SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

Government Contracts BLOG
For the Latest Updates on Laws Affecting Government Contracts

Government Contracts Blog

Posted at 8:01 AM on November 11, 2010 by Sheppard Mullin

"Loose Tweets Sink Fleets" - What Government Contractors Should Include In Their Social Media Policy

By Michelle Sherman

"Loose tweets sink fleets" is a new twist on a familiar saying. It is also borrowed from the Navy Command Social Media Handbook issued October 15, 2010. The Navy appreciates that social media is widely used, and that a ban on social media is not the answer. Trying to turn a blind eye to the use of social media, or banning its use in the workplace is naive. Whether they are doing it at work or in their free time, people who hold security clearances, or have access to classified or sensitive information, are using Facebook to connect with friends who may be one to three degrees removed. They are connecting with other professionals on Linkedin, and sometimes tweeting about their every day activities on Twitter.

Any shred of doubt that your employees are using social media should be quickly dispelled by the following. Facebook fan pages for the military services and defense contractors number in the thousands. Some of the more popular pages include the National Guard (610,450+ fans) Marines (436,000+), US Marines in Afghanistan (20,450+), Navy (222,000+), Northrop Grumman Corporation (6,790+), and BAE Systems Land & Armaments (2,160+).

The issuance of the Navy Social Media Handbook is a good reminder that government contractors should include a social media policy in their employment manuals. Because government contracts may involve work on a classified program with employees holding security clearances, a "cookie cutter" social media policy is not enough.

The social media guidelines that we have discussed in "Why Every Business Should Have A Social Media Policy" are a good starting point. However, there are some additional guidelines that a government contractor may want to include in its social media policy.

First, employees should be encouraged to use the highest privacy settings on Facebook. And, they should appreciate that even "private" information may be made public. There are various back door methods for other people to have access to their information. Comments on a friend's status update are viewable by anyone who is friends with that mutual friend, or anyone else who happens to comment on their post. Also, if you have a Facebook friend who plays one of several popular Zynga game applications (*i.e.*, Farmville, Mafia Wars), then Zynga may have gained access to your information in addition to the friend who is using its application. Courts are also ordering the disclosure of Facebook posts and activity in more and more legal disputes.

Second, it is recommended that employees friend only people they actually know. This applies in particular to employees who have anything in their profile (including fan pages they have liked) that gives an indication that they work for a defense contractor. Other countries spy on the United States, and may use social media to do it. There was a widely reported case in the 1990s of a country allegedly stealing U.S. nuclear design information. Among other things, the country reportedly solicited answers to seemingly benign questions in the

context of scientific symposiums and interactions with U.S. scientists, and then pieced together a highly confidential, U.S. nuclear program. Put simply, it is easy for someone to pose on social media as someone else, and elicit information that may possibly lead to, or result in, an inadvertent disclosure of classified information.

And, finally, successful completion of a government contract may be jeopardized if employees working on it are at risk of losing their security clearances through their uninformed use of social media. A useful starting point is the Questionnaire for National Security Positions, SF-86, and cautioning employees to be mindful of the following questions: (1) having to list foreign nationals with whom the employee has had "close and/or continuing contact" within the last 7 years which may possibly be interpreted to include social media contacts; and (2) describing all instances outside official U.S. government business in which the employee was asked to provide advice even informally by any foreign government official or agency. Linkedin discussion groups are one area for example where someone could inadvertently participate in a work related discussion without realizing that the discussion was initiated by someone working on behalf of a foreign spy organization. Social media does not have country boundaries. For example, the government of North Korea has a Twitter account with over 4,600 followers.

Whether or not company employees have access to social media at work, a government contractor should have a social media policy that addresses the unique nature of its business. A sound policy coupled with training on the informed use of social media makes good business sense for any government contractor.

Authored by:

Michelle Sherman
(213) 617-5405
msherman@sheppardmullin.com