



# Employees Should Consider Security Risks While Socially Networking

Cassandra Locke | DCMA Public Affairs

*Defense Contract Management Agency employees are reminded not to divulge agency and Department of Defense information while using social media sites. (U.S. Navy photo by Mass Communications Specialist 2nd Class Gregory Mitchell)*

**Social networking can be worthwhile and advantageous, but it can also lead to risky operational and personal security situations.**

Information posted on social networking sites such as Facebook, MySpace, LinkedIn, Twitter and YouTube can spread like wildfire, so Defense Contract Management Agency employees need to understand that they are accountable for any information

released without proper authorization and coordination.

Employees with questions as to whether information is restricted from public release are required to contact the DCMA Public Affairs Office for review and coordination.

“With the expanded use of social networking sites, it is a good time to remind everyone that all DCMA employees have a responsibility, on and off duty, to ensure

**“Social networking profiles can be adjusted to protect your privacy and control who has access to the information you put out.”**

— Roland Grondin, Defense Contract Management Agency security officer

Department of Defense information is protected against unauthorized disclosure to include release to the general public,” said Jackie Noble, DCMA Congressional and Public Affairs director.

“It is required that official DoD information intended for public release undergo both a public affairs and security review prior to release,” added Noble.

DoD Directive 5230.09 defines official DoD information as all information that is in DoD’s custody and control, relates to information in the department’s custody and control, or was acquired by DoD employees as a part of their official duties or because of their official status within the department.

DoD information can include classified information, technical information, operational plans and operational procedures. It can also include privileged information, personnel rosters and results of operations. “DCMA employees deploying overseas should not post their flight information, duty station, rotation schedule or provide descriptions of overseas military facilities and their capabilities,” said Noble.

Noble added posting DoD information to social networking sites is an unauthorized release to the general public. “It’s critical DCMA employees understand that they are accountable for any

**“All Defense Contract Management Agency employees have a responsibility, on and off duty, to ensure Department of Defense information is protected against unauthorized disclosure to include release to the general public.”**

— Jackie Noble, DCMA Congressional and Public Affairs director

information put out to the general public,” said Noble.

Employees should also consider being vigilant not only from an operational standpoint but also to protect personal interests. According to Roland Grondin, DCMA security officer, the Internet has become the preferred method of gathering information. He said employees should consider not posting personal information such as a Social Security number, address, phone numbers, children’s after-school activities, photos, financial information, birth year, etc.

Grondin said to be cautious of posting information that could be used to identify a person’s current physical location. Updating a current status message by posting a person’s whereabouts may invite security risks.

“Deploying DCMA members and members of the Armed Forces have a role in their families’ security. These members who are constantly worrying about the

safety and security of family members will not be focused on their missions,” said Grondin.

Grondin urges employees to remain aware of the risks presented with the widespread dissemination of information and recommends employees who use these sites learn how to adjust the available safety features.

“Social networking profiles can be adjusted to protect your privacy and control who has access to the information you put out,” said Grondin.

As technology advances in this digital age, it is crucial DCMA employees are mindful of the information posted on social networking sites to protect both the agency’s interests and its employees. 

*For more information about the unauthorized release of public information, visit [https://home.dcma.mil/Guidebook/Common\\_Info\\_Tasking\\_Etc/dc11-067.htm](https://home.dcma.mil/Guidebook/Common_Info_Tasking_Etc/dc11-067.htm).*

## The following are several examples where public affairs and security reviews are required prior to release by a Defense Contract Management Agency employee:

**Example 1:** A DCMA employee deployed overseas is considering writing about his/her job experiences and posting the information on a social networking site. Any discussion of Department of Defense information would require prior approval.

**Example 2:** A DCMA employee wants to forward an e-mail containing official DoD information from his or her DCMA account to a personal or commercial account.

**Example 3:** A DCMA employee is giving a speech/presentation at a conference, convention or to a civic organization where non-DoD participants are in attendance.

**Example 4:** A DCMA employee is considering posting presentations, photos and/or products/information containing information about DCMA or DoD to a non-DoD website.

*(Courtesy of DCMA Information Memorandum 11-067, Unauthorized Public Release of DoD Information)*