TMA Privacy and Civil Liberties Office Information Paper

SOCIAL NETWORKING OVERVIEW

Social Networking ◆ May 2010

What is Social Networking?

Social networking is a communication medium that enables individuals, communities and groups of users to interact with each other over the Internet through computers and mobile phones. Social networking services (SNS), including Facebook, MySpace, and Twitter, enable users to share ideas, activities, events and interests within their individual networks. These sites are worldwide in scope and allow people to create a network of contacts that can be reached individually or as a group.

The Department of Defense (DoD) Position on Social Networking:

DoD Directive-Type Memorandum (DTM) 09-026, "Responsible and Effective Use of Internet-based Capabilities" authorizes the responsible use of Internet-based capabilities, including SNS, on the Non-Classified Internet Protocol Router Network (NIPRNET) by military and civilian personnel. Internet-based capabilities are defined as all publicly accessible information capabilities and applications across the Internet in locations *NOT* owned, operated, or controlled by the DoD or the Federal Government. This includes collaborative tools such as SNS, user-generated content, e-mail, instant messaging, and discussion forums.

DTM 09-026 also makes it DoD policy that Commanders and Heads of DoD Components shall:

- Continue to defend against malicious activity affecting DoD networks
- Take immediate and commensurate actions to safeguard missions, including temporarily limiting access to the Internet to preserve Operations Security (OPSEC) or to address bandwidth constraints
- Continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites

Responsible Use of Social Networking and Internet-Based Capabilities:

As the DoD works to include social networking and other capabilities into its communications strategy, it is weighing OPSEC against the increasing need to share information.

DTM 09-026 is a significant step for the DoD in developing the process of becoming an up-to-date source of the information needed by DoD staff and the public. Training and awareness are integral to assuring that all military and civilian staff members and their dependents know and adhere to their legal responsibilities under military and civilian law. It is vital that users understand that they should not be disclosing Personally Identifiable Information (PII) and Protected Health Information (PHI) in their communications. Disclosure of this information could be considered a breach and therefore is not permitted. Additionally, sharing of sensitive information could significantly harm individuals on a personal level via identity theft and could potentially be used to compromise OPSEC.

Substantial emphasis in DTM 09-026 is placed on the responsibility of Commanders and Heads of DoD Components to ensure that users in their commands understand and demonstrate by their actions that they know their OPSEC responsibilities. It is critical that Commanders and Heads of DoD Components make decisions regarding training and counseling to ensure that sound OPSEC practices are followed, and that the DoD is not negatively impacted. As the DoD gains more experience with these tools, additional guidance and information will be made available.

Social Networking Resources:

- Department of Defense, "Responsible and Effective Use of Internet-based Capabilities" Directive – Type Memorandum 09-026, (http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf).
- Department of Defense Directive 5400.11, "DoD Privacy Program" May 8, 2007 (http://www.dtic.mil/whs/directives/corres/html/540011.htm).
- Defense Information Systems Agency, "DoD Information Assurance Awareness" October 2009, (http://iase.disa.mil/eta/iaav8/iaav8/index.htm).
- Federal Trade Commission, "Social Networking Sites" September 2007, (http://www.onguardonline.gov/topics/social-networking-sites.aspx).
- The Privacy Act of 1974, as amended (5 U.S.C. § 552a) (http://privacy.defense.gov/files/pa1974.pdf).