FM SECNAV WASHINGTON DC
TO ALNAV
INFO SECNAV WASHINGTON DC
CNO WASHINGTON DC
CMC WASHINGTON DC
BT

UNCLAS

ALNAV 056/15

MSGID/GENADMIN/SECNAV WASHINGTON DC/-/JUL//

SUBJ/OFFICE OF PERSONNEL MANAGEMENT DATA BREACH – LIST OF AFFECTED PERSONNEL GROWS//

RMKS/1. In ALNAV 052/15 I informed you about the loss of personnel information at the Office of Personnel Management (OPM) where the electronic Official Personnel Folder (eOPF) of current and former federal employees was compromised.

2. On Thursday, 9 July, OPM announced the results of the interagency forensics investigation into a second recent cyber incident involving federal background investigation data and the steps it is taking to protect those impacted. OPM confirmed an incident affecting background investigation records of current, former, and prospective federal employees, military members, and contractors. The interagency team has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million included fingerprints. If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of standard forms (SF) 86, 85, or 85P for a new background investigation or periodic reinvestigation), it is highly likely that the individual is impacted by this cyber breach. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely.

3. Significant numbers of current, former, and prospective military members and government civilians, as well as contractors, have been affected. This additional loss of data affects a much larger group of Department of the Navy (DON) members than the incident announced in June. Timely and accurate information will continue to be available at: http://www.secnav.navy.mil/OPMBreachDON.

4. In the coming weeks OPM will send notification packages to affected DON personnel. It is not known when this process will be complete. As with the first OPM data breach, affected federal employees and Service Members will be provided a comprehensive suite of monitoring and protective services for those whose SSNs, and in many cases, other sensitive information, were stolen. Additional resources will be made available to help protect the personal information of others affected by this data breach. Complete information concerning coverage will be available at: http://www.secnav.navy.mil/OPMBreachDON as soon as it becomes available.

5. DON continues to assess the risks associated with these data breaches. It is prudent to assume we are all affected by the compromise of this information. OPM will provide educational materials and guidance to help those affected prevent identity theft, better secure their personal and work-related data, and become more generally informed about cyber threats and other risks presented by malicious actors. As always, report any suspicious activity to your Commanders, Security Managers, Privacy Officials and Naval Criminal Investigative Service.

6. Released by Mr. Thomas W. Hicks, Performing the Duties of the Under Secretary of the Navy.//

BT
#0001
NNNN
UNCLASSIFIED//