



FAQs for Congressional Offices Regarding Notifications to Individuals Impacted by U.S. Office of Personnel Management Cybersecurity Incidents

OPM is committed to providing Congressional offices with information and support that will enable individuals to be responsive to constituent inquiries regarding the recent cybersecurity incidents. This document highlights resources currently available relating to the background investigation incident and answers some frequently asked questions regarding both incidents. With respect to any of the materials below or to answer any further questions, individuals can visit OPM's website (www.opm.gov/cybersecurity) for more information.

What Happened

In early June 2015, while investigating another cybersecurity incident, OPM discovered malicious cyber activity on its network. It was later determined that the activity resulted in the theft of background investigation records of current, former, and prospective Federal employees and contractors from OPM's systems. OPM and an interagency incident response team have concluded with high confidence that sensitive information, including the Social Security numbers of 21.5 million individuals, was stolen from the background investigation databases. Approximately 5.6 million of the records included fingerprint data.

What steps is OPM taking to protect the people who were impacted by the incidents?

OPM and its partners across government are working to protect the safety and security of the information of Federal employees, military service members, contractors, and others who provide their information to the U.S. Government. OPM will continue work with the interagency incident response team to review the impacted data to enhance its quality and completeness, and to monitor for any misuse of the data.

On September 1, 2015, OPM and the Department of Defense (DOD) announced the award of a contract to Identity Theft Guard Solutions LLC, doing business as ID Experts, to provide a comprehensive suite of identity theft and credit monitoring services to those individuals whose personal information was stolen from OPM's background investigations database. ID Experts is a national company with extensive experience and a track record of customer satisfaction in identity protection and credit monitoring, and will provide three years of services (ending December 31, 2018), at no cost to those impacted. These services will also be provided to the minor dependent children of impacted individuals. The U.S. Government will continue to evaluate the coverage being provided and whether any adjustments are needed in association with this incident.

ID Experts is being held to requirements carefully drafted by an interagency, interdisciplinary group of subject matter experts, including security and privacy representatives from the Department of Homeland Security, DOD, Federal Trade Commission, and other agencies. OPM and DOD also took additional steps to ensure the security of information needed to enroll in services. ID Experts demonstrated compliance with National Institute for Standards and Technology privacy and other security requirements as outlined in the performance work statement; provided system security plans; and will support onsite security inspections by the U.S. Government at any location where protected information is collected, stored, or used.

Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security Numbers were impacted. All impacted individuals should have received notification related to this incident. For more information on the services being provided, please visit: <http://www.csid.com/opm> or call: (844) 777-2743.

***What do the notices include?***

The notices contain a 25 digit individualized Personal Identification Number (PIN) which is necessary to enroll for the covered services. The PIN contains only numbers and no letters or special characters.

Who is providing services to those impacted by the background investigation incident?

ID Experts is providing complete protection and restoration services for all individuals impacted by this incident and their minor dependent children for 3 years ending December 31, 2018.

What if an individual hasn't received a letter, but believes their information was stolen?

Letters are being mailed out over an estimated 12 week period via letter correspondence delivered by the U.S. Postal Service. It is estimated this process will be completed by the middle of December. (Each correspondence will contain a 25 digit individualized PIN that is required to enroll in credit monitoring and identity monitoring services covered under the government contract. The letter and PIN are necessary to complete enrollment. The PIN contains only numbers and no letters or special characters.)

For those individuals who have not received a letter after this period, DOD has established a verification center for individuals who feel they may have been impacted and did not receive a notification letter. The verification center may be accessed through a link at <https://www.opm.gov/cybersecurity>, or via phone (866-408-4555) Monday through Friday, between 9 a.m. and 9 p.m., Eastern Time. Individuals who have PINs and have questions about registration or services can either call ID Experts at 800-750-3004 or visit OPM's website. To receive updates, individuals can also sign up here: <https://www.opm.gov/cybersecurity>.

What happens when an individual contacts the verification center?

Individuals who contact the verification center will be asked to provide their name, address, Social Security number, and date of birth. This information will be used to determine whether their Social Security Number and other personal information were included in the cyber intrusion involving background investigation records. If the information was included, the individual will receive a notification letter via U.S. mail listing an individualized PIN code with enrollment directions. If an individual contacts the Verification Center and it is concluded that the individual's Social Security Number was not compromised in the intrusion, the individual will receive a letter with that information via U.S. Postal Service, after the Verification Center has compared the identity data the individual provided with our records. In either case, it will take approximately 2–4 weeks for the letter to arrive via U.S. Postal Service to the address provided on the website or shared with a call center agent.

What if an individual has a freeze on his or her credit report? How will this affect their ability to sign up for services?

If an individual has a freeze on their credit report, it is possible they may not be able to complete the account creation process until the freeze is lifted, depending upon which credit reporting bureau (or bureaus) has the freeze. A credit freeze, also known as a security freeze, lets an individual restrict access to their credit report, which in turn makes it more difficult for identity thieves to open new accounts in their name. That's because most creditors need to see an individual's credit report before they approve a new account. If they can't see the file, they may not extend the credit. If an individual has placed a credit freeze on their credit report, or a "fraud alert" has been placed on their credit report, we recommend attempting to register for services with ID Experts via telephone instead of online.



For more information on credit freeze please visit the Federal Trade Commission Website at <http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

What if an individual says their PIN from the background investigations incident does not work?

Each letter, sent notifying impacted individuals of the theft of background investigation records, included a 25 digit PIN which must be used in conjunction with the last four digits of the individual's Social Security Number to access the webpage that will allow the individual to sign up for services. They should be able to sign up for services using this information at the OPM cybersecurity website <https://www.opm.gov/cybersecurity>. Please note that the PIN only includes numbers and does not include any letters or special characters.

If the PIN does not work on the first attempt, please attempt to re-enter it. After three failed attempts to enter a PIN through the automated phone system, they will be transferred to an agent, who can try to enter the information for the individual. If they are not able to get into the system through the OPM website or the website rejects the PIN, we encourage individuals to try the phone system, which is at 800-750-3004.

Once registered, do impacted individuals need to keep their PIN?

Once registered, an individual will need to use the username and password created for online access to their ID Experts account. However, to access an account via phone, individuals will need to use their PIN. For this reason we recommend impacted individuals retain their letter with their PIN even after creating an account with ID Experts.

Why are some letter addressed not in full names? For example, an individual's letter included initials, a nickname or previous address, etc.

The U.S. Government has attempted to locate the best address for impacted individuals. Due to the nature of this data in our systems, unfortunately some letters have been mailed with old addresses or names. We are continuously assessing this process and making adjustments as we go. We understand this can be an inconvenience and we appreciate everyone's patience. If an individual believes they are the intended recipient of the letter, individuals may register using the Personal Identification Number (PIN) in conjunction with the last four digits of their Social Security Number at <https://www.opm.gov/cybersecurity>.

If individuals believe they may have been impacted by the cyber intrusion but do not believe the letter they received was intended for them, they will be now able to get more information by contacting the Verification Center established by DOD. The Verification Center may be accessed through a link at <https://www.opm.gov/cybersecurity>, or via phone (866-408-4555) Monday through Friday, between 9 a.m. and 9 p.m., Eastern Time. The Verification Center will also allow individuals to update their address if it has recently changed.

Why is an email address required to sign up for credit monitoring services?

Credit and identity theft monitoring services are designed to provide timely information to the individual whose credit or identity is being monitored. Because timeliness is so important when attempting to prevent or limit credit or identity theft, email is the most efficient and timely means for ID Experts to reach individuals to notify them if there has been potential activity on their account. ID Experts recommends that individuals who do not have their own email account choose to provide the email address of a family member or a trusted friend who can receive the updates on the impacted individual's behalf. At this time there is no postal mail option to receive these alerts. Identity restoration and insurance services remain available for those impacted by the cyber incidents even if they choose not to sign up for the monitoring via email.



Why is personally identifiable information such as Social Security numbers needed when signing up for services?

Social Security Numbers are needed to validate and authenticate the credit and identity monitoring services that are being made available to each impacted individual. For the monitoring services, the impacted individual will also need to answer a series of verification questions (such as date of birth) to validate their identity. OPM has not released an individual's personal information to ID Experts previously.

How can minor children be enrolled?

Individuals who had a Social Security number listed on a background investigation form that was impacted by the incident involving the theft of background investigation records will receive a notification regarding their eligibility for services. Although the Social Security numbers of children generally did not appear in background investigation records, because this population faces different challenges generally because of the lack of a credit history dependent minor children of impacted individuals are eligible to receive the suite of services for the next 3 years.

For purposes of coverage, dependent minor children are defined as children of impacted individuals who were under the age of 18 as of July 1, 2015, even if they were not listed on the form.

Why are letters addressed to deceased individuals?

OPM reviews the federal agency version of the public death master file list from the Department of Commerce before mailing letters and does not send letters to individuals it knows to be deceased. Unfortunately in some instances we did not receive accurate information. OPM will be mailing letters to next of kin of deceased individuals who were impacted by the cybersecurity intrusion.

What should next of kin do when they receive a notification letter?

OPM recommends the deceased individual and any dependent minor children of the deceased impacted individual be enrolled in the identity theft protection services which are being offered. If there is a credit freeze on the deceased individuals' Social Security Numbers they will not be eligible for credit monitoring services. However, the identity monitoring and restoration services will remain available. The deceased and any eligible dependents may be enrolled in these services at the OPM cybersecurity website <https://www.opm.gov/cybersecurity> using the 25-digit PIN in the notification letter associated with the deceased. Other personal information about the deceased, including the last four digits of the individual's Social Security Number, will be necessary to enroll. Please note that the twenty-five digit PIN only includes numbers and does not include any letters or special characters.

If these individuals have difficulty enrolling in services on-line, please call ID Experts at 800-750-3004.

Are dependent minor children of deceased individuals who were impacted by the recent OPM cyber incident eligible for identity protection and restoration services?

Dependent minor children of deceased individuals who were impacted by the recent OPM cyber incident are entitled to identity protection and restoration service and credit monitoring services. The eligible dependent minor children of the deceased may be enrolled in these services at the OPM cybersecurity website <https://www.opm.gov/cybersecurity> using the 25-digit PIN in the notification letter associated with the deceased. Other personal information about the deceased, including the last four digits of the individual's



Social Security Number, will be necessary to enroll. Please note that the twenty-five digit PIN only includes numbers and does not include any letters or special characters.

For purposes of coverage, dependent minor children are defined as children of impacted individuals who were under the age of 18 as of July 1, 2015, even if they were not listed on the form.

If these individuals have difficulty enrolling in services on-line, please call ID Experts at 800-750-3004.

Why is OPM contacting people? Doesn't the Website say no one from OPM will contact anyone?

OPM and ID Experts will not contact individuals to obtain or confirm any personal information. If individuals are contacted by anyone asking for personal information in relation to this incident, they should not provide it. However, in certain instances upon specific request, OPM may reach out to a specific individual in response to an inquiry received from the individual or someone acting on their behalf.

In response to these incidents, what is OPM doing to improve their systems?

OPM continues to take aggressive action to strengthen its broader cyber defenses and information technology (IT) systems, in partnership with experts from DoD, DHS, FBI and other interagency partners.

As outlined in the Cybersecurity Action Report, OPM has identified 15 new steps to improve security and modernize its systems, including:

- Completing deployment of two-factor Strong Authentication for all users;
- Expanding continuous monitoring of its systems;
- Hiring a new cybersecurity advisor

The full report is available online at: <https://www.opm.gov/cybersecurity/cybersecurity-incidents/opm-cybersecurity-action-report.pdf>.

OPM has also directed a comprehensive review of OPM's IT system security to identify and immediately address any other vulnerabilities that may exist, and assess OPM's data sharing and use policies.

What is a background investigation?

In general, background investigation forms collect personal information for people occupying positions with the Federal government, including Social Security numbers to:

- Check criminal histories;
- Validate background investigation applicants' educations;
- Validate employment histories;
- Validate background investigation applicants' living addresses; and
- Gain insight into the character and conduct of background investigation applicants, through checks of references.

In addition, some people occupying public trust or national security positions provide additional types of information that may include:

- Personal information of a spouse or a cohabitant (including Social Security numbers);
- Personal information of parents, siblings, other relatives, and close friends (but does not include Social Security numbers);



- Foreign Countries visited and individuals the applicant may know in those countries;
- Current or previous treatment for mental health issues; and/or
- Use of illegal drugs.

For public trust and national security investigations, other information may be collected related to parents, siblings, other relatives, close friends, and previous places a background investigation applicant may have lived, worked, or attended school. This information is used to interview employers, friends, and neighbors about the applicant, their conduct, and personal history, and to conduct local law enforcement checks at previous locations lived.

Some records also include findings from interviews conducted by background investigators and approximately 5.6 million include fingerprints. The notification letters have information about whether the recipient's fingerprints were impacted. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

Please note that while background investigation records do contain some information regarding mental health and financial history provided by applicants and sources contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USAJOBS, Employee Express).

How can an individual tell if they have been impacted by the background investigation records incident?

If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P for a new investigation or periodic reinvestigation), it is highly likely that individual is impacted by this cyber incident. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely.

For those impacted by the background investigation records incident, the U.S. Government began mailing notifications to individuals in late September. It is estimated this process will be completed by the middle of December.

For those individuals who have not received a letter after this period, DOD has established a verification center for individuals who feel they may have been impacted and did not receive a notification letter. The verification center may be accessed through a link at <https://www.opm.gov/cybersecurity>, or via phone (866-408-4555) Monday through Friday, between 9 a.m. and 9 p.m., Eastern Time. Individuals who have PINs and have questions about registration or services can either call ID Experts at 800-750-3004 or visit OPM's website. To receive updates, individuals can also sign up here: <https://www.opm.gov/cybersecurity>

Please note that OPM and ID Experts will not individually contact impacted individuals to confirm any personal information. If individuals are contacted by anyone asking for personal information in relation to this incident, **do not** provide it.

What services do individuals impacted by the background investigation records incident need to register for?

As of September 1, 2015, all individuals impacted by the background investigation incident are covered by identity theft insurance and eligible for identity theft insurance and restoration services should their identity be compromised. Upon receiving notification, impacted individuals will also have the opportunity to sign themselves and their minor dependent children up for the identity and credit monitoring services.



When will identity theft protection services begin and end for individuals impacted by the background investigation records incident?

Identity theft insurance and identity restoration coverage began on September 1, 2015, and will end on December 31, 2018. Impacted individuals will also be able to enroll in credit monitoring and identity monitoring services once they receive their notification and PIN.

Can I enroll my spouse/partner/family member? Why are individuals not providing services to family members who are on the form? Was my spouse/partner/family member's personal information impacted?

Impacted individuals' dependent minors can be enrolled. Some background investigation forms ask for the Social Security number of a spouse or a co-habitant. If the Social Security numbers for these individuals were provided, these impacted spouses or co-habitants will receive a notification and will be able to sign up for services. Other family members' requested information on the background investigation form was most likely name, address, date of birth, or other similar information. Social Security numbers for these other family members were not requested on the background investigation forms. In such cases, this information is likely the same as what is generally available in public forums such as online directories or social media. This information generally does not present the same level of risk of identity theft or other issues as with a Social Security number.

OPM also recommends visiting <https://www.opm.gov/cybersecurity>. This website offers information regarding the personnel records and background investigation incidents and provides answers to frequently asked questions. The website includes a "Recent Updates" section and a "Stay Informed" feature, which includes options to sign up for email alerts, links to OPM social media, and an RSS feed. The site also directs individuals to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online.

Why were fingerprints included in the data?

Fingerprints are requested as part of all initial Federal background investigations. The fingerprint enables a biometric check of the criminal history records of the Federal Bureau of Investigation, which is a standard part of every initial background investigation.

Will those whose fingerprints were taken be given additional protections?

Impacted individuals will be provided with a comprehensive suite of identity monitoring and protection services at no cost to them. Identity monitoring is included in these services, which includes monitoring of criminal records, arrest records, and court records for any misuse of an individual's identity.

Federal experts believe that, as of now, the ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves. Therefore, an interagency working group with expertise in this area – including the Federal Bureau of Investigation, the Department of Homeland Security, the Department of Defense, and other members of the Intelligence Community – 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 incident.



How many people are impacted?

The total impacted population in the background investigations incident is 21.5 million individuals. Approximately 5.6 million of the records included fingerprint data.

What if an individual was impacted by both the incidents personnel incident and the background investigation incident? Is such a person eligible for services offered in response to both incidents?

Yes. If an individual was impacted by both incidents, that individual will receive a notification from OPM about the background investigation incident and will be eligible to sign up for services from both incidents. If an impacted individual makes a claim under the identity theft insurance option, they should only file that claim with one company. Please note that the service from the personnel data incident provides coverage until December 1, 2016 for impacted individuals and the service from the background investigation incident provides coverage until December 31, 2018 for impacted individuals and their minor dependent children (under the age of 18 as of July 1, 2015).