OPM Cybersecurity Incident Update #3 – 16 June 2015

Point of Contact: HRPolicy@aafes.com

Fellow Associate,

On 15 June 2015, we sent you an update regarding the OPM cybersecurity incident. As of today on 16 June 2015, OPM announced that systems containing information related to the background investigations of current, former and prospective Federal government employees, as well as other individuals for whom a Federal background investigation was conducted had been compromised. Below is the main body of the update and FAQs regarding the breach.

We will continue to provide updates as more information becomes available. If you have any questions please refer them to the **hrpolicy@aafes.com.**

Through the course of the ongoing investigation into the cyber intrusion that compromised personnel records of current and former Federal employees announced on June 4, **OPM has recently discovered that additional systems were compromised.** These systems included those that contain information related to the background investigations of current, former, and prospective Federal government employees, as well as other individuals for whom a Federal background investigation was conducted.

This separate incident – like the one that was announced on June 4th affecting personnel information of current and former federal employees – was discovered as a result of OPM's aggressive efforts to update its cybersecurity posture, adding numerous tools and capabilities to its network.

OPM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) are working as part of this ongoing investigation to determine the number of people affected by this separate intrusion. OPM will notify those individuals whose information may have been compromised as soon as practicable. OPM will provide updates when we have more information on how and when these notifications will occur.

For those individuals potentially affected by the incident announced on June 4 regarding personnel information, OPM is offering affected individuals credit monitoring services and identity theft insurance in order to mitigate the risk of fraud and identity theft with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM. Additional information is available on the company's website and by calling toll-free 844-777-2743 (International callers: call collect 512-327-0705).

OPM Security Breach FAQs

What personal information was compromised? OPM maintains personnel records for the Federal workforce. The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, and current and former addresses. It is the type of information you would typically find in a personnel file, such as job assignments, training records, and benefit selection decisions, but not the names of family members or beneficiaries and not information contained in actual policies. The notifications to potentially affected individuals will state exactly what information may have been compromised.

I did not receive a letter stating that my information was compromised, but feel that I should have. Can you help me? OPM is aware of the affected data and the networks and the data on which it resides. OPM will begin sending notifications to individuals whose PII may have been compromised on June 8, 2015. These notifications will take place

on a rolling basis through June 19, 2015. The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services being provided to those Federal employees impacted by the data breach. In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

Has the information been misused? At this time, we have no evidence that there has been any use or attempted use of the information compromised in this incident. This is an ongoing investigation and OPM will continue to be vigilant to ensure that necessary security measures are in place to further strengthen and protect our networks, systems, and data.

What are the risks of identity theft with the information that was compromised? Receiving a letter does not mean that the recipient is a victim of identity theft. OPM is recommending that people review their letters and the recommendations provided. In order to mitigate the risk of fraud and identity theft, we are offering credit monitoring service and identity theft insurance through CSID, a company that specializes in identity theft protection and fraud resolution. All potentially affected individuals will receive a complimentary subscription to CSID Protector Plus for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have $1 million of identity theft insurance and access to full-service identity restoration provided by CSID.

How long will it take to inform all the potential victims involved in the incident? OPM will begin conducting notifications to affected individuals using email and/or USPS First Class mail on June 8, 2015 and will continue notifications on a rolling basis through June 19, 2015.

Can my family members also receive services if they are part of my file/records? Family members of employees were not affected by this breach.

I haven't gotten an email or a letter yet. Does this mean I am not affected? Because of the volume of affected individuals, OPM is sending notifications on a rolling basis. All notifications will be sent by June 19th. Please note that while all letters will be mailed by June 19th, you may receive a letter after this date, depending on the postal service in your area.

I received an email from opmcio@csid.com. Is this email from OPM, or is this a phishing scam? The sender "OPM CIO" and email address "opmcio@csid.com" are the sender and email address that OPM is using to notify affected individuals. If you get an email about the breach from a different address, it is spam. Do not click on any links or provide any personal information. Make sure the link takes you to www.csid.com/opm, where you will need to click the "Enroll Now" button and provide your information. When you enroll, you will be required to provide personal information to begin your credit monitoring services. If you would like to validate an email that indicates you have been impacted by this incident, you may confirm with your agency's privacy officer. The government's privacy officers have been provided information by OPM to help them validate the emails for you.

How will OPM contact me if I no longer work for the government? What if I have changed agencies once or multiple times in recent years? If you have left the government, OPM will send you a notification via postal mail to the last address the agency has on file. OPM will verify this address with the National Change of Address (NCOA) service before mailing a letter. If you have moved between agencies, OPM will send an email notification to your government email account for the agency at which you are currently employed. If your email address is unavailable, notification will be sent via postal mail.