

USAID AGENCY NOTICE ON OPM DATA BREACH, JULY 16 2015

As noted in the previous update, OPM launched a new, online incident resource center, located at <https://www.opm.gov/cybersecurity>, offering up-to-date information regarding the incidents. This site contains training and useful information on best practices to secure data, protect against identity theft, and stay safe online. I encourage you to use this resource. If you still have questions after reviewing the website, or have suggestions for additional content, please email isso@usaid.gov or OPM's new email dedicated to the cyber incidents at cybersecurity@opm.gov.

The following are updates on both incidents:

1. Personnel Records: OPM has largely concluded notifications to individuals whose information may have been compromised by the incident involving personnel records. As previously mentioned, OPM is offering credit restoration and monitoring services and other protections through CSID, a company that specializes in identity theft protection and fraud resolution. *Please note that CSID is working on the personnel records incident only and will not have further information about the background investigations incident.*

As a reminder, all affected employees are automatically enrolled in identity theft insurance and identity restoration services. This means that, if your information was affected by the breach, you are already enrolled in these programs even if you have not yet contacted CSID.

If you have NOT yet received your notification by email or mail, or have deleted or lost the notification, or are wondering if your records were affected, I encourage you to call CSID at [\(844\)-777-2743](tel:844-777-2743).

2. Background Investigations: In the coming weeks, OPM will begin sending notification letters to those whose Social Security number appeared on files impacted by the background investigation records incident. OPM and the Department of Defense will work with a private sector firm specializing in credit and identity theft monitoring to provide services. *Notifications to those affected by this incident have not yet begun.*

Please continue to send us feedback and any unanswered questions you may have about the two incidents.

Alfonso E. Lenhardt
One Team...One Mission!

FROM CSID:

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. The communication to potentially affected individuals will state exactly what information may have been compromised.

Your family member was not affected by this breach. The only data potentially exposed as a result of this incident is your personal data.

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, OPM will offer credit report access, credit monitoring and identify theft insurance and recovery services at no cost, through CSID®. This comprehensive, 18-month membership includes credit monitoring and \$1 million in identity theft protection services.

You have the right to ask the credit bureaus to place fraud alerts in your file, letting potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures that protect you.

There are two types of alerts: initial and extended. An initial fraud alert stays in your file for 90 days. An extended alert stays in your file for seven years. If you ask for an extended alert, you will have to provide an identity theft report, which includes a copy of a report you have filed with a federal, state or local law enforcement agency.
How do I set a fraud alert?

You can call any of the three credit bureaus to place a fraud alert:

- Equifax: (800)525-6285
- Experian: (888)397-3742
- TransUnion: (800)680-7289

To place an initial or extended fraud alert, the credit bureaus will require you to provide appropriate proof of your identity, which may include your Social Security number.

Our identity protection services reduce your risk of identity theft; however, you may still become a victim of identity theft. Because you are subscribed to our monitoring services, you will receive an early warning about the theft and be able to start the recovery process faster. In addition, your service includes Identity Theft Insurance and Restoration services to help alleviate some of the financial burden of identity theft and guide you through the process.