Government Contracts & International Trade Blog
The Latest Updates on Developments Affecting Government Contracts
Presented By SheppardMullin

10 Social Media Must Haves for Your Company's FAR-Mandated Compliance Program

July 15, 2011 by Michelle Sherman

As we discussed here last November, the United States Navy, the other military services, and the Department of Defense, have all recognized that their personnel are using social media and have responded by establishing detailed social media policies. Similarly, there is not a shred of doubt that your company's employees are using social media. And, just like the military services and DoD, if you're a government contractor then you must establish a social medial policy—and it cannot be a "cookie cutter" version of standard corporate social media policies. Among other things, it must address the risk of classified information being leaked, and the ways in which your employees' security clearances can be put in jeopardy if they are not using social media prudently.

Put simply, your social media policy is an extension of the compliance programs mandated by FAR 52.203-13 (Contractor Code of Business Ethics and Conduct). The social media practices discussed below should be incorporated into the ethics training that government contractors are required to give pursuant to FAR 52.203-13. These practices will help bring your company into line with what the government is doing with respect to social media activity by government contractors and their employees. This list is intended to supplement recommendations for corporations engaged in the commercial sector, and is not exhaustive.

1. Adopt a social media policy that reflects the policies adopted by your primary government customers—Air Force, Navy, Army, Department of Defense—and include their basic list of “Do’s” and “Don’ts” in your policy. Don’t try to prohibit lawful protected activity such as complaining about work conditions or compensation/benefits, or whistle blowing.

2. Re-emphasize the importance of reporting improper activity through channels, including the company’s obligations under FAR 52. 203-13. You cannot prevent employees from discussing protected activity on social media sites, but you can emphasize the importance of reporting inappropriate activity through established internal procedures.

3. Implement an effective employee training program on the use of social media that addresses the relationship between such use and the company’s mandatory disclosure obligations under its government contracts. For example, employees need to understand that, while they are free to discuss activities for which the company has a disclosure obligation under FAR 52.203-13 on social media, their discussion could place the company at risk if the same information is not reported internally to enable an appropriate investigation to be conducted.

4. Employees should be instructed that information disseminated through social media that reflects a lack of professionalism, unethical behavior, or potential criminal misbehavior on the part of company employees could have a negative impact on a future determination as to the company’s responsibility. In some cases, it could result in the employee being barred from working on government contracts.

5. Employees who have security clearances should be given special instructions (*e.g.* do not connect with people they do not know (it could be a foreign national), use the highest privacy settings, and be mindful of

what would need to be disclosed on the SF-86 Questionnaire). Your employees should be made aware that publicly available information on social networking sites is being considered in their background investigations for security clearances and program access. Further, information that reflects a lack of professionalism, unethical behavior, or potential criminal misbehavior may prevent them from having a security clearance.

6. Update your e-discovery policies and procedures and make sure that you include social media activity and cloud computing because it is discoverable.

7. Update your document retention policy to make sure you are capturing and storing the social media activities of your company, and don't forget employees conducting business from their smart phones and tablets.

8. Update your Sarbanes-Oxley Act compliance program to ensure that financial information posted on your Facebook fan page, Twitter, website, etc. is updated to reflect material changes in financial condition and operations. Do not release financial information on social networking sites that you have not also published in a press release.

9. Train your HR department, managers, and anyone making employment decisions so they do not use information from social networking sites to discriminate against anyone based on protected factors under federal or state law. Set up protocols so protected factors are not considered and take steps to assure that your equal employment affirmative action programs include appropriate use of social media.

10. Take reasonable measures to protect your trade secrets and data subject to limited rights under your government contracts. Update your confidentiality agreements and computer use policies with employees. Clearly communicate what are the company's trade secrets

and limited rights information and the ways in which use of them is restricted.

Authored by:

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