DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

SEP 22 2008

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

SUBJECT: Protection of Controlled Unclassified Information on DoD Information Systems Connected to the Internet

References: See Attachment

This memorandum reiterates the importance of properly protecting controlled unclassified information (CUI) placed on information systems connected to the Internet, especially those that use file transfer protocol (FTP), peer-to-peer (P2P), and other protocols that are inherently insecure and pose significant security risks. DoD is currently hosting thousands of such sites and, in spite of previous direction, far too much CUI data is still publicly accessible from these DoD sites. This situation must be corrected promptly. All information to be made accessible to the general public must be properly cleared for public release before it is posted and the hosting site safeguarded per References (a) through (l). Particular attention should be paid to safeguarding personally identifiable information (PII) (Reference (b)).

Proper system configuration and the employment of specified risk mitigation techniques as set out in the Security Technical Implementation Guides (STIGs) are critical to properly protecting sensitive DoD data. These should be verified during system certifications. Additionally, due to inherent risks, sites using FTP, P2P and other insecure protocols should migrate to more secure protocols where feasible.

Whenever appropriate safeguards are not employed, such as when it is not "possible" or "practical," such exceptions shall be appropriately assessed for risk by the Designated Accrediting Authority (DAA) and documented in a Plan of Actions and Milestones, in accordance with the guidance set out in Reference (l). I have directed the Defense-wide Information Assurance Program office to follow-up to ensure such documentation is maintained.

To ensure information regarding the requirement for protecting CUI on information systems is widely and effectively disseminated, DoD components are highly encouraged to incorporate it in training for in-processing new personnel and in annual security refresher training and periodic security awareness briefings for the workforce. Components are also encouraged to publish this information in installation newspapers, daily bulletins, and other media to reemphasize the policy.

For additional information or assistance regarding this memorandum, please contact Mr. Rick Aldrich, richard.aldrich.ctr@osd.mil, 703-602-9991, or Mr. John Hunter, john.hunter@osd.mil, 703-602-9927.

for Cheryl J. Roby
John G. Grimes

Attachment:
As stated

ATTACHMENT

REFERENCES

(a) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(b) DoD CIO Policy Memorandum, "Guidance on Protecting Personally Identifiable Information," August 18, 2006
(c) Joint Deputy Secretary of Defense/Vice Chairman of the Joint Chiefs of Staff Message, "Information Security/Website Alert," August 6, 2006
(d) DoD Senior Privacy Official policy memorandum, "Safeguarding Personally Identifiable Information," June 15, 2006
(e) DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996
(f) DoD Regulation 5200.1-R, "DoD Information Security Program," January 14, 1997
(g) DoD Directive 8500.01E, "Information Assurance," October 24, 2002
(h) DoD Instruction 8500.02, "Information Assurance (IA) Implementation," February 6, 2003
(i) Assistant Secretary of Defense for Command Control Communications and Information (C3I) Memorandum, "Web Site Administration Policies and Procedures," November 25, 1998 (with amendments through January 11, 2002)
(j) Assistant Secretary of Defense for Networks and Information Integration (NII), "Use of Peer-to-Peer (P2P) File-Sharing Applications across DoD," November 23, 2004
(k) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004
(l) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007