OPM Cybersecurity Incident Update - January 8, 2016

We have updated information regarding the cybersecurity breach from June 2015. OPM recently announced that it has completed the initial process of notifying individuals impacted by the breach involving background investigation records. Individuals who think they might have been affected, but who have not yet received a notification letter can contact the OPM verification center at **www.opm.gov/cybersecurity** or at the phone numbers below.

- 866-408-4555 Toll Free
- 503-520-4453 International
- 503-597-7662 TTY

Also, Section 632 of the Consolidated Appropriation Act of 2016, signed into law on December 18, requires OPM to provide additional identity protection coverage for individuals affected by OPM breach #1 (personnel records) and OPM breach #2 (background investigations). Specifically, Section 632 says the following.

a) The Office of Personnel Management shall provide to each affected individual as defined in subsection (b) complimentary identity protection coverage that:

   (1) is not less comprehensive than the complimentary identity protection coverage that the Office provided to affected individuals before the date of enactment of this Act;

   (2) (2) is effective for a period of not less than 10 years; and (3) includes not less than $5,000,000 in identity theft insurance.

b) Definition.--In this section, the term ``affected individual'' means any individual whose Social Security Number was compromised during:

   (1) the data breach of personnel records of current and former Federal employees, at a network maintained by the Department of the Interior, that was announced by the Office of Personnel Management on June 4, 2015; or

   (2) the data breach of systems of the Office of Personnel Management containing information related to the background investigations of current, former and prospective Federal employees, and of other individuals.

OPM has provided a resource guide to help support your needs.

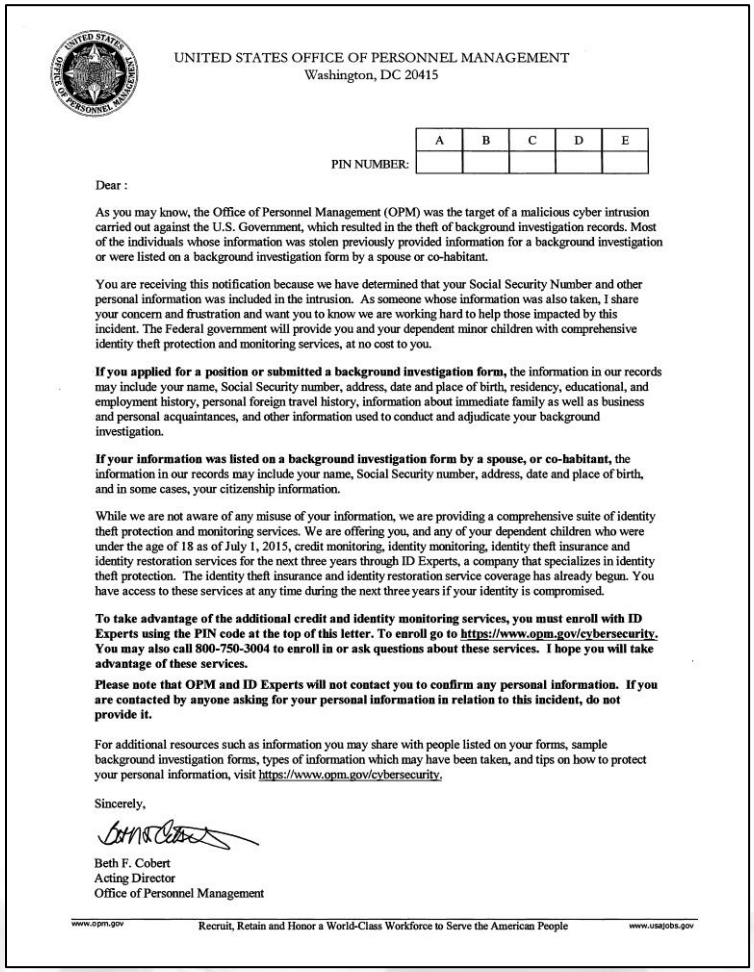
- Copy of the OPM CIO letter to the individual
- Tips on how to be cyber savvy
- Resources on how to register if you received/didn't receive a letter
- Additional websites to help protect your personal identifiable information

FAQs and other materials are posted on the **OPM cybersecurity website**.

DoD CIO All Hands – OPM Breach Update and Cybersecurity

Resources

Official OPM Notification Letter Templates



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

PIN NUMBER:	A	B	C	D	E

Dear :

As you may know, the Office of Personnel Management (OPM) was the target of a malicious cyber intrusion carried out against the U.S. Government, which resulted in the theft of background investigation records. Most of the individuals whose information was stolen previously provided information for a background investigation or were listed on a background investigation form by a spouse or co-habitant.

You are receiving this notification because we have determined that your Social Security Number and other personal information was included in the intrusion. As someone whose information was also taken, I share your concern and frustration and want you to know we are working hard to help those impacted by this incident. The Federal government will provide you and your dependent minor children with comprehensive identity theft protection and monitoring services, at no cost to you.

If you applied for a position or submitted a background investigation form, the information in our records may include your name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation.

If your information was listed on a background investigation form by a spouse, or co-habitant, the information in our records may include your name, Social Security number, address, date and place of birth, and in some cases, your citizenship information.

While we are not aware of any misuse of your information, we are providing a comprehensive suite of identity theft protection and monitoring services. We are offering you, and any of your dependent children who were under the age of 18 as of July 1, 2015, credit monitoring, identity monitoring, identity theft insurance and identity restoration services for the next three years through ID Experts, a company that specializes in identity theft protection. The identity theft insurance and identity restoration service coverage has already begun. You have access to these services at any time during the next three years if your identity is compromised.

To take advantage of the additional credit and identity monitoring services, you must enroll with ID Experts using the PIN code at the top of this letter. To enroll go to https://www.opm.gov/cybersecurity. You may also call 800-750-3004 to enroll in or ask questions about these services. I hope you will take advantage of these services.

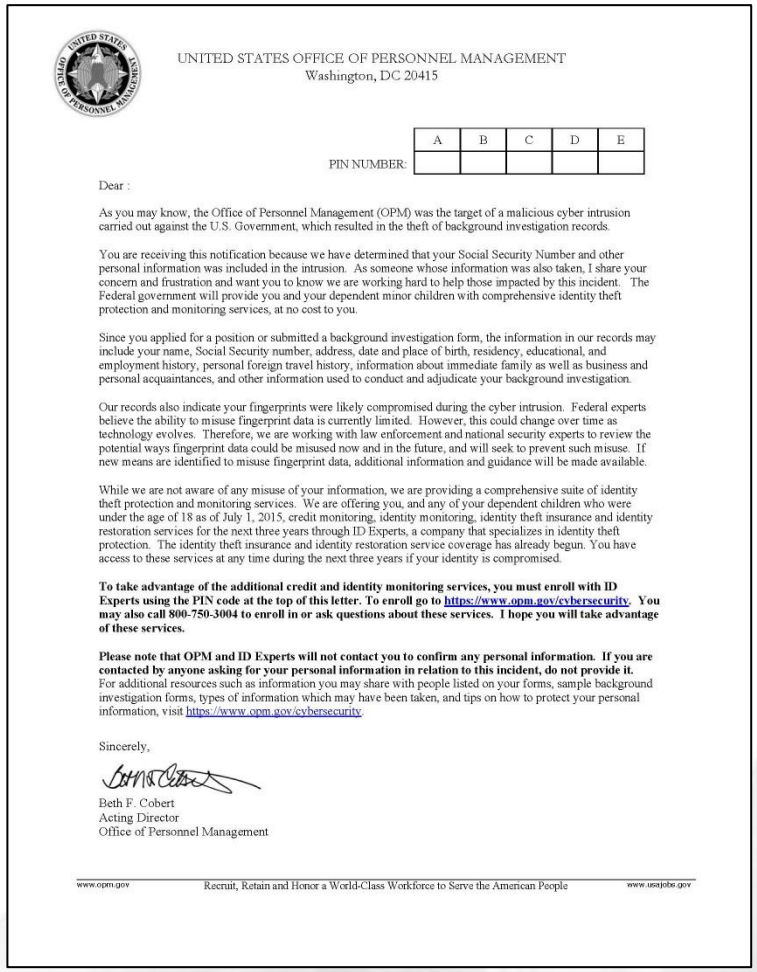
Please note that OPM and ID Experts will not contact you to confirm any personal information. If you are contacted by anyone asking for your personal information in relation to this incident, do not provide it.

For additional resources such as information you may share with people listed on your forms, sample background investigation forms, types of information which may have been taken, and tips on how to protect your personal information, visit https://www.opm.gov/cybersecurity.

Sincerely,

Beth F. Cobert
Acting Director
Office of Personnel Management

www.opm.gov Recruit, Retain and Honor a World-Class Workforce to Serve the American People www.usajobs.gov



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

PIN NUMBER:	A	B	C	D	E

Dear :

As you may know, the Office of Personnel Management (OPM) was the target of a malicious cyber intrusion carried out against the U.S. Government, which resulted in the theft of background investigation records.

You are receiving this notification because we have determined that your Social Security Number and other personal information was included in the intrusion. As someone whose information was also taken, I share your concern and frustration and want you to know we are working hard to help those impacted by this incident. The Federal government will provide you and your dependent minor children with comprehensive identity theft protection and monitoring services, at no cost to you.

Since you applied for a position or submitted a background investigation form, the information in our records may include your name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation.

Our records also indicate your fingerprints were likely compromised during the cyber intrusion. Federal experts believe the ability to misuse fingerprint data is currently limited. However, this could change over time as technology evolves. Therefore, we are working with law enforcement and national security experts to review the potential ways fingerprint data could be misused now and in the future, and will seek to prevent such misuse. If new means are identified to misuse fingerprint data, additional information and guidance will be made available.

While we are not aware of any misuse of your information, we are providing a comprehensive suite of identity theft protection and monitoring services. We are offering you, and any of your dependent children who were under the age of 18 as of July 1, 2015, credit monitoring, identity monitoring, identity theft insurance and identity restoration services for the next three years through ID Experts, a company that specializes in identity theft protection. The identity theft insurance and identity restoration service coverage has already begun. You have access to these services at any time during the next three years if your identity is compromised.

To take advantage of the additional credit and identity monitoring services, you must enroll with ID Experts using the PIN code at the top of this letter. To enroll go to https://www.opm.gov/cybersecurity. You may also call 800-750-3004 to enroll in or ask questions about these services. I hope you will take advantage of these services.

Please note that OPM and ID Experts will not contact you to confirm any personal information. If you are contacted by anyone asking for your personal information in relation to this incident, do not provide it.
For additional resources such as information you may share with people listed on your forms, sample background investigation forms, types of information which may have been taken, and tips on how to protect your personal information, visit https://www.opm.gov/cybersecurity.

Sincerely,

Beth F. Cobert
Acting Director
Office of Personnel Management

www.opm.gov Recruit, Retain and Honor a World-Class Workforce to Serve the American People www.usajobs.gov

Nine Tips to be Cyber Savvy

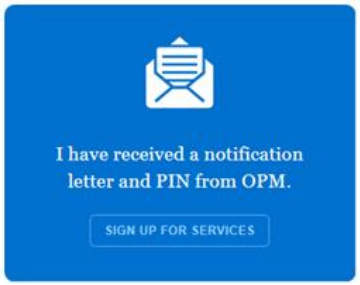
1. **Carefully Browse the Web when using Public Hot Spots** - These unsecure and anonymous networks are targeted by adversaries. Also avoid accessing websites that require login or personal information.
2. **Do Not Exchange Home and Work Content** - Using e-mail or removable media to exchange documents and other data between less-secure home systems and work systems can increase risk of compromise for work systems.
3. **Be Cognizant of Device Trust Levels** - Avoid using a less cyber-savvy user's (like a child's) computer for sensitive functions, like online banking or storing family photos.
4. **Be Wary of Storing Personal Information on the Internet** - Data in the cloud can be difficult to delete, and search engines can help you see personal information that is already online.
5. **Avoid Posting Photos with GPS Coordinates** - An attacker can leverage the GPS coordinates that are automatically enabled in many phones and cameras.
6. **Share Cautiously and Privately on Social Networking Sites** - Think twice about posting data that could be used to target you, like your address, vacation schedules, and photos that may have location data embedded.
7. **Enable the Use of SSL Encryption** - When conducting sensitive personal activities, like account logins and financial transactions, Look for the "lock" that indicates that SSL is enabled.
8. **Follow E-mail Best Practices** – Use different usernames for home and work e-mails, and different passwords for every account. Also, be wary of any e-mail requesting personal information.
9. **Protect Passwords** - Use unique and strong passwords for each account; disable the feature that allows Web sites or programs to remember passwords; and use two-factor authentication whenever available.

How Do I Register?

To register for services:
Visit OPM's Cyber Security Resource Center and click on **"I have received a notification letter and PIN from OPM"**

Or,

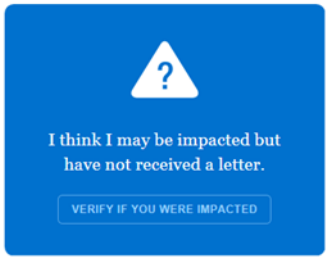
Call ID Experts, if you have difficulty enrolling in services on-line (**800-750-3004)**



To verify if your PII was stolen:
Visit OPM's Cyber Security Resource Center and click on **"I think I may be impacted but have not received a letter"**

Or,

Call the Verification Call Center at
866-408-4555 Toll Free
503-520-4453 International
503-597-7662 TTY



OPM Cyber Security Resource Center (www.opm.gov/cybersecurity)

Resources to Help Protect Yourself and Your PII

Visit **OPM's Cyber Security Resource Center** for more information, helpful resources, and frequently asked questions about this data breach

www.opm.gov/cybersecurity

View the **Defense Security Service "Protecting your Identity Toolkit"** to learn about reporting identity theft and protecting yourself

http://pyi-toolkit.cdse.edu

Download **Antivirus Software** available free-of-charge to active duty military and civilian employees

http://www.disa.mil/Cybersecurity/Network-Defense/Antivirus/Home-Use

Visit the **National Counterintelligence and Security Center website** to view informative, topical videos and print materials, like posters and table tents

www.ncsc.gov

Watch videos from the **Office of the Director of National Intelligence** at about relevant subjects like cyber-crime, social media deception, and spear phishing

https://www.youtube.com/user/ODNIgov

More Online Information on How to Protect Your Identity

Federal Trade Commission's Identity Theft Website
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Federal Trade Commission's Complaint Assistant
https://www.ftccomplaintassistant.gov

Federal Government's one-stop resource for identity theft victims
https://www.identitytheft.gov/

Department of Justice
http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud