback, OPM will be working with you and other Federal employee representatives in the coming months to develop a proposal for the types of credit monitoring and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

In addition to the efforts of our personnel, I want to assure you that OPM has made a serious financial commitment to cybersecurity capabilities. For Fiscal Years (FY) 2014 and 2015, we have committed nearly $67 million towards this effort. The President's Budget requests additional funds to support our current defensive measures, and we are working aggressively with OMB to get more resources for FY 2016 so that we can expedite our reforms. Additional significant resources will be needed and requested in future years to complete implementation.

Thank you for your letter. Please continue to reach out to me and my staff if you have any additional questions or concerns you would like to address.

Sincerely,

Beth F. Cobert
Acting Director