DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY, PACIFIC
FORT SHAFTER, HAWAII 96858-5100

REPLY TO
ATTENTION OF

APCG

14 Jun 10

MEMORANDUM FOR All Personnel, U.S. Army Pacific, U.S. Army Installation Management Command – Pacific Region, and Tenant Commands

SUBJECT: Use of Social Networking Sites Policy Memorandum 10-15

1. References:

a. CIO/G6 Memorandum, Responsible Use of Internet-based Capabilites, 25 Mar 2010.

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

c. CIO/G6 Memorandum, Use of Social Media Tools, 27 Aug 2009.

2. The above references provide guidance regarding the official and unofficial use of internet-based collaborative technologies, also known as social media tools. Recognizing the DOD intent to provide Internet-based capabilities, to include social networking sites, the Pacific LandWarNet (PLWN) NIPRNET shall be configured to provide access to Internet-based capabilities across the Pacific Theater. Although using these capabilities can enhance mission effectiveness, Operations Security (OPSEC) and Information Assurance (IA) regulations must be followed to ensure success of our mission.

3. Social media sites are often deployed in an environment that is not under the Army's direct control. Therefore, protection of sensitive information is the responsibility of the individuals that use these technologies. To prevent inadvertent disclosure of sensitive information, via the public domain, commanders at all levels will ensure adequate training and processes are put into place prior to granting access. All USARPAC MSC/TEC personnel will complete the training package located at https://portal.usarpac.army.mil/staff/g6/iapm/training.

4. It is imperative that the security of Army networks be maintained and that OPSEC rules be followed when utilizing social media and other Internet-based capabilities. Unit commanders are expected to stress the areas of OPSEC and IA while holding our Soldiers, Civilians and Contractors to the highest of standards. At any time, commanders may limit access to Internet-based capabilities in order to safeguard and preserve our informational advantage for an ongoing operational mission.

5. Involving basic common sense and trust, the protection of information is the responsibility of every member of this command and remains paramount. For more information regarding precautions that must be considered before officially using social media sites, refer to the the memorandum from the Office of the General Counsel (in addition to the above references) which is located at the following link: https://www.us.army.mil/suite/folder/18595064.

6. The Point of Contact is Mr. David Boucher, Information Assurance Program Manager, 808-438-9284 or email: USARPAC_IAPM@shafter.army.mil.

BENJAMIN R. MIXON
Lieutenant General, USA
Commanding

DISTRIBUTION:
A, B, C