



(October 2, 2015)

In order to further improve the lines of communication and to respond to the concerns between the National VA Council and you our members, I have established a National VA Council Briefing. This NVAC Briefing will bring you the latest news and developments within DVA and provide you with the current status of issues this Council is currently addressing. I believe that this NVAC Briefing will greatly enhance the way in which we communicate and the way in which we share new information, keeping you better informed.

Alma L. Lee
National VA Council, President

~ ~ ~ ~ ~

In This Briefing: OPM Cyber Incident Update

~ ~ ~ ~ ~

Dear Colleagues,

Yesterday, we began mailing notification letters to the individuals whose personal information was stolen in a malicious cyber intrusion carried out against the Federal Government. Impacted individuals will be notified by OPM via U.S. Postal Service mail. Email will not be used.

The letters being mailed to those affected by this incident will describe the comprehensive suite of identity theft protection and credit monitoring services that will be provided for at least three years, at no cost, to impacted individuals and to their dependent minor children. An impacted individual is someone whose personal information, including Social Security Number, was stolen.

As we have noted before, those impacted by this breach are already automatically covered by identity theft insurance and identity restoration services. However, the Federal Government is providing additional services that impacted individuals are encouraged to enroll in, free of charge.

The notices will contain a personalized identification number (PIN) number which is necessary to enroll in the covered services. Please note that neither OPM, nor anyone acting on OPM's behalf, will contact you to confirm any personal information. If you are contacted by anyone asking for your personal information in relation to compromised data or credit monitoring services, do not provide it.

As you know, a very large number of people were impacted by this breach, and the nature of the information involved has national security implications as well. OPM and the Department of Defense have continued to analyze the impacted data to verify its quality and completeness, and in this process, we determined that approximately 5.6 million of the impacted individuals had their fingerprints stolen. If an individual's fingerprints were taken, this will be noted in their letter.

While Federal experts believe that, as of now, the ability to misuse fingerprint data is limited, an interagency working group with expertise in this area will review the potential ways adversaries could misuse fingerprint data now, and in the future. This group will also seek to develop potential ways to prevent such misuse. If in the future, new means are developed to misuse the fingerprint data, the government will provide additional information to individuals whose fingerprints may have been stolen in this breach.

All of these factors make it important that we take the time necessary to make sure the notification process is carried out carefully. We're committed to getting this right. What this means is that, while the notifications are beginning this week, it could take considerable time to deliver them all.

I understand that many of you are frustrated and concerned, and would like to receive this information soon. My personal data was also stolen in this breach, and I am eager to get my notification letter as soon as possible so that I can sign up for these services. However, given the sensitive nature of the database that was breached – and the sheer volume of people affected – we are all going to have to be patient throughout this notification process.

In the meantime, please check OPM's online cybersecurity resource center at www.opm.gov/cybersecurity for updates and additional information. This website has valuable suggestions about how to reduce the risk of becoming a victim of cybercrime, has answers to many frequently asked questions, and allows you to sign up for automatic updates. We are continually refreshing the site and will continue to do so as this process unfolds.

OPM and our partners across government are working hard to protect the safety and security of the information of Federal employees, contractors and others who entrust their information to us.

Together with our interagency partners, OPM is committed to delivering high quality identity protection services to the Federal community. We will continue to update you as this process continues. Thank you for your patience, your service to the American people, and your continuing support.

Sincerely,

Beth F. Cobert
Acting Director, Office of Personnel Management

