STATE OF WEST VIRGINIA
OFFICE OF THE ADJUTANT GENERAL
1703 COONSKIN DRIVE
CHARLESTON, WEST VIRGINIA 25311-1085

James A. Hoyer
Major General, WVARNG
The Adjutant General

(304) 561-6316
DSN: 623-6316
FAX: (304) 561-6327

19 September 2013

MEMORANDUM FOR All Units/Activities of the West Virginia Army and Air National Guard

SUBJECT: Responsible Use of Social Networking Sites and other Internet-based Technologies

1. The Internet is a valuable tool for commanders and service members to communicate their units' activities to the general public, family members and friends. Research shows journalism moving away from television, newspapers and radio, particularly among younger audiences who use the Internet as their primary source for acquiring and sharing information.

2. It is important that all service members realize the broad reach – both positive and negative – that Internet-based forms of communication have on our organization and the importance of maintaining a presence in these emerging domains. No longer is Public Affairs solely responsible for communicating the organization's message. Now, all service members are communicators who must be entrusted to provide information about topics within their areas of expertise.

3. While useful as part of the West Virginia National Guard's overall communications strategy, it is important to note that Internet technologies, particularly social media networking sites, provide opportunities for adversarial groups to glean both operational and personal information to target our organization and its members. As such, all personnel have a responsibility to ensure that no information that might place West Virginia National Guard operations or service members in jeopardy, or otherwise be of use to potential adversaries, be posted to public Web sites.

4. This memorandum provides updated guidance to all West Virginia National Guard members on the proper use of Internet-based technologies, including social media sites. It should be used in conjunction with my memorandum of 13 May 2010, SUBJ: External Social Networking Sites, and appropriate Operations Security (OPSEC) and Information Assurance (IA) regulations.

5. My point of contact for questions regarding responsible use of the Internet is Lt. Col. Todd Harrell or Sgt. Anna-Marie Ward, State Public Affairs Office. They can be reached at 304-561-6763 or 6764.

JAMES A. HOYER
Major General, WVARNG
The Adjutant General

POLICY ON RESPONSIBLE USE OF THE INTERNET TO COMMUNICATE INFORMATION ABOUT THE WEST VIRGINIA NATIONAL GUARD

General

1. The Internet, particularly social networking sites, provides a valuable tool for commanders and service members to stay in touch with families during deployments, to publicize unit training activities, and to announce job openings or new benefit programs, among other things. Coupled with traditional media and community outreach programs, effective use of the Internet can increase significantly the West Virginia National Guard's visibility in local communities.

2. The Department of Defense recently issued policy requiring military organizations to provide access to social media sites through unclassified military computer networks. Sites such as Facebook, Flickr, Twitter and YouTube are now viewable from most computers on the .mil domain. This access allows for use of the Internet to better communicate with our internal and external audiences in the public domain.

3. As social media sites are often deployed in the public domain and outside the military's direct control, commanders, service members and civilians affiliated with the West Virginia National Guard must follow basic guidelines to ensure Dept. of Defense networks are protected and operations security maintained. All personnel must understand that online communications in the .com domain are directed at the public, and public contacts made through online communications cannot be trusted until verified.

4. There are two kinds of Internet posts – official and unofficial (personal). Official Internet posts involve content released in an official capacity by a National Guard Public Affairs Office. Unofficial posts are not initiated by any part of the National Guard or reviewed within any National Guard approval process.

Official use of external social media or other Internet sites

1. Commanders must maintain up-to-date critical information lists and ensure all employees are trained to protect against public release of sensitive information. The following includes, but is by no means a comprehensive list, types of information that should never be published on a public Web site:

- Classified information
- Casualty information before the next-of-kin has been formally notified by DoD
- Privacy Act information
- Information regarding incidents under investigation
- Essential Elements of Friendly Information (EEFI)
- For Official Use Only (FOUO) information
- Information identified on the current Critical Information List
- Personally Identifiable Information (PII)
- Excessive information on families of deployed soldiers (home town, names and ages of spouse and children, address, spouse occupation, etc. – individual elements are acceptable, but putting together too much information could make family members easily identifiable)
- Sensitive acquisition or contractual information
- Internal documents or information that the National Guard has not officially released to the public, including memos, e-mails, meeting notes, message traffic, white papers, public affairs guidance, pre-decisional materials or proprietary information

2. To assist in identifying the potential consequences of an official Internet presence and to gain advice on secure implementation, all West Virginia National Guard organizations considering establishment of a social networking site or other external Internet presence will contact the State Public Affairs Office PRIOR TO launching the site. Additional policy guidelines include:

- Each site must have an appointed administrator to review content and coordinate with State Public Affairs Office.
- Each site must be a component of official public affairs activities and clearly identifiable through use of official command logos.
- Each site must provide a link to the West Virginia National Guard official public Web site on the .mil domain and must clearly indicate the purpose and scope of the site.
- All sites must be linked to the Army Knowledge Online (AKO) or official Air Force e-mail account of the site administrator.
- Sites should be established as "fan" pages instead of "friend" pages. The purpose of a fan page is to encourage interaction and two-way communication, and "friending" may result in denial of access to those who could help spread the West Virginia National Guard message.
- Site administrators will inform the State Public Affairs Office of existing sites and provide a link and access to their sites.
- Content posted will not be political or discriminatory and will not endorse, or appear to endorse or show favoritism to, non-federal entities. Content or views posted on official sites must reflect U.S. Government policy and may not appear to endorse views contrary to such policy.
- State Public Affairs Office will monitor all sites and may require modification and/or removal of content posted in violation of appropriate OPSEC/Information Assurance regulations or policy.
- Units that maintain external official sites must ensure that site administrators complete OPSEC training annually and review all information to be posted for public affairs, OPSEC and privacy considerations prior to posting.
- Government computers are authorized to be used to access official sites that have been properly registered with the State Public Affairs Office and had content approved by the site administrator.
- Internal official business may not be conducted on external social media sites.

3. Service members not in compliance with this policy may be referred to their command for appropriate disciplinary action.

Unofficial (Personal) use of social media or other Internet sites

1. Service members and civilian employees may establish personal accounts on social media sites off the .mil domain.

2. Personal accounts should not be established:

- Using government e-mail addresses
- Employing the use of West Virginia National Guard or other government logos
- In the name of the West Virginia National Guard, West Virginia Air National Guard or West Virginia Army National Guard or any unit within these organizations
- As a means of conducting official business or releasing official agency information
- As an official communication device related to the employee's government job or activities.

3. When communicating about the National Guard in unofficial posts, Guard members may identify themselves as such and include their rank, military component and status. However, when expressing personal opinions Guard members should identify that they are speaking for themselves and not on behalf of the National Guard. It is recommended that personnel use a disclaimer on personal sites on which they've identified themselves as members of the West Virginia National Guard. Such a disclaimer might read: "The postings on this site are my own and don't represent the National Guard's positions or opinions."

4. Service members, family members, or civilian employees who have already created personal social networking sites in the name of the West Virginia National Guard, their specific service or unit are asked to remove these pages from the social networking site they occupy. Service members not in compliance with this policy may be referred to their command for appropriate disciplinary action.

5. Service members and others affiliated with or employed by the West Virginia National Guard should use privacy settings on social networking sites so posted personal information and photos can be viewed only by their "friends." It is also important to recognize that social network "friends" and "followers" could affect determination in background investigations for security clearances.

6. Service members accessing social media sites must comply with the Joint Ethics Regulation and Standards of Conduct for Ethical Conduct of Employees of the Executive Branch. These rules prohibit the release of non-public information, require appropriate disclaimers of opinions being expressed, and restrict use of government computers to access and manage personal sites during duty hours.

7. Service members should discuss the proper use of social media technology with family members in order to protect them from the inadvertent release of sensitive information.

Do's and Don'ts for Official Sites (list does not include every possible situation)

- **DO** post photos of training or deployment events once cleared by the site administrator.
- **DO** publicize unit activities (remember OPSEC!).
- **DO** release good news stories about soldiers or the unit.
- **DO** list military positions or full-time positions that may be available in your unit.
- **DO** post information on educational, financial or veteran's benefits available to service members or their families.
- **DO** correct errors and misrepresentations made by others about the National Guard, but do so respectfully and professionally – contact the Public Affairs Office if uncertain about the need for a response

- **DON'T** post information that will compromise operational security (mission specifics, times, dates, locations, number of personnel, etc.).
- **DON'T** be afraid to report suspicious activity or something that goes against the social media policy.
- **DON'T** post graphic, obscene, explicit or racial comments or material or abusive, hateful material intended to defame anyone or any organization.
- **DON'T** post anything offensive or inappropriate that would bring discredit upon yourself or the West Virginia National Guard
- **DON'T** post solicitations or advertisements. This includes promotion or endorsement of any financial, commercial or non-governmental agency.
- **DON'T** post comments that suggest or encourage illegal activity.

Conclusion

Internet communication provides a new toolset that commanders can use to achieve military public affairs objectives. The rules of the game have clearly changed as the paradigm has changed from a message-pushing process to two-way communication. Because soldiers and airmen are the best voices of the organization, we need to tell the West Virginia National Guard story in a thoughtful, engaging and exciting manner – by taking advantage of the Internet tools used by corporate and industry leaders.

But opening our .mil networks and allowing creation of external official sites on the .com domain also exposes our organization to greater risk of unauthorized disclosure of sensitive information. It is imperative that every service member, family member, and civilian employee connected to the West Virginia National Guard understand the public affairs, OPSEC and Privacy Act considerations present in this level of openness. Only through improved education and awareness of the pitfalls inherent in using the Internet can we protect sensitive information and our members while increasing our visibility and standing among key audiences that are so vital to our continued success.