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

CHIEF INFORMATION OFFICER

May 9, 2008
Incorporating Change 3, May 11, 2012

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
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 SECRETARIES OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement

References: (a) DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems–Standard Consent Banner and User Agreement," November 2, 2007
(b) DoD CIO Memorandum, "Temporary Hold on Implementation of New Banners and User Agreements," December 6, 2007
(c) ASD(C3I) Memorandum, "Policy on Department of Defense (DoD) Electronic Notice and Consent Banner," January 16, 1997
(d) DoD/GC Memorandum, "Communications Security (COMSEC) and Information Systems Monitoring," March 27, 1997

This memorandum establishes Departmental policy on the use of DoD information systems. It requires the use of a standard Notice and Consent Banner and standard text to be included in user agreements. This memorandum supersedes references (a) through (d). Conforming changes will be made to the relevant policy documents. This Directive-Type Memorandum shall expire effective ~~*May 1, 2012*~~ *March 1, 2013*.

The banner at Attachment 1, "Standard Mandatory DoD Notice and Consent Banner," shall be displayed at log on to all DoD information systems. (Choose either

banner A or B based on the character limitations imposed by the system.) The banner is mandatory and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance.

The language in Attachment 2, "Standard Mandatory Notice and Consent Provision for All DoD Information System User Agreements," shall be included in all DoD information system user agreements. DoD components shall also conform component user agreements to this policy.

This policy is effective immediately and shall be implemented no later than 60 days from the date of this memorandum. Any portion of component policy conflicting with this policy is superseded 60 days from the date of this memorandum unless the component obtains an extension through the POC listed below.

Use of the following measures to widely and effectively disseminate this new policy is encouraged:

1) Training, both initial in-processing of new personnel and annual security refresher training
2) Publication of this information in installation newspapers, daily bulletins, and other media to reemphasize this policy
3) Periodic security awareness briefings for all users

Additional information or assistance regarding this policy may be obtained from Mr. Rick Aldrich, richard.aldrich.ctr@osd.mil, 703-602-9991 or Mr. John Hunter, john.hunter@osd.mil, 703-602-9927.

Attachments:
As stated

ATTACHMENT 1

STANDARD MANDATORY
DOD NOTICE AND CONSENT BANNER

[A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

[B. For Blackberries and other PDAs/PEDs with severe character limitations:]

I've read & consent to terms in IS user agreem't.

ATTACHMENT 2

STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

  - At any time, the U.S. Government may inspect and seize data stored on this information system.

  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications

and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data

other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.