



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

December 9, 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF, NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Online Verification Center Announcement for Those Affected by OPM Data Breach

The following is an update on progress made to help those within the DoD community—employees, contractors, retirees, families, and friends – who were affected by the breach of the Office of Personnel Management’s (OPM) databases. As a result of this cyber intrusion, information was stolen from about 21.5 million background investigation applicants and non-applicants, primarily spouses or co-habitants of applicants. This information included personally identifiable information (PII), like names and Social Security numbers, as well as findings from interviews conducted by background investigators. Approximately 5.6 million records included fingerprints.

Because this personal information was compromised, each of us should think about the best ways to protect ourselves and our information in this new environment. Minimizing the impact of this theft on DoD personnel is a top priority, so the Government contracted with ID Experts to offer a suite of identity theft and credit monitoring services to those who were affected. These optional services include three years of coverage, ending on December 31, 2018, free-of-charge, for impacted individuals and their minor dependent children. Please note, dependent children are also eligible for the three years of coverage if they were younger than 18 years of age as of July 1, 2015. I encourage you to consider enrolling in these voluntary protective services.

If your background investigation records were affected by this data breach, you will need a personal identification number (PIN) to enroll in the services offered by ID Experts. Affected individuals will receive their PINs in a notification letter mailed by OPM. Many of you already received these notification letters, and the remainder of the letters will be mailed by the second week of December. This letter will confirm whether your personal information and fingerprints were

compromised. Providing the PIN from the notification letter along with the last four digits of your Social Security number is the only way the credit and identity monitoring services contractor, ID Experts, will be able to verify if you are eligible for services. Along with providing your PIN, the letter will also explain how you can enroll in the identity theft and credit monitoring services, and will include a phone number to call with any questions.

If you think that it is likely that you were affected and are eligible for these credit monitoring and identity theft protection services, but did not receive a letter, or if you received a letter and lost your PIN, OPM recently launched an online verification center website and a call center. However, we ask that you wait until the end of December – in case your notification is still in the mail.

The online verification center will be accessible from the OPM Cybersecurity Resource Center (www.opm.gov/cybersecurity) 24-hours per day, seven days a week, through the end of December, 2018. If you are unable to access the website, or if you have questions that cannot be answered online, please contact the call center at 866-408-4555 to speak directly with an agent. This call center will be available from 9 a.m. to 9 p.m. EST, Monday through Friday.

When you visit the website or call an agent, you will be asked for your name, address, Social Security number, and date of birth. The Government will use this data to research and determine whether you were affected by the cyber intrusion. Two to four weeks after you submit your request, you should receive a letter response via U.S. mail. If you were affected, your notification letter will include a PIN and directions to enroll in services. If you were not affected, your letter will confirm that your personal information was not compromised.

We have worked very diligently to ensure that the contract for services and verification process are in compliance with the federal cybersecurity standards issued by the National Institute of Science and Technology.

Additional updates and information are currently available at the links below to help you secure your PII. These resources can help *all* individuals protect themselves and their personal information:

- Visit OPM’s Cybersecurity Resource Center at www.opm.gov/cybersecurity for more information, helpful resources, and frequently asked questions about this data breach
- Watch the DoD-wide All Hands video on the OPM Cyber Intrusion online at <http://live.gcds.disa.mil/streaming/video.html?id=DODCIOCyberSecurity&bitrate1=400&bitrate2=800> any time after December 18, 2015
- View the Defense Security Service “Protecting your Identity Toolkit” at <http://pyi-toolkit.cdse.edu> to learn about reporting identity theft and protecting yourself
- Download Antivirus Software available free-of-charge to active duty military and civilian employees at <http://www.disa.mil/Cybersecurity/Network-Defense/Antivirus/Home-Use>

In addition to being careful about your personal information, I hope you will also be attentive to potential activities by foreign intelligence organizations. The Office of the Director of National

Intelligence's (ODNI) National Counterintelligence and Security Center has launched a "Know the Risk – Raise your Shield" campaign to raise the awareness of federal employees, contractors, and their families of issues about exploitation tactics of foreign and criminal entities via spear fishing, social media, human targeting, and safeguarding personal information during overseas travel. You can learn more by visiting their website and by watching videos on the ODNI YouTube page.

- Visit the National Counterintelligence and Security Center website at www.ncsc.gov to view informative, topical videos and print materials, like posters and table tents
- Watch videos from the Office of the Director of National Intelligence at <https://www.youtube.com/user/ODNIgov> about relevant subjects like cyber-crime, social media deception, and spear phishing

I understand that many of you have concerns about this data breach. As mentioned earlier in this letter, the resources identified above are available to help you protect your personal information as we move forward together in the wake of this cybersecurity incident.

Terry A. Halvorsen

Attachment:
Postmaster on OPM Online Verification Center

Postmaster

Dear Colleagues:

The U.S. Office of Personnel Management has launched an online verification center to help individuals impacted by the malicious cyber intrusion carried out against the Federal Government which resulted in the theft of background investigation records.

The online verification center is available to help individuals who believe their data may have been taken, but have not received a notification letter. The center will also assist those who have received a letter informing them that they were impacted by the background investigation intrusion, but have lost their PIN code.

Individuals will be able to access the verification website via a link at www.opm.gov/cybersecurity 24-hours a day, 7 days a week. The site will be available through the end of December, 2018. If individuals cannot get their questions answered online, they may request assistance by calling 866-408-4555 and speaking with an agent. The call center will be open from 9 a.m. to 9 p.m. Eastern Time, Monday through Friday.

The notification process is still continuing and because of the large volume of letters, some impacted individuals may not have received their letters. We are encouraging those who believe their data may have been taken, but have not been notified, to wait until mid-December before contacting the verification center. We anticipate mailing all letters by the end of the second week of December.

More information and some frequently asked questions are posted at www.opm.gov/cybersecurity. We will continue to refresh the site as the process unfolds and individuals may sign up for automatic updates.

OPM and our partners across government continue to work hard to protect the safety and security of the information of Federal employees, contractors, and others who entrust their information to us. The online verification center is one more way we are working to help individuals impacted receive the services available to them.

We will continue to update you as this process continues. Thank you for your patience, for your service to the American people, and for your continuing support.

Sincerely,

Beth Cobert

Acting Director, U.S. Office of Personnel Management