DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

FEB 25 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities

References: See Attachment 1

Purpose. This memorandum establishes DoD policy and assigns responsibilities for responsible and effective use of Internet-based capabilities, including social networking services (SNS). This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense. This DTM is effective immediately; it will be converted to a new DoD issuance within 180 days.

Applicability. This DTM applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

- All authorized users of the Non-Classified Internet Protocol Router Network (NIPRNET).

Definitions. Unless otherwise stated, these terms and their definitions are for the purpose of this DTM.

- Internet-based capabilities. All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as SNS, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).

- External official presences. Official public affairs activities conducted on non-DoD sites on the Internet (e.g., Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter).

- Official public affairs activities. Defined in DoD Instruction (DoDI) 5400.13 (Reference (a)).

Policy. It is DoD policy that:

- The NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD Components.

- Commanders at all levels and Heads of DoD Components shall continue to defend against malicious activity affecting DoD networks (e.g., distributed denial of service attacks, intrusions) and take immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve operations security or to address bandwidth constraints).

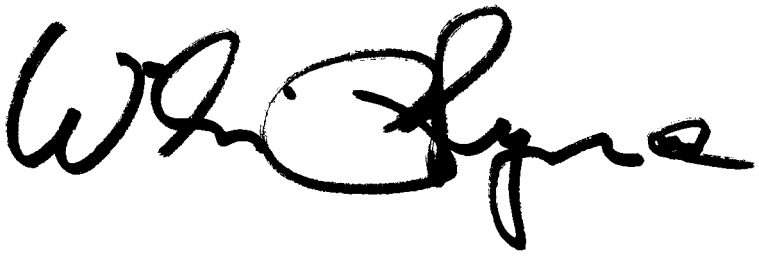
- Commanders at all levels and Heads of DoD Components shall continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (e.g., pornography, gambling, hate-crime related activities).

- All use of Internet-based capabilities shall comply with paragraph 2-301of Chapter 2 of the Joint Ethics Regulation (Reference (b)) and the guidelines set forth in Attachment 2.

Responsibilities. See Attachment 3.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

Attachments:
As stated



DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
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

ATTACHMENT 1

REFERENCES

(a) DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008
(b) DoD 5500.7-R, "Joint Ethics Regulation," August 1, 1993
(c) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(e) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
(f) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(g) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(h) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(i) DoD 5200.1-R, "Information Security Program," January 14, 1997
(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982
(k) DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001
(l) Unified Command Plan, "Unified Command Plan 2008 (UCP)," December 17, 2008

ATTACHMENT 2

GUIDELINES FOR USE OF INTERNET-BASED CAPABILITIES

1. GENERAL. This attachment applies to the official and/or authorized use of Internet-based capabilities by DoD personnel and all authorized users of the NIPRNET. Examples include, but are not limited to:

a. SNS.

b. Image- and video-hosting web services.

c. Wikis.

d. Personal, corporate, or subject-specific blogs.

e. Data mashups that combine similar types of media and information from multiple sources into a single representation.

f. Similar collaborative, information sharing-driven Internet-based capabilities where users are encouraged to add and/or generate content.

2. OFFICIAL PRESENCES. External official presences shall comply with Reference (a) and clearly identify that the Department of Defense provides their content. In addition, external official presences shall:

a. Receive approval from the responsible OSD or DoD Component Head. Approval signifies that the Component Head concurs with the planned use and has assessed risks to be at an acceptable level for using Internet-based capabilities.

b. Be registered on the external official presences list, maintained by the Assistant Secretary of Defense for Public Affairs (ASD(PA)), on www.Defense.gov.

c. Comply with References (a) and (b) as well as DoD Directive (DoDD) 8500.01E, DoDI 8500.2, DoDD 5400.11, DoDD 5230.09, DoD Manual 5205.02-M, DoDD 5015.2, DoD 5200.1-R, and DoD 5240.1-R (References (c) through (j), respectively).

d. Use official DoD and command seals and logos as well as other official command identifying material per ASD(PA) guidance.

e. Clearly indicate the role and scope of the external official presence.

f. Provide links to the organization's official public Web site.

g. Be actively monitored and evaluated by DoD Components for compliance with security requirements and for fraudulent or objectionable use (References (d), (g), and (i)).

3. OFFICIAL USE. Official uses of Internet-based capabilities unrelated to public affairs are permitted. However, because these interactions take place in a public venue, personnel acting in their official capacity shall maintain liaison with public affairs and operations security staff to ensure organizational awareness. Use of Internet-based capabilities for official purposes shall:

a. Comply with References (b) through (j).

b. Ensure that the information posted is relevant and accurate, and provides no information not approved for public release, including personally identifiable information (PII) as defined in Reference (e).

c. Provide links to official DoD content hosted on DoD-owned, -operated, or -controlled sites where applicable.

d. Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Department of Defense").

4. RECORDS MANAGEMENT. Internet-based capabilities used to transact business are subject to records management policy in accordance with Reference (h). All users of these Internet-based capabilities must be aware of the potential record value of their content, including content that may originate outside the agency.

5. LIMITED AUTHORIZED PERSONAL USE. Paragraph 2-301 of Reference (b) permits limited personal use of Federal Government resources when authorized by the agency designee on a non-interference basis. When accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures in accordance with Reference (g) and shall not represent the policies or official position of the Department of Defense.

ATTACHMENT 3

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in section 4 of this attachment, shall:

a. Establish and maintain policy and procedures regarding Internet-based capabilities use, risk management, and compliance oversight.

b. Provide implementation guidance for responsible and effective use of Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities with information assurance (IA) education, training, and awareness activities.

d. Establish mechanisms to monitor emerging Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Heads of the OSD and DoD Components, develop a process for establishing enterprise-wide terms of service agreements for Internet-based capabilities when required.

2. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in addition to the responsibilities in section 4 of this attachment, shall:

a. Develop procedures and guidelines to be implemented by the OSD and DoD Components for OPSEC reviews of DoD information shared via Internet-based capabilities.

b. Develop and maintain threat estimates on current and emerging Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities into OPSEC education, training, and awareness activities.

d. Ensure that all use of Internet-based capabilities that collect user or other information is consistent with DoD 5240.1-R (Reference (j)).

3. ASD(PA). The ASD(PA), in addition to the responsibilities in section 4 of this attachment, shall:

a. Maintain a registry of external official presences.

b. Provide policy for news, information, photographs, editorial, community relations activities, and other materials distributed via external official presences.

c. Provide guidance for official identifiers for external official presences.

4. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall, within their respective Components:

a. Approve the establishment of external official presences.

b. Ensure the implementation, validation, and maintenance of applicable IA controls, information security procedures, and OPSEC measures.

c. Ensure that computer network defense mechanisms that provide adequate security for access to Internet-based capabilities from the NIPRNET are in place, effective, and compliant with DoD Instruction O-8530.2 (Reference (k)).

d. Educate, train, and promote awareness for the responsible and effective use of Internet-based capabilities.

e. Monitor and evaluate the use of Internet-based capabilities to ensure compliance with this DTM.

f. Coordinate with USD(I) regarding the use of all Internet-based capabilities that collect user or other information, to ensure compliance with Reference (j).

5. DoD COMPONENT CHIEF INFORMATION OFFICERS (CIOs). The DoD Component CIOs shall:

a. Advise the ASD(NII)/DoD CIO and ensure that the policies and guidance for use of Internet-based capabilities issued by ASD(NII)/DoD CIO are implemented within their Component.

b. In coordination with Component OPSEC and Public Affairs offices, provide advice, guidance, and other assistance to their respective Component Heads and other

Component senior management personnel to ensure that Internet-based capabilities are used responsibly and effectively.

c. Assist their respective Component Head to ensure effective implementation of computer network defense mechanisms as well as the proper use of Internet-based capabilities through the use of existing IA education, training, and awareness activities.

d. Establish risk assessment procedures to evaluate and monitor current and emerging Component Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Component Public Affairs Office, assist their respective Component Head in evaluating external official presences' intended use.

6. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM). The CDRUSSTRATCOM, in addition to the responsibilities in section 4 of this attachment, shall:

a. In accordance with Unified Command Plan 2008 (Reference (l)), direct the defense and operation of the DoD Global Information Grid (GIG).

b. Assess risks associated with the use of Internet-based capabilities, identify operational vulnerabilities, and work with the ASD(NII)/DoD CIO to mitigate risks to the GIG.