OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

JUN 0 7 2013

INTELLIGENCE

MEMORANDUM FOR DOD SECURITY DIRECTORS

SUBJECT: Notice to DoD Employees and Contractors on Protecting Classified Information and the Integrity of Unclassified Government Information Technology Systems

Classified information, whether or not already posted on public websites, disclosed to the media, or otherwise in the public domain remains classified and must be treated as such until it is declassified by an appropriate U.S. government authority. It is the responsibility of every DoD employee and contractor to protect classified information and to follow established procedures for accessing classified information only through authorized means. Leadership must establish a vigilant command climate that underscores the critical importance of safeguarding classified material against compromise.

Accordingly, we request all DoD components send prompt notification to your employees and contractors reminding them of these obligations. Procedures for responding to classified information found in the public domain are attached. These procedures will be promulgated in future DoD issuances. My point of contact is Mr. Jeremy Bouchard at (703) 604-0217 or Jeremy.Bouchard@osd.mil.

V-07 Timothy A. Davis
Director of Security

Attachment:
As stated

NOTICE TO DOD EMPLOYEES AND CONTRACTORS FOR RESPONDING TO CLASSIFIED INFORMATION IN THE PUBLIC DOMAIN

- DoD employees and contractors shall not, while accessing the web on unclassified government systems, access or download documents that are known or suspected to contain classified information.

    - This requirement applies to accessing or downloading that occurs when using government computers or employees' or contractors' personally owned computers that access unclassified government systems, either through remote Outlook access or other remote access capabilities that enable connection to government systems.

    - DoD employees or contractors who inadvertently discover potentially classified information in the public domain shall report its existence immediately to their Security Manager. Security Managers and Information Assurance Managers are instructed to document the occurrence and report the event to the Director of Security Policy and Oversight, Office of the Under Secretary of Defense for Intelligence (OUSD(I)). The offending material will be deleted by holding down the SHIFT key while pressing the DELETE key for Windows-based systems and clearing of the internet browser cache. Administrative Inquires and other investigative responsibility will be determined by the OUSD(I) Director of Security Policy and Oversight.

- DoD employees or contractors who seek out classified information in the public domain, acknowledge its accuracy or existence, or proliferate the information in any way will be subject to sanctions. The procedures outlined above apply only to the inadvertent identification of classified information in the public domain.

The OUSD(I) Security Policy and Oversight Directorate stands ready to clarify guidance on these issues. Components may send inquiries via electronic submission on:

- NIPRNet (ousdisec@osd.mil),
- SIPRNet (ousdi.dusd.issecurity@osd.smil.mil), or
- JWICS (mladd-ousdidusdi&s-security@osdj.ic.gov).