WRITTEN TESTIMONY BY
DAVID SNELL
FEDERAL BENEFITS SERVICE DIRECTOR
NATIONAL ACTIVE AND RETIRED FEDERAL EMPLOYEES ASSOCIATION

BEFORE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

AND

SUBCOMMITTEE ON OVERSIGHT

HEARING TITLED
"IS THE OPM DATA BREACH THE TIP OF THE ICEBERG?"

July 8, 2015

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and Subcommittee members:

On behalf of the five million federal workers and annuitants represented by the National Active and Retired Federal Employees Association (NARFE), I appreciate the opportunity to express our views regarding the recent data breaches at the Office of Personnel Management (OPM) and its implications for current, former and prospective federal employees.

We are deeply concerned over the failure of the federal government to adequately protect its personnel computer systems and the devastating impact the recent breaches of these systems may have on national security, as well as on the financial and personal security of millions of current and former federal employees.

Make no mistake: The potential consequences of these breaches are severe. The personnel records obtained through the data breaches include the highly personal and sensitive information of millions of current and former employees, and even applicants for federal employment. The extent of the breaches is enormous, likely reaching beyond 18 million individuals.

Possession of the information contained in the SF-86, the security clearance form data exposed by the latest incursion, could give our enemies the means to attempt to corrupt or blackmail government employees, compromise military and intelligence secrets, and even recruit Americans to join or assist terrorist organizations. Moreover, it could lead to the possibility that particular public servants would become vulnerable to grave risks that could threaten their personal security and that of their families and loved ones.

While the perpetrators of this act bear the obvious and primary fault in this matter, the federal government – including both the Administration and Congress – has an obligation to do its best to adequately protect the sensitive information its employees and job applicants are required to disclose as a condition of employment. It failed to meet that obligation.

Despite explicit warnings by inspectors general since 1997, OPM continually failed to put in place adequate safeguards for both its aged and newer computer systems. Through acts of omission and commission, the agency permitted the theft of massive amounts of personally identifiable information. Even now, as OPM works to remedy the situation, the current OPM inspector general issued a flash audit of OPM's plans to improve its data security and found them to have a "very high risk of project failure."

Our government has failed its employees. It is imperative that we not only act swiftly to remedy this situation, but we must also ensure an incident of this magnitude does not repeat itself. We must do a better job of protecting the millions of federal employees who serve this nation. The congressional oversight and response, including this hearing, is a good start. But we must become even more vigilant in our efforts to improve the federal government's information technology and data security to ensure that such a massive and damaging breach never happens again.

Improve Communication to Federal Employees and Retirees

The federal government – including both the Administration and Congress – now has an obligation to correct, to the best of its ability, what has transpired. This should have started with effective communication with federal employees, retirees, others affected by the breaches and the organizations that represent them. Unfortunately, communication has fallen short of expectations.

While OPM has provided notice to those affected by the breach announced on June 4, and has communicated with organizations in that regard, it has thus far failed in its basic duty to inform individuals affected by the second and more troubling breach, announced June 12, and continues to fail to answer many important questions about both breaches.

The OPM website with Frequently Asked Questions on the cyberattack has barely been updated since June 4. Federal employee and retiree representatives learned about the second breach from the news media, not from the Administration. It has been nearly four weeks since the second breach was announced, and we have yet to receive *any* information from the Administration on this incident. The lack of information from an official source has fueled rumors and exacerbated the unease of federal employees and retirees and their friends and families.

The failure of OPM to adequately safeguard the personal information of federal employees, retirees, prospective employees and their families should not be compounded by deflecting questions, the answers to which would benefit both active and retired federal employees. We call on OPM to provide the very information that the perpetrators of this crime already have. Notably, NARFE continues to seek answers to the following questions.

As it relates to the first breach announced on June 4, 2015:

- Why were only some retirees affected in the first breach?

- Which, if any, federal agency personnel records were not included in those that were accessed?

- Is there a specific date before which the employment records would **not** be included in those accessed? And a closely related question: How long does OPM retain employment information after someone has retired?

- Given the insecurity of the Internet, how can an affected party know for certain that the outreach they are receiving at OPM's direction from a commercial source (CSID) is, in fact, legitimate? Why are PINs and other information being sent via email from a non-government email address? One of our members asked: "How can I be sure this email is really from CSID?"

- After the June 4 announcement, OPM repeatedly stated that it does not keep congressional or legislative branch employment data, yet several individuals who work or have worked on Capitol Hill have received notification that their personal information

has been exposed. To what extent does OPM maintain legislative branch employment data?

- Notifications are being sent to individuals who have died since leaving federal service. How can their next of kin take action? What if no one related to the deceased is living at the last known address? How will next of kin be notified? The answer provided on the OPM website in this regard is insufficient and unhelpful.

- We are receiving reports that individuals logging in to the website with their PIN and username are getting someone else's information. Is this issue widespread? Is this issue being fixed?

- Will those affected be asked to provide their Social Security number once they provide their PIN over the phone? We have received reports of this, which is making individuals uneasy.

As it relates to the second breach announced on June 12, the questions are endless. However, in particular, NARFE members would like to know if retirement records were exposed in the second hack. These records contain bank account information and annuity identification numbers.

The federal community and everyone affected by this breach deserve answers to these questions.

Provide Credit Monitoring and Identity Theft Insurance

The financial credit reporting measures OPM has offered to those whose information has been compromised are woefully inadequate. Protection should logically and fairly meet the scope of the threat to federal employees and retirees.

In light of the magnitude of the records breached, the nature of the information compromised, and the potential for a lifetime of identity theft and fraud, the federal government should offer free credit monitoring services for the lifetime of anyone affected and increase the amount of identity theft insurance provided (in specific circumstances, unlimited coverage may be required). It may be years before the information taken is used by criminals, and it is only fair to provide continued financial protection for the many victims who spent a lifelong career in federal service.

Congress should provide the appropriations necessary to provide adequate credit and identity theft protection for the federal employees and retirees affected.

Conclusion

The question posed in the title of this hearing, "Is this the tip of the iceberg?" is a valid one. While I cannot answer that, I will say: I certainly hope not. We have seen cybersecurity breaches at the U.S. Postal Service, the contractor USIS, the Department of Energy and the Department of

Homeland Security. If the OPM security breaches are the tip of the iceberg, we have challenging times ahead of us.

The recent breaches should be a wake-up call to this country and its leaders about the dangers of cyberterrorism and the critical need to protect our government's core functions. In preparing for the future, it is necessary for our leaders to properly evaluate how we ended up in this situation yet again. It also is incumbent on Congress to ensure federal agencies have the necessary resources to ensure a breach of this magnitude does not reoccur. Let's make sure this isn't the tip of the iceberg, but rather the last time our federal government has to deal with a cybersecurity breach that threatens the financial security of its employees.

Thank you again for the opportunity to share our views with you.