



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

INTELLIGENCE

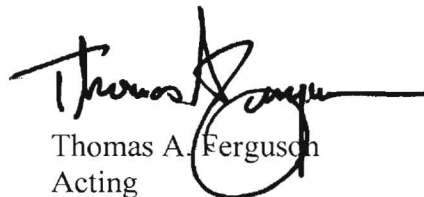
JAN 11 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

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

The recent disclosure of U.S. Government documents by WikiLeaks has caused damage to our national security. Classified information, whether or not already posted on public websites or disclosed to the media, 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. A model notice is attached for your use or modification as appropriate. The Defense Security Service will also notify those companies for which they have oversight.


Thomas A. Ferguson
Acting

Attachment:
As stated



**NOTICE TO DOD EMPLOYEES AND CONTRACTORS
ON PROTECTING CLASSIFIED INFORMATION
AND THE INTEGRITY OF UNCLASSIFIED
GOVERNMENT INFORMATION TECHNOLOGY (IT) SYSTEMS**

The recent disclosure of U.S. Government documents by WikiLeaks has caused damage to our national security. Each DoD employee and contractor is obligated to protect classified information and the integrity of government IT systems in accordance with applicable laws and DoD policies.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, *classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by DoD employees and contractors, until it is declassified by an appropriate original classification authority.*

DoD employees and contractors are reminded of the following obligations with respect to protecting classified information and the integrity of unclassified government IT systems.

- DoD employees or contractors shall not access classified information unless they have:
 - received a favorable determination of eligibility for access by an appropriate authority,
 - signed an approved nondisclosure agreement,
 - demonstrated a need to know the information, and
 - received training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.
- DoD employees or contractors shall not remove classified information from official premises or disclose it without proper authorization.
- Except as authorized by DoD policy and procedures, DoD employees or contractors shall not, while accessing the web on unclassified government systems (including BlackBerries or other smartphones), access or download documents that are marked classified (including classified documents publicly available on WikiLeaks.org and other websites), as doing so risks putting classified information on unclassified IT systems.
 - This requirement applies to accessing or downloading that occurs 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 these government systems.

This requirement does not restrict employee or contractor access to unclassified, publicly available news reports (and other unclassified material) that may in turn discuss classified material, as distinguished from access to the underlying classified documents available on public websites or otherwise in the public domain.

- DoD employees or contractors shall refer all public queries on this matter to their servicing Public Affairs office; they shall neither confirm nor deny the presence of classified information in articles or websites in the public domain.
- DoD employees or contractors shall refer Congressional queries pertaining to the presence of classified information in articles or websites in the public domain to their servicing Congressional Affairs office.
- DoD employees and contractors who believe they have inadvertently accessed or downloaded classified information from a public website via an unclassified government IT system, or without prior authorization, shall contact their information assurance manager (IAM) or information assurance office (IAO) for assistance. *Note: In the case of classified documents inadvertently accessed or downloaded from the WikiLeaks website or other websites posting WikiLeaks-related classified documents, the IAM will document each occurrence and delete the affected file(s) by holding down the SHIFT key while pressing the DELETE key for Windows-based systems. No incident report or further sanitization of government IT systems is required. This guidance pertains only to the accessing or downloading of the classified documents described above because of the extent of the compromise and the prohibitive cost of standard sanitization procedures. All other classified spillages must be handled in accordance with existing regulations.*

Thank you for your cooperation and vigilance in implementing these responsibilities.