June 24, 2016

As we approach the Independence Day holiday, the Office of Personnel Management (OPM) wants to wish you a happy July 4th.

It's been about a year since OPM announced the malicious cyber intrusions carried out against the Federal Government. We want to take a moment to update you on our continued response, including what services we have provided to those impacted by these intrusions, what OPM and its interagency partners are doing to enhance cybersecurity, and the steps all Federal employees can take to practice good cyber hygiene.

First, we have completed notifying those who were impacted by the personnel records incident and we have also completed the initial mailing of the notification letters to individuals impacted by the background investigation records incidents. About 10 percent of the letters intended to reach those impacted by the background investigation incident were returned because people had moved, the letters were incorrectly addressed, or other factors.

We have worked to get updated addresses for those whose letters were returned and we are now remailing letters to those who did not receive their original notification letter for the background investigation records incident. The letter being mailed will clearly state at the top that it is a duplicate of the letter previously sent, but not successfully delivered. Those receiving this letter are being invited to sign up for credit and identity monitoring services if they have not already done so.

OPM will be posting a copy of the letter at https://www.opm.gov/cybersecurity/ so recipients can verify the authenticity of the letter they received.

Second, we have made steady progress in implementing the FY 2016 Consolidated Appropriations Act, which contained provisions to increase the amount of identity theft insurance being provided to impacted individuals, as well as the length of coverage. You will be pleased to learn that OPM has increased the amount of identity theft insurance provided to those impacted by the cyber incidents involving personnel records or background investigations records from $1 million to $5 million. This

increase was put into effect on June 1st, and impacted individuals do not have to do anything to be covered by this increase. In addition to increasing the identity theft insurance coverage, OPM is continuing to work on extending credit monitoring and identity protection services to those impacted by either incident for a period of not less than 10 years. We will share additional information later this year.

Identity protection services such as identity restoration and identity theft insurance are included in the free services that we are providing to those impacted by either cyber incident. You can enroll in identity theft protection and credit monitoring services through the OPM website, www.opm.gov/cybersecurity, or by calling either service provider.

If you experience identity theft and need help restoring your identity or want to file a claim under the identity theft insurance, we have set up call centers to assist you. For those impacted by the background investigations incident, please call ID Experts at 800-750-3004. For those who were only impacted by the personnel records incident, please call Winvale / CSID at 844-777-2743.

Third, we have recently updated our OPM Cybersecurity Resource Center website and would encourage anyone with questions to visit and review the updated frequently asked questions section. The updated site includes new information as well as information we're providing as a result of questions and feedback we have received from those who have visited the site. You may access the OPM Cybersecurity Resource Center website at https://www.opm.gov/cybersecurity/.

Fourth, OPM and our partners across government continue to work hard to protect the safety and security of the information that Federal employees, contractors, and others provide to us. Over the past year, OPM has worked with these partners to take significant steps to enhance our cybersecurity posture. You can find a list of the actions we have taken at https://www.opm.gov/cybersecurity/fact-sheet.pdf. For more information on actions the Federal Government has taken to continually strengthen its

cyber defenses, please see Fact Sheet: Administration Cybersecurity Efforts 2015.

Finally, I want to remind you how important it is that we all are vigilant when it comes to practicing good cybersecurity hygiene. In the increasingly complex electronic environment in which we operate, it's up to each one of us to be on guard against malicious actors and to protect the security of the technology we use every day. From regularly updating your passwords to being aware of phishing email scams, there are actions we can each take to protect ourselves from cyber intrusions. Our partners at the Department of Homeland Security (DHS) and the National Counterintelligence and Security Center (NCSC) have a list of tips and best practices that can help you practice cyber safety. Please visit their websites to get more information.

Have a Happy July 4th and a wonderful summer.

Sincerely,

Beth F. Cobert

Acting Director, U.S. Office of Personnel Management