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

CHIEF INFORMATION OFFICER

August 26, 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
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Data Breaches and Steps to Protect the DoD Workforce and Others

This memo will provide the DoD workforce with an update on the current situation involving recent cybersecurity incidents that impacted DoD personnel, and share resources and information about steps we all should take to protect our identities in the event that personal information is stolen.

OPM has confirmed two separate cybersecurity incidents that impacted the personal data of government employees, contractors, and others. This letter offers background about these incidents and an update on the notification process for the second breach announced in July. DoD's identity theft protection toolkit at the hyperlink address below will be useful to those affected by either breach.

In April 2015, OPM discovered the first incident, which involved the personnel data of 4.2 million current and former civilian Federal government employees. OPM began providing individual notifications in early June, and those impacted by this first incident should already have received their notifications. Affected employees are being offered--at no cost--eighteen months of identity insurance and credit monitoring from CSID, a company specializing in identity theft protection and fraud resolution. If you have questions about this incident, please contact CSID at 844-777-2743 or opmsupport@csid.com.

In July 2015, OPM announced a second cybersecurity incident affecting background investigation records of 21.5 million current, former, and prospective Federal civilian and military employees and contractors who have undergone clearance investigations, as well as non-applicants, specifically spouses and cohabitants of these applicants. Security clearance information that was compromised includes data provided on the SF85, SF85p, and SF86 questionnaires.

DoD, in support of OPM, is taking the lead on contracting credit monitoring and identity theft protection services for all 21.5 million people affected by the second cybersecurity incident. We anticipate that a contract for this notification process will be awarded in the next two weeks, with notifications beginning by the end of September. We will provide the workforce with updates on this notification process moving forward as they become available.

Most DoD employees were affected by these incidents. We urge you to take immediate measures to protect yourself from scams and from the misuse of your personal information. To protect your financial health, we recommend that you immediately:

- Change passwords on all of your financial accounts
- Monitor your financial accounts for unusual activity
- Report any unusual activity to your financial institutions

DoD has compiled an identity theft protection toolkit with useful information about how to protect yourself; it is available online at http://pyi-toolkit.cdse.edu. Additional online resources include:

- OPM Online Cybersecurity Incident Resource Center (https://www.opm.gov/cybersecurity)
- Department of the Navy Resource Center (www.secnav.navy.mil/OPMbreachDON)
- U.S. Air Force Cybersecurity Resource Center (www.af.mil/cybersecurity.aspx)

We appreciate your patience as we work to notify each of you in a timely and secure a manner.

Terry A. Halvorsen