Colleen M. Kelley

National President

National Treasury Employees Union

Statement for the Record

For

House Committee on Oversight and Government Reform

"Office of Personnel Management: Data Breach"

June 16, 2015

1750 H Street, N.W. • Washington, D.C. 20006 • (202) 572-5500

Chairman Chaffetz, Ranking Member Cummings and distinguished members of the committee, I would like to thank you for the opportunity to share our members' perspectives on the recent announcements of agency data breaches impacting federal employees. I also commend you for holding this hearing and for devoting Committee attention to this extremely urgent issue. As President of the National Treasury Employees Union (NTEU), I have the honor of representing over 150,000 federal workers in 31 agencies.

Mr. Chairman, as you can imagine, there is great fear and outrage on the part of federal employees and retirees in the wake of the U.S. Office of Personnel Management's (OPM) announcements on June 4th, and more recently on June 12th, that millions of current and former federal employees may have had personally identifiable information (PII) compromised owing to breaches in databases containing various personnel records. Federal employees have had a difficult few years, facing multi-year pay freezes, furloughs, sequestration, and this type of exposure of personal information is the final straw. Such exposure is simply unacceptable.

It is important to note that these breaches follow wide-scale breaches of health insurance carriers earlier this year that included federal employees enrolled in several Federal Employees Health Benefits Program (FEHBP) plans, and multiple announcements of agency breaches in 2014 affecting background investigation and suitability records. Federal employees are required to provide significant amounts of personal data to their employing agencies, for general employment purposes, as well as for suitability and security clearance purposes. NTEU asks that this Committee act to ensure that agencies have the ability to immediately safeguard federal employees' information going forward. It should come as no surprise that employees are questioning the idea of submitting this type of detailed personal information to their agencies in the future, and are particularly pointing to the suitability and security clearance process, forms, and storage as areas that need to be immediately changed. We also ask the Committee to keep these breaches in mind as serious consideration of so-called "Continuous Evaluation" (CE) policies move forward in the security clearance and suitability reform areas, as well as for oversight purposes of the Administration's Insider Threat program.

At the moment, a principal outstanding concern for federal employees and retirees is the confusion about what exact type of individual data and information was in fact compromised, and of whom. In its first statements, OPM confirmed that a breach had potentially compromised names, dates and places of birth, Social Security numbers, and addresses. However, a multitude of media and other public statements followed maintaining that the exposure was far greater in number and the information even more intrusive—that the type of information that may have been accessed by outsiders involved information about family members, beneficiary information from employee benefit programs, bank accounts, data submitted and stored from Declarations of Federal Employment and Standard Forms 85 and 86[i] (among others) as part of routine background investigations, including detailed financial information and medical history, home addresses and other PII and data for annuitants. Last Friday evening, OPM informed NTEU that this was indeed the case—that the worst case scenario for individuals' privacy—be they federal civilians, military personnel, contractors or other individuals simply appearing in various documents, and our nation's national security has occurred. However, NTEU wants to be clear that which employees have been affected by this apparent wider, and more serious breach, is still

unknown to us and most importantly to the affected individuals. OPM's statement does not contain any information about whether individuals who do not possess security clearances, but who provide detailed information for suitability determinations and Standard Form 85 for critical non-sensitive positions, are also included in this breach. Not knowing whose data, and what exactly has been accessed and compromised, is creating widespread confusion and anxiety, on top of the general frustration of having one's personal information compromised be it from a foreign power, a thief, or otherwise ill-intended individual. Employees deserve to know what exact databases and information was hacked, and they need to be in a position to act, given the high level of risk they and their families are facing. It will also be important to address whether spouses, siblings, and other relatives, as well as former non-federal coworkers and acquaintances whose PII and contact information is provided, also had their information compromised, and whether there are plans to notify these members of the public, and to provide them with credit and identity protection services. We do not currently have any notification details to share with our members concerning the latest news from OPM, which again is unacceptable. I ask this Committee to ensure that the notification plan for all of these affected individuals is made public, and that it is put into action immediately.

OPM responded positively to NTEU's initial request that federal employees be allowed to use government computers in order to be able to contact CSID, the OPM-selected contractor, for credit monitoring purposes and to enroll in the identify theft protection services. Additionally, OPM also acted on NTEU's request to ensure access to government computers for those employees who do not regularly use computers on the job. While OPM has encouraged agencies to do these things, NTEU urges agency heads and this Committee to ensure that this access is indeed granted.

It is critically important for employees and retirees to be able to access and enroll in protection services as soon as possible. While NTEU is aware that OPM's contractor-provided notifications have begun to be emailed directly to active employees for the first breach, we are aware of various difficulties that may exist in reaching affected annuitants and former employees, whose mailing addresses are not actively maintained by employing agencies or OPM. Consideration needs to be given to setting up a process that allows individuals, particularly former employees and retirees, to affirmatively verify whether or not they were impacted by these breaches. Additionally, we are not yet clear whether all information has been announced for this breach.

A major concern for employees is the delay in notification from the time of the actual discovery of the breaches. It is imperative that affected individuals receive swift notification of any type of breach compromising PII and other information. Any delay in notification only increases the likelihood of individuals experiencing identity theft and suffering financially. As you know, Mr. Chairman, NTEU represents employees at U.S. Customs and Border Protection (CBP), and in September 2014, the Department of Homeland Security (DHS) became aware of a breach involving KeyPoint, a contractor providing background investigations and support. The overall volume and sensitive type of information that is provided by employees undergoing a background investigation—either as a new hire or for a periodic reinvestigation—is significant, and includes extremely personal details of employees, their family members, and of their friends, and even of their coworkers and acquaintances. However, it was not until June 4, 2015 that DHS

began providing and notifying CBP employees of their ability to enroll in credit monitoring and identity theft protection services. A nine month delay is simply unacceptable for all individuals involved. Moreover, two simultaneous, ongoing employee notification processes of compromised employee personnel records at CBP is leading, not surprisingly, to major confusion in the workplace.

Mr. Chairman, I also want to share that I have requested that, as we move forward, serious consideration be given by OPM to providing both the credit monitoring services and the identity theft protection services for an extended period of time beyond the current eighteen months. Additionally, we ask that OPM and DHS provide, at no cost, affected individuals with the option of setting up credit freezes with the credit reporting companies. Given how long these breaches may have gone undetected, and since the exact identities and data compromised is not yet known, NTEU believes these items to be prudent courses of action. As an example, following this year's Blue Cross Blue Shield health care breaches, carriers provided twenty-four months of protective services to affected enrollees.

I again thank the Committee for the opportunity to provide NTEU's views on these alarming employee data breaches, and for your work to identify the source of these intrusions, as well as to identify the compromised employee records and personal information. And, most importantly to help ensure that this does not happen again. However, for the information already compromised, time is of the essence, and clear guidance and immediate notification, with adequate levels of protection, is warranted. Ultimately, NTEU members want to be assured that their information, and their family members' information, is not at risk because of their profession. Our members deserve to be able to trust that the government can properly secure their private information.

---

[i] Questionnaires for Public Trust, Non-Sensitive, and National Security Positions.