DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

MAR 25 2010

SAIS-GKM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Responsible Use of Internet-based Capabilities

1. References:

a. Directive-Type Memorandum 09-026, Responsible and Effective Use of Internet based Capabilities, 25 February 2010.

b. CIO/G-6 Memorandum, Use of Social Media Tools, 27 August 2009.

2. This memorandum provides updated guidance to the Army regarding the use of Internet-based Capabilities, and is based on policy released by the Deputy Secretary of Defense (reference a). This policy supersedes prior social media guidance released in August 2009 (reference b).

3. Per DoD policy, the NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD components. Commanders at all levels must continue to defend against malicious activity affecting Army networks. They therefore may take actions to limit access to Internet-based capabilities on a temporary basis in order to ensure that a mission is safeguarded or to preserve operations security.

4. Social media sites are often deployed in an environment that is not under the Army's direct control. Commanders, Soldiers and civilians affiliated with the Army must follow the requirements outlined in the enclosures to ensure that Army networks are protected and that operations security is maintained.

5. The point of contact for this memorandum is Ms. Amber Pittser; she can be reached at amber.pittser@us.army.mil or 703-602-0274.

JASorenson

2 Encls

JEFFREY A. SORENSON
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER
U.S. ARMY FORCES COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY EUROPE AND SEVENTH ARMY
U.S. ARMY CENTRAL
U.S. ARMY NORTH
U.S. ARMY SOUTH
U.S. ARMY PACIFIC
U.S. ARMY SPECIAL OPERATIONS COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY STRATEGIC COMMAND
EIGHTH U.S. ARMY

CF:
COMMANDER
U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH SIGNAL COMMAND
U.S. ARMY MEDICAL COMMAND
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY CORPS OF ENGINEERS
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY TEST AND EVALUATION COMMAND
U.S. ARMY RESERVE COMMAND
U.S. ARMY INSTALLATION MANAGEMENT COMMAND
U.S. MILITARY ENTRANCE PROCESSING COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY
DIRECTOR, U.S. ARMY ACQUISITION SUPPORT CENTER

Enclosure 1 - Guidelines for Responsible Use of Internet-based Capabilities

1. References:

a. Directive-Type Memorandum 09-026 – Responsible and Effective Use of Internet-based Capabilities, 25 February 2010.

b. CIO/G-6 Memorandum, Use of Social Media Tools, 27 August 2009.

c. 5 CFR Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

d. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 4 December 2008.

e. Army Regulation 25-2, Information Assurance, 23 March 2009.

f. Army Regulation 25-400-2, The Army Records Information Management System (ARIMS), 2 October 2007.

g. Army Regulation 360-1, The Army Public Affairs Program, 15 September 2000.

h. Army Regulation 380-5, Department of the Army Information Security Program, 29 September 2000.

i. Army Regulation 530-1, Operations Security, 19 April 2007.

j. DODD 5230.09, Clearance of DoD Information for Public Release, 22 August 2008.

k. DODD 5500.7-R, Joint Ethics Regulation, 29 November 2007.

2. Definitions:

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 (DoD) or the Federal Government. Internet-based capabilities include collaborative tools, such as social media, user-generated content, social software, e-mail, instant messaging and discussion fora (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).

External official presences (EOPs). Official public affairs activities conducted on non-DoD sites on the Internet (e.g., Combatant Commands' fan pages on Facebook, CIO/G-6 presence on Twitter). EOPs are established on commercial venues for the purposes of creating a transparent information-sharing environment and gaining feedback from the public.

Official public affairs activities. Defined in DoD Instruction (DODI) 5400.13.

3. Effective immediately the NIPRNET must be configured to provide access to Internet-based capabilities across all Army Commands. Army commanders shall:

a. Continue to defend LandWarNet from malicious activity (e.g., distributed denial-of-service attacks, intrusions) and take immediate action, as necessary, to secure Army networks.

b. Continue to deny access to sites with prohibited content (e.g., pornography, gambling and hate sites).

c. Temporarily limit access to Internet-based capabilities on an as-needed basis in order to preserve operations security (OPSEC), to safeguard a mission or to address bandwidth constraints.

4. Social networking sites provide opportunities for adversarial groups, such as foreign intelligence services, to glean personal information for use in directly targeting Army and DoD users. All Army personnel have a personal and professional responsibility to ensure that no information that might place Soldiers in jeopardy or be of use to adversaries (including local criminal elements) be posted to public Web sites. Sensitive organizational information, to include Controlled Unclassified Information (CUI), shall not be discussed on any externally facing Web site. The following includes, but is by no means a comprehensive list of, examples of information that should never be published on a public Web site:

a. Classified information

b. Casualty information before the next-of-kin has been formally notified by the Service concerned

c. Information protected by the Privacy Act

d. Information regarding incidents under investigation

e. Information considered Essential Elements of Friendly Information (EEFI)

f. For Official Use Only information

g. Information identified on the current Critical Information List

h. Personally Identifiable Information (PII)

i. Sensitive acquisition or contractual information

5. It is imperative that OPSEC and Information Assurance (IA) regulations be followed in accordance with Army Regulations 25-2, 530-1 and 380-5. Army personnel must safeguard classified and sensitive information in all online communications and must understand that online communications on the .com domain are directed at the public. Contacts made through online communications with the public are unverified and therefore should not be trusted.

6. All Army OPSEC officers should update their OPSEC Orientation and Annual Refresher Briefings to include training regarding the vulnerabilities associated with the use of internet and social media sites. OPSEC officers who need assistance with the development of materials to include in Command briefings should contact the Army OPSEC Support Element, 1st IO Command, at 703-428-4785 or 703-428-4506. ACOM, ASCC and DRU OPSEC program managers are required to report the status of updates made to their awareness programs through the annual reporting process, conveyed in AR 530-1, Appendix I.

7. Commanders must maintain up-to-date critical information lists and must ensure that all employees are trained to protect against the public release of sensitive information. Commanders shall ensure that public affairs officers and Web site managers work closely with OPSEC officers to put in place adequate processes to prevent inadvertent disclosure of information, including CUI, via the public domain.

8. To assist in identifying risks associated with social media sites and to provide advice on secure implementation, each Army organization that is considering the establishment of an EOP will contact the appropriate IA manager and Privacy Act official. The requirements of the information security program address the safeguarding and disclosure of both classified and sensitive information, and both will be afforded protection against unauthorized disclosure (commensurate with the level of classification and sensitivity assigned). All Army personnel are responsible for ensuring that classified and sensitive information and materials are adequately protected from compromise.

9. Policy governing the usage of EOPs.

a. All EOPs must have approval from the Office of the Chief of Public Affairs (OCPA).

b. All EOPs must be a component of official public affairs activities and registered with OCPA at http://www.army.mil/media/socialmedia. All EOPs must be able to be clearly identified through the use of official Army/Command logos, must provide links to the organization's official public Web site on the .mil domain, and must clearly indicate their role and scope. Internal agency business will not be conducted on publically accessible EOPs.

c. Due to exploitation and elicitation exposure and risks, EOPs will not be utilized for personal use and must be linked to an Army Knowledge Online (AKO) email address. Content posted on these sites by the site administrator(s) will not be political or discriminatory, and will not endorse, appear to endorse or show favoritism to non-federal entities. Content or views posted on these sites by the site administrator(s) must reflect U.S. Government policy and may not appear to endorse views contrary to U.S. Government policy.

d. Organizations that utilize EOPs must: validate the security and management of the systems and networks to be used; ensure that content contributors annually complete updated OPSEC training, as described in paragraph 6 of this document; and ensure public affairs, privacy and OPSEC reviews of content before release or disclosure. All information contained on publicly accessible Web sites is subject to the policies and clearance procedures described in AR 360-1, chapter 5, for the release of information to the public. Furthermore, all organizations engaging in social media/EOPs must comply with records management requirements detailed in AR 25-400-2.

10. The Army Web Risk Assessment Cell shall add the sites listed at OCPA's registry, referenced at paragraph 9b, to its regular rotation of sites to be monitored in order to assess compliance with security requirements and to monitor for fraudulent or objectionable use.

11. Policy governing official use of Internet-based capabilities.

a. Official use of Internet-based capabilities unrelated to public affairs is permitted. Official use would be conducted, for example, to perform research, to collaborate with members of the public or to liaise with other governmental entities.

b. Individuals using Internet-based capabilities for official use must ensure that any material posted is relevant and accurate and provides no information not approved for public release. Liaison with public affairs and OPSEC staff should be maintained to ensure organizational awareness of these activities.

c. When applicable, links to official Army content hosted on externally facing Army owned/operated sites must be provided.

d. All personal opinions must be accompanied by a disclaimer (e.g., "This is my opinion and does not constitute an endorsement, opinion or official position of the U.S. Army.").

12. Policy governing personal use of Internet-based capabilities.

a. Soldiers, DoD/Department of the Army employees, and contractors may establish personal accounts on social media sites. However, personal accounts should not: be established with government email addresses, employ the use of government logos, be used to conduct official business, release official agency information, or be used as an official communication device related to the employee's government job or activities.

b. In some cases public figures, Public Affairs officers and other Army personnel may engage through Internet-based capabilities where the line between personal and professional accounts cannot be clearly defined. In such cases, Army personnel should ensure that any official business communication is carried over to an official platform.

c. Agency personnel utilizing or accessing social media technologies must comply with the Joint Ethics Regulation and the Standards of Ethical Conduct for Employees of the Executive Branch (see: Ref A, 5 CFR Part 2635). These rules include prohibition of release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict the use of government computers to access and to manage personal sites during official duty time.

d. The risk to Army and personal information must be clearly understood by all Army personnel who utilize Internet-based capabilities. All members of the Army community must employ sound OPSEC measures, and personnel must discuss the proper use of social media technology with their family members in order to protect them from the inadvertent release of sensitive information. For OPSEC guidance specifically created to share with family members, refer to the following AKO link: https://www.us.army.mil/suite/page/589183.

Enclosure 2 - Matrix of Responsibilities for Use of Internet-based Capabilities

Commanders

Should	Should not
Defend LandWarNet from malicious activity.	Block access to Internet-based capabilities on a prolonged basis.
Ensure that prohibited Internet content is blocked (e.g., pornography, gambling, hate-sites).	
Limit access to Internet-based capabilities TEMPORARILY on an as-needed basis in order to preserve operations security, to safeguard a mission or to address bandwidth constraints.	
Maintain up-to-date critical information lists and ensure that all employees are trained to protect sensitive information from public release.	

Soldiers, Army Civilians and Contractors Affiliated with the Army

Should	Should not
Use Internet-based capabilities to communicate with friends and family during personal time, such as after-duty hours or lunch periods, but must ensure that such contact is of a reasonable duration and frequency.	Allow use of Internet-based capabilities to adversely affect the performance of official duties.
Safeguard classified and sensitive information in all online communications and follow all Information Assurance and Operations Security Regulations (see Army Regulations 25-2, 530-1 and 380-5).	Display official Army seals, logos or other marks on their personal profile on any Internet-based site.
Ensure that all personal opinions stated regarding the Army or Department of Defense are accompanied by a disclaimer (e.g., "This is my opinion and does not constitute an endorsement, opinion or	Use government email addresses to establish personal accounts on Internet-based capabilities or use personal accounts as on official communication

official position of the U.S. Army.").	device for work-related duties.

Organizations Seeking to Establish an External Official Presence (EOP)

Should	Should not
Request/Register EOP through the Office of the Chief of Public Affairs (OCPA) http://www.army.mil/socialmedia.	Post any political or discriminatory content, or endorse, appear to endorse or show favoritism to non-federal entities.
Register any website or account (e.g., Facebook or Twitter) with an Army Knowledge Online email address.	
Utilize official Army/Command logos and provide links to the organization's official public Web site on the .mil domain.	
Ensure that content contributors attend annual OPSEC training.	