

Tennessee National Guard
3041 Sidco Dr.
Nashville, TN 37204

Joint Public Affairs Office
2 May 2013

***Use of Social Media for Tennessee National Guard Units
Standard Operating Procedures (SOP), Version 2***

COMPLIANCE WITH THIS INSTRUCTION IS MANDATORY

OPR:
Tennessee Military Department
JFHQ PAO

Certified By:
JFHQ/PAO
Maj. (Ret.) Randy Harris

These procedures implement the *U.S. Army Social Media Handbook, Version 3, Social Media and the Air Force, Version 2*, and DTM 09-026, *Responsible and Effective Use of Internet-based Capabilities* by establishing local procedures and supplementing Army and Air Force guidance as appropriate. These Standard Operating Procedures (SOPs) establish procedures for members of the Tennessee Army National Guard and Tennessee Air National Guard utilizing Social Media for promotion and further communication within their respective units. In addition to these SOPs, members are responsible for complying with other appropriate Army and Air Force directives. This SOP is in compliance with DoD Directive (DoDD) 8500.01E, DoDI 8500.2, DoDD 5400.11, DoDD 5230.09, DoD Manual 5205.02-M, DoDD 5010.2, DoD 5200.1-R, and DoD 5240.1-R.

STANDARD OPERATING PROCEDURES
TABLE OF CONTENTS

Preface

1 – What is Social Media?

- 1.1. Social Media
- 1.2. Local Posts can have Global Significance
- 1.3. The Internet is Permanent

2 – Operations Security (OPSEC) and Social Media

- 2.1. Maintaining OPSEC
- 2.2. Regulations
- 2.3. Security
- 2.4. How to Protect Yourself and Your Critical Information when Using Social Media
- 2.5. Checklist for OPSEC for Official Pages

3 – Establishing and Maintaining a Social Media Presence

- 3.1. Social Media Guidance
- 3.2. Terms of Participation to be Posted on Sites
- 3.3. Posting Guidelines
- 3.4. Copyright/Trademark

4 – Tips for Social Media

- 4.1. Tennessee National Guard Guide to Dealing with the News Media
- 4.2. Freedom of Information and Transparency
- 4.3. Privacy
- 4.4. Security
- 4.5. Online Social Media Activities
- 4.6. Expectations for Online Spokespeople
- 4.7. Frequently Asked Questions

Attachment 1 –Web Posting Response Assessment

Attachment 2 – Tennessee National Guard PAO Social Media Presence Request Form

Attachment 3 – References

Preface: Use of Social Media technologies

1. REASON FOR ISSUE: The Tennessee Military Department Joint Public Affairs Office endorses the secure use of approved social networking and social media tools to enhance communication, outreach, and information exchange. This standard establishes policy and enforces DoD and National Guard Bureau policies on the proper use of these tools, consistent with applicable laws, regulations and policies.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Standard provides mandatory instruction for all Tennessee Military Department agencies. As such, they apply to all employees of the Tennessee Military Department, Tennessee Army National Guard, Tennessee Air National Guard, contractors, vendors and all entities that use or whose activities affect official Tennessee Military Department social networking and social media sites.

3. RESPONSIBLE OFFICE: Tennessee National Guard Joint Public Affairs Office - Social Media Manager. The most current version of these standards can be found at the Tennessee Military Department website at <http://tnmilitary.org/SocialNetworks.html>.

CERTIFIED BY:

/s/
Master Sgt. Robin Olsen
Social Media Manager, JPAO
Tennessee Military Department

BY DIRECTION OF THE TENNESSEE MILITARY DEPARTMENT PUBLIC AFFAIRS DIRECTOR:

/s/
Randy D. Harris
Director, TNNG Joint PAO
Tennessee Military Department

1 - What is Social Media?

1.1. Social Media

1.1.1. **Definition.** The definition of Social Media as it pertains to the Tennessee National Guard Soldiers and Airmen is any external official presence that represents the Tennessee National Guard or one of its units on any social media site.

1.1.2. **Social Media Sites.** Social Media sites include Facebook, Twitter, MySpace, YouTube, Flickr, Digg, Delicious, blogs, and any other online platform that can be used to disseminate information other than the unit's official Web page. Official uses of Internet-based capabilities unrelated to public affairs are permitted. However, because these interactions take place in a public venue, personnel acting in their official capacity shall maintain liaison with public affairs and operations security staff to ensure organizational awareness.

1.2. Local Posts can have Global Significance

1.2.1. **Never disclose non-public information.** Never disclose non-public information about the Tennessee National Guard or violate operational security. Ensure that the information posted is relevant and accurate, and provides no information not approved for public release, including Personally Identifiable Information (PII). Provide links to official DoD content hosted on DoD-owned, -operated, or -controlled sites where applicable.

1.2.2. **Public Positions.** Be aware that taking public positions online which are counter to the Tennessee National Guard's interests could cause or result in conflict.

1.2.3. **Rights.** Give credit where credit is due and don't violate other people's rights. Do not claim something that is not yours. If you are using or referring to another's content, make certain that they are credited for it in your post and that they approve of you using their content. Include a disclaimer when personal opinions are expressed (e.g., "This statement is my own and does not constitute an endorsement by or opinion of the Department of Defense").

1.2.4. **Convergence.** Online efforts spread faster than traditional email, fax, or mailings. For example, a converged product employed by the Air Force Public Affairs Agency was a collaboration of internal and external print, photos and social media efforts. It highlighted an impromptu memorial in the Area of Responsibility for a fallen Soldier, who was the brother of an Air Force U-2 crew chief. Photos were emailed to AFPAA and were posted on various Web sites, including CNN's iReport. The photos and story were then posted to Reddit, LinkedIn, StumbleUpon, Delicious, Digg and other social media sites, with the whole process taking three hours. In less than a week, it had been viewed hundreds of times. The photo was eventually the lead photo for CNN.com.

1.3. The Internet is Permanent

1.3.1. **Permanence.** Once information is published online, it is essentially part of a permanent record, even if Soldiers and Airmen “remove” or “delete” it later, or attempt to make it anonymous. The way you answer an online question may be accurate to you, but inaccurate to others. Keep in mind the “world view” when participating in online conversations.

1.3.2. **Be responsible for your duty assignment.** The Tennessee National Guard understands that Soldiers and Airmen sometimes engage in online social media activities at work for legitimate purposes and that these activities may be helpful for the Tennessee National Guard Public Affairs. However, Soldiers and Airmen are encouraged to exercise sound judgment and common sense to prevent online social media sites from becoming a distraction at work.

2 - Operations Security (OPSEC) and Social Media

2.1. **Maintaining OPSEC.** Sharing what seems to be even trivial information online can be dangerous to loved ones and fellow Guard members. America's enemies scour blogs, forums, chat rooms and personal websites to piece together information that can be used to harm the United States. When using social media, avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.

2.1.1. **What is OPSEC?** Operations Security is the process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. Operations Security protects critical information from adversary observation and collection in ways that traditional security programs cannot. Basically, OPSEC is identifying what small pieces of information can be put together to obtain a larger picture of operations.

2.2. **Regulations.** Army Regulation 530-1, Operations Security (OPSEC), prohibits disclosure of critical and sensitive information in any public domain to include, but not limited to, the World Wide Web, open source publications and the media. Do not publicly disseminate or publish photographs displaying critical or sensitive information. Do not publicly reference, disseminate, or publish critical or sensitive information that has already been compromised.

2.2.1. **Required OPSEC courses.** Per the U.S. Army Social Media Handbook, Version 3, Social media managers are required to take two OPSEC courses. The Information Assurance Training Center offers the computer-based Social Media and Operations Security Training Course (ia.signal.army.mil/sms.asp). It is a self-paced class that takes approximately 60 minutes to complete. Social media managers must also take the DISA Social Networking Class (iase.disa.mil/eta/sns_v1/sn/launchPage.htm). The class is available 24 hours a day, seven days a week and takes approximately 50 minutes to complete.

2.2.2. **Requirements for Operations Security.** All content must be submitted to and approved by the commander or the organization's release authority prior to posting. All content must be in accordance with organization public affairs guidance, as well as Army and Air Force regulations. ***Be vigilant. Never become complacent when it comes to OPSEC. Check social media presences within your organization for OPSEC violations. Never stop working to protect OPSEC. Once the information is out there, you can't get it back.***

2.3. **Security.**

2.3.1. **Typical types of attacks.**

- *Access Privileges* - anyone using the Internet with "administrator" privileges is inviting attackers to permanently invade their computers; and social media sites have

become notorious targets for attackers looking for users that are unsuspecting and unaware of these risks.

- *Cross-Site Scripting (XSS)* - a security vulnerability that allows attackers to insert code into a target user's web page.
- *Identity Spoofing* - usually involves one person, system, or website successfully masquerading as another by falsifying identity-related information and thereby being treated as a trusted user or system by another user or program.
- *Malware Downloads* - one of the highest risks associated with social media is the ability of attackers to exploit known vulnerabilities, allowing them to covertly hide executable programs on unsuspecting users' computers, which give the attackers the ability to take over the computer and use it for any purpose they desire.
- *Social Engineering* - an attack that involves gathering and using personal information about a target in a deceitful manner in order to convince the target to provide the attacker permissions to obtain or access restricted information.
- *URL Spoofing* - an attack in which a legitimate web page is reproduced on a server under the control of the attacker and then a target is directed to this site, thinking that they are on the legitimate site.

2.3.2. Security Items to Consider. Take a close look at all privacy settings. Do not reveal sensitive information about yourself such as schedules and event locations. Ask “What could the wrong person do with this information?” and “Could it compromise the safety of myself, my family or my unit?” Consider turning off the GPS function on your Smartphone, as it can be utilized to expose specific geographical location information that can be devastating to National Guard operations.

2.3.3. Social Engineering/Individual Targeting. Since social networking encourages socialization and collaboration with not only friends but with strangers, the potential for social engineering attacks is magnified. Attackers can use social engineering techniques to lure the user to take an action that leads to an adverse action to the user. The more pieces of information an adversary can collect, the more opportunities they have to meet their objectives. An adversary may be a hacker on the other side of the world simply targeting you to obtain a good credit card or bank account number, or an adversary could be a militant, collecting data to identify members of the armed forces to either inflict harm on the member(s) or collect small pieces of data leaked by many members to consolidate a picture of our capabilities and plans. An adversary may never target you directly, rather they may use data they collect from you and others to harm other servicemembers in the AOR.

2.3.4. Due to the relative vulnerability of social media and social networking sites to security exploits, it is important to be cautious when using these technologies. In order to prevent potential harm, users of social networking sites should minimize the amount of information an attacker is likely to gain from a successful attack.

2.4. How to protect yourself and your critical information when using social media. It is easy to collect and consolidate information made available through public social networking sites. It is possible to build a picture of an individual based solely on information made public on

the internet. In addition, it is remarkably easy to obtain information ‘protected’ by the privacy controls of a social media profile.

2.4.1. User applications on social networking sites and unauthorized and/or malicious software programs. There are many third party applications in social media that users can add to their profile such as sharing music, and playing video games. These applications may have capabilities that increase the likelihood of a user unwittingly disclosing personal information. When an individual installs an application, it typically allows the developer to see private information from the installer’s profile. People can be duped into going to third party sites to download applications. Once at these sites, the social networking site no longer controls what may be downloaded to your computer.

2.4.2. Safety precautions. Verify the identity of those who attempt to friend you on social media sites. A name and photograph do not constitute verification. Lock down your profile by making it private. Always be suspicious. Do a web search on yourself, your unit, and family members to see what information is posted to the internet. Review information and photos before posting. Be aware of any public affairs implications of your activities. Watch out for your friends and ensure they aren’t posting any OPSEC disclosures. Data aggregation from different sources could reveal sensitive or even classified information. Educate your fellow unit members, family members and friends on the risks associated with social networking. Don’t use the same password for each form of social media you use. Do not use information commonly associated with you (family name, pet names, etc.).

2.4.3. Risk Reduction. To reduce some of the risks , the following actions are recommended:

- Do not allow users to have "administrative privileges" on government/state owned computers that access the Internet.
- Each unit information security officer/NCO must review selected technologies and associated plug-ins to identify potential security vulnerabilities prior to their use.
- Use a username/password that is different from other network login IDs and passwords.
- ***Transferring sensitive information over these technologies is prohibited.***
- These technologies make a user's computer vulnerable to attacks. It is suggested to configure social media outlets in a way that does not receive messages from unauthorized users. Do not ban messages altogether, as this is an important way for servicemembers and the community to connect with the unit.

2.5. Checklist for OPSEC for official pages.

- Designate members of your team responsible for posting content to the official online presence and make sure those individuals are current on all OPSEC training.
- Make sure all content is submitted to and approved by the commander or the organization’s release authority.
- Make sure all content is posted in accordance with organization Public Affairs Guidance and Army and Air Force regulations.
- Monitor your social media presence and make sure external social media users are not posting sensitive information on your official pages. Monitor your Facebook wall and comments posted to your YouTube, Flickr and Blog presences.
- Produce training Materials and conduct regular social media OPSEC training within your team and with other units in your organization.
- Distribute social media OPSEC training to the families of your Soldiers and Airmen. It’s important to keep them just as informed and up-to-date as the Soldiers and Airmen in your unit.
- Be vigilant. Never become complacent when it comes to OPSEC. Check social media presences within your organization for OPSEC violations. Never stop working to protect

2.5.1. Making dangerous social media posts safer.

Dangerous	Safer
My Soldier is in XYZ at ABC Camp in ABC City, Afghanistan.	My Soldier is deployed to Afghanistan.
My Airman will be leaving Kuwait and heading to Iraq in three days.	My Airman deployed this week.
My Soldier is coming back at XYZ time on XYZ day.	My Soldier will be home this summer.
My family is back in Edwardsville, IL.	I’m from the Midwest.

3 - Establishing and Maintaining a Social Media Presence

3.1. Social Media Guidance.

3.1.1. **Social Media Policy and Guidelines.** Some key elements of building trust to be considered when posting content or maintaining a social network site: be open with the public when declaring what the Tennessee National Guard values and principles are, provide a means for direct invitation or key publics to engage in dialogue, develop methods of engagement to maintain dialogue with key publics, deliberate mirror imaging of actions and the information we communicate, take certain risks with negative public statements and allow for a public forum to defend your position, manage the Tennessee National Guard's reputation and relationships built on social networks (by ensuring there are adequate methods to maintain decorum, rules of engagement and site/content moderation), and provide full disclosure of who you are when engaging in the social media network. Post only approved content and have a method in place to ensure thorough content review before posting, (OPSEC, FOUO, FOIA, SAPP, etc.)

3.1.2. Regulations.

- Two OPSEC courses, see section 2.2.1.
- Register the social media site with the Department of Defense, <http://www.defense.gov/RegisteredSites/SubmitLink.aspx>; and National Guard Bureau - send an email to socialmedia@ng.army.mil. You can check for your posting with NGB here: http://www.ng.mil/features/Social_media/default.aspx. The Assistant Secretary of Defense for Public Affairs (ASD(PA)) maintains an external official presences list on www.Defense.gov. (The Office of the Chief of Public Affairs has the right to deny any page during the approval process if one or more of these guidelines are not followed.
- Must have JFHQ Public Affairs Office approval in writing. The Tennessee National Guard PAO Social Media Presence Request Form, attachment 2, will meet this requirement. If not in compliance, an unofficial statement must be present.

3.1.3. **Requirements for Social Media Sites.** All social media platforms designed to promote any part of the Tennessee National Guard must adhere to the following standards:

- Must be categorized as a government page.
- Include the Commander approved names and logos, not nicknames or mascots.
- Branding (official names and logos) across all social media platforms are uniform.
- Include a statement acknowledging this is the "official" page of your unit or organization, as well as a terms of use statement. See section 3.2, below.
- Change Facebook setting to only show posts made by the page itself, and not from fans of the page.
- Facebook pages must include "Posting Guidelines" under the "Info. Tab".
- Be recent and up-to-date. Post must be no older than one month.

- Adhere to OPSEC guidelines.
- Should not be used as a place for personal advertisement nor endorsement.
- In addition to DoD and NGB, all Army pages must be registered through the U.S. Army at www.army.mil/socialmedia.

3.2. Terms of participation to be posted on sites. These should be posted in a visible location on the social media page.

- Welcome, this is the official Tennessee National Guard (Facebook, Twitter, YouTube, Flickr) for (Unit) where you will find the most recent information and news about (Unit). It is our goal to provide the public with information and news about (Unit) and allow for an open forum of discussion about (Unit) topics.
- If you are looking for our official web page, please visit (official page).
- Please feel free to express your opinion about the Tennessee National Guard in an objective and respectful way that allows for a continued information relationship.
- While this is an open forum, it's also intended to maintain respect for those who participate (i.e. family-friendly). Please keep your comments clean.
- Participants are asked to follow our posting guidelines below. Violation of the guidelines below may result in your post being removed.

3.3. Posting Guidelines.

- We do not, under any circumstance, allow graphic, obscene, explicit or racial comments or submissions, nor do we allow comments that are abusive, hateful, or intended to defame anyone or any organization.
- We do not allow solicitations or advertisements. This includes promotion or endorsement of any financial, commercial or non-governmental agency. Similarly, we do not allow attempts to defame or defraud any financial, commercial or nongovernmental agency.
- We do not allow comments that suggest or encourage illegal activity.
- You participate at your own risk, taking personal responsibility for your comments, your username and any information provided.
- Lastly, the appearance of external links on this site does not constitute official endorsement on behalf of the Tennessee National Guard or Department of Defense.

3.4. Copyright/Trademark. Do not use logos that you do not have permission to use. Soldiers and Airmen cannot include copyrighted or trademarked material on their social media platforms. This includes embedding a song, or linking to unattributed artwork. Social media platforms exist to help individuals connect and express their personalities, but this should be done without using a copyrighted material unless they are authorized to do so by the copyright or trademark owner.

4- Tips for Social Media

4.1. Tennessee National Guard guide to dealing with the news media. Within established guidelines, it is our responsibility to talk to the media (and subsequently, the public). Leaders, Soldiers and Airmen who refuse to talk to the media give the impression that they are withholding information.

4.1.1. There is no such thing as off the record with social media. If it's posted online, the media can quote you.

4.1.2. Stay in your lane. Talk about your job, your responsibilities, and other matters within your expertise of control. Avoid speculating and answering "what if" questions—you can't predict the future.

4.1.3. Local support. Do talk about the support from family/friends you have received since your deployment.

4.1.4. Audience. Always remember who the audience will be. If you have complaints, consult your chain of command first.

4.1.5. Discussions with reporters. All discussions with reporters are "on the record" – if you do not want to read it in the paper or hear it on TV, don't say it.

4.1.6. Protect classified information. Protect classified information and preserve operational security. Exact numbers and locations of troops and equipment, ongoing or future operations, and rules of engagement are not releasable. If classified or sensitive information is inadvertently released through words or photography, servicemembers are not authorized to confiscate film, audio/video tapes or reporters notes. Report the incident by the quickest means possible to the unit commander or the public affairs officer.

4.1.7. Honesty. Be honest, open and forthright. If you do not know the answer to a question, simply say, "I don't know." Don't be evasive—If a question is classified, simple tell the reporter so. Think about your answer before opening your mouth—you do not have to answer immediately.

4.1.8. Communicate clearly to your audience. This is your opportunity to communicate to a large audience. Make your answer clear and relevant, and use examples that are easily understood (avoid using jargon and acronyms).

4.1.9. Professionalism. Be professional even if the reporter is aggressive or the questions seem silly. If the reporter interrupts you, pause, let the reporter finish, then continue your response.

4.1.10. Speak for you, not the reporter. Don't let the reporter put words in your mouth. Don't repeat their "buzz words." You don't have to accept their facts or figures as the truth. Don't be afraid to ask a reporter to repeat a question.

4.1.11. **Relax.** You're telling a great story about what the Tennessee National Guard does—this is your chance to educate. If you feel uncomfortable, or have any questions or concerns about dealing with the media, contact the Joint Public Affairs Office at DSN 683-0633 or 0662.

4.2. **Freedom of information and transparency.** Freedom of information and transparency of releasable, unclassified and non-sensitive information will be made readily available to the public, provided upon request. Our organization's activities are legitimate and the assumption is, an informed public will agree with this principle. This guidance is formalized in law by the Freedom of Information Act that emphasizes the importance of transparency in military activities. The Tennessee National Guard does not condone manipulating the social media flow by creating posts designed to mislead followers and control a conversation. Every website, "fan page", or other online destination that is ultimately controlled by the Tennessee National Guard must make that fact known to users and must be authorized according to applicable internal protocols in order to track and monitor the state's National Guard collective online presence. All Soldiers and Airmen engaging in social media must disclose this to their readers, when they're associating with them, whether it is done in an official or un-official capacity. Tennessee National Guard PAOs or the OIC must monitor whether Guard members are complying with this principle.

4.3. **Privacy.** The privacy of individual servicemembers must be protected. The Privacy Act of 1974 set this principle into law. Soldiers and Airmen must remain conscientious with regard to any personally identifiable information that we collect, including how we collect, store, use, or share that information; all which should be done pursuant to applicable privacy policy, laws and information technology rules.

4.4. **Security.** Security to operations, personnel, equipment and facilities must be anticipated and evaluated before information is communicated to the public. Examples include preventing the premature disclosure of dates, time and locations of deployments and homecoming to and from the continental United States.

4.5. **Online social media activities.** The Tennessee National Guard respects the rights of its Soldiers and Airmen to use blogs and other social media tools not only as a form of self-expression, but also as a means to further explain the National Guard story. It is important that all Guardsmen are mindful of the implications through social media and online conversations that make reference to the Tennessee National Guard. These Guardsmen are potentially viewed as spokespersons and should be made aware that the Tennessee National Guard may be held responsible or accountable for their behavior, statements and opinions in that capacity.

4.5.1. **Expectations for personal behavior in social media.** There is a big difference between speaking "on behalf of the Tennessee National Guard" and speaking "about" the Tennessee National Guard. This following set of principles refers to personal or unofficial online activities where Soldiers and Airmen might refer to the Tennessee National Guard:

4.5.1.a. **Adhere to the UCMJ and other applicable policies.** All Soldiers and Airmen, from officers to enlisted, must adhere to Department of Defense policy, Secretaries of the Army and Air Force Instructions and National Guard orders and directives related to online media in every public setting.

4.5.1.b. **Soldiers and Airmen are responsible for their actions.** Anything a National Guard member posts that can potentially tarnish the Tennessee National Guard image will ultimately be their responsibility. The Tennessee National Guard encourages Soldiers and Airmen to participate in the online social media space, but urge them to do so properly, exercising sound judgment and common sense.

4.5.1.c. **Be a ‘scout’ for compliments and criticism.** Even if a Guard member is not an official spokesperson, they are one of the most vital assets for monitoring the social media landscape. If a Guard member comes across positive or negative remarks about the Tennessee National Guard online, they should consider sharing it with their local or command Public Affairs Office.

4.5.1.d. **Let subject matter experts respond to negative posts.** You may come across negative or disparaging posts about the Tennessee National Guard, or see third parties trying to spark negative conversations. Unless you are a trained Tennessee National Guard online spokesperson, avoid the temptation to react yourself. Pass the post(s) along to official spokespersons who are authorized to address such comments at the units or command Public Affairs Office.

4.5.1.e. **Be conscious when mixing business and personal lives.** Online, a Guard member’s personal and business personas are likely to intersect. The Tennessee National Guard respects the free speech rights of all Soldiers and Airmen, but they must remember that civilians, fellow Guardsmen and supervisors often have access to the online content that is posted. Soldiers and Airmen must keep this in mind when publishing information online that can be seen by more than friends and family, and know that information originally intended just for friends and family can be forwarded on. Online content can, and will, be shared with thousands or more people and is nearly impossible to retract once it has entered the public arena.

4.6. **Expectations for online spokespeople.** Just as with traditional media, Soldiers and Airmen have an opportunity to provide an inside perspective to the Tennessee National Guard’s reputation online and to engage and participate in potentially thousands of online conversations that mention the Tennessee National Guard every day. Remember that you are representing the Tennessee National Guard, as well as the Army/Air Force. As a Guard member, it is important that your posts convey the same journalistic excellence the National Guard instills in all of its communicators and public affairs professionals. How you conduct yourself in the online social media space not only reflects on you—it is a direct reflection on the Tennessee National Guard. Fully disclose your affiliation with the Tennessee National Guard. It is never acceptable to use aliases or mislead. Keep records of your online interactions and monitor the corresponding

conversations with whom you engage. The internet is permanent. Once something is posted, it cannot be removed or changed to anonymous. Provide meaningful content. If your complete thought cannot be squeezed into a character-restricted space, provide a link to an online space where the message can be expressed completely and accurately. Collaborate and ask for guidance when needed. There is never a topic so important or urgent that it requires and immediate post. Always gather the facts, know the rules, and understand the audience. If you need assistance, contact the Joint Force Headquarters Public Affairs Office.

4.7. Frequently Asked Questions.

Q: Who can manage my units Facebook page?

A: Currently, social media manager is not an MOS or AFSC, so it is often viewed as an additional duty. Often, Public Affairs Specialists take the role of social media managers since much of the content loaded to social media sites is news and command information. But it doesn't necessarily have to work that way. If a Soldier or Airman is motivated and the commander approves him managing the site, anyone can run a social media site as long as they work closely with their unit's public affairs office in accordance with DTM 09-026, *Responsible and Effective Use of Internet-based Capabilities*.

Q: What happens if someone is impersonating me or someone in my unit?

A: Report the impersonation to the social media platform by clicking on the report button or emailing the platform directly. If the platform is unresponsive and the impersonation becomes a threat to reputation or personal safety, contact the Online and Social Media Division and we will assist in getting the page or profile removed.

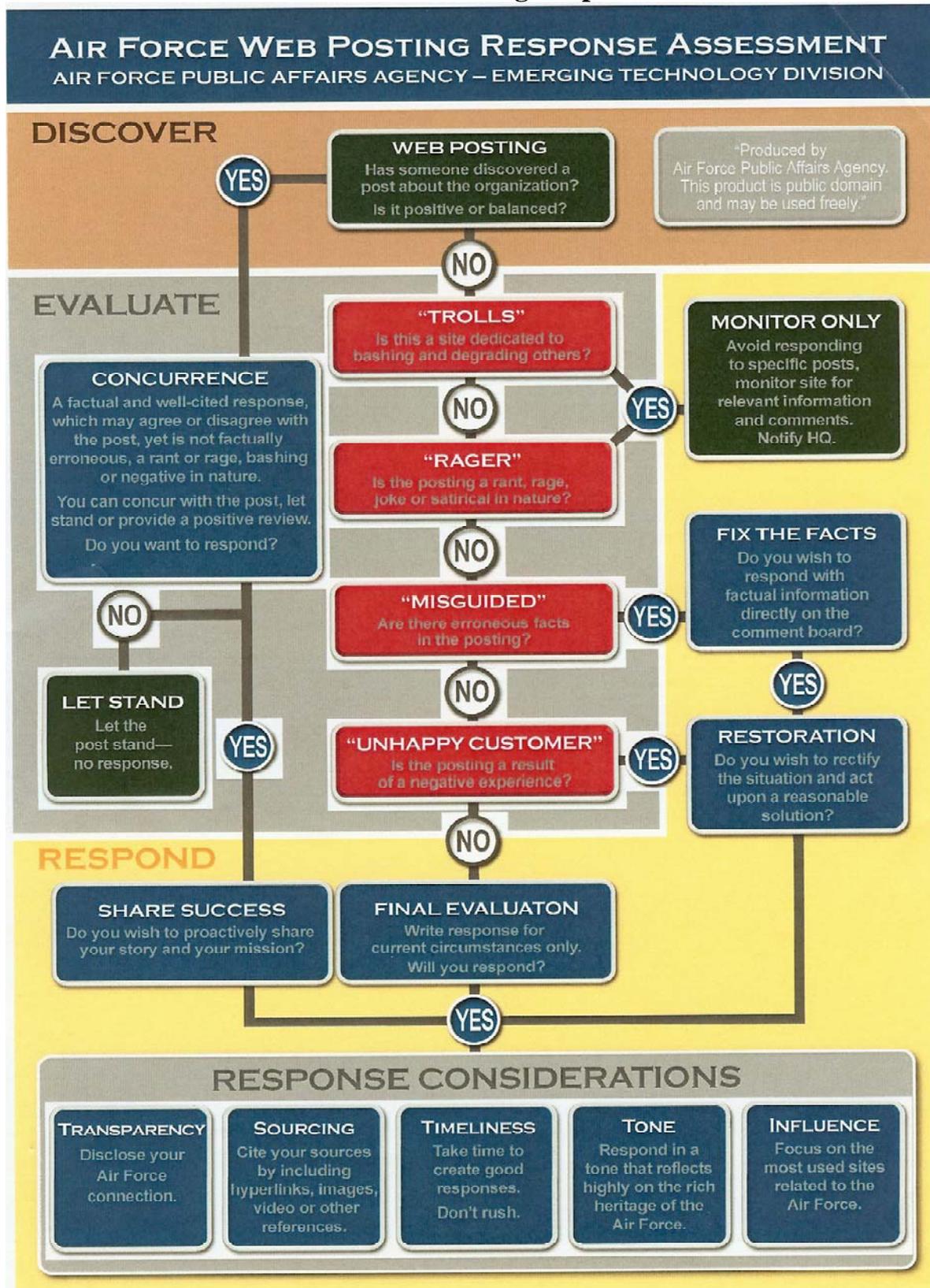
Q: A family member has posted something to one of the social media presences that violates OPSEC. What do I do now?

A: The first thing you should do is engage that person in as discreet a manner as possible and ask them to remove the post immediately. Explain that information isn't appropriate for conversation online. If the person refuses or persists you have the option to block or report them. This should be used as a last resort because it is difficult to undo and only shifts the problem to out of view—the person will more than likely continue to post inappropriate content somewhere else. In either case, you should notify your command so that they are informed of the OPSEC breach.

Q: I did some searching and found that this command already has a non-official Family Group on Facebook (Twitter, YouTube, etc.). What should I do?

A: Many commands have unofficial social media presences established by former Soldiers and Airmen, Veterans, or just fans excited about that command. We do not have the right to remove these presences nor would we want to unless they portrayed themselves as an official presence. In the meantime, work with the command leadership to determine if you want to approach the page and/pr simply monitor it and chime in when you have information to add. You may also want to contact the administrator and touch base. They may be eager to have your participation. Regardless, this should not stop you or the command from creating an official presence for the command and its families.

Attachment 1 – Web Posting Response Assessment



Attachment 2 – Tennessee National Guard PAO Social Media Presence Request Form

Tennessee National Guard Joint Public Affairs Office
Social Media Presence Request Form

Date: _____
Requestor Name (and rank): _____
Unit: _____
Phone: _____
Email: _____
Fax: _____

Social Media Presence Being Requested:
(Check all that apply and provide link.)

- Facebook _____
- Twitter _____
- YouTube _____
- Blog _____
- Other (Specify) _____

Does social media presence use official logo:

- Yes
- No

Does social media presence have official statement:

- Yes
- No

Has social media presence been registered with:

- Department of Defense
- National Guard Bureau
- No (Reason) _____

Required OPSEC Training Completed:
(Submit certificates with request form.)

- Social Media and Operations Security Training Course (ia.signal.army.mil/sms.asp) and
- DISA Social Networking Class (iase.disa.mil/eta/sns_v1/sn/launchPage.htm)
- or
- I, _____, agree to complete the required OPSEC training courses to maintain the above social media presence(s). I will ensure all administrators of above presence(s) complete the same training and all certificates will be forwarded to the TNNG JPAO within 15 days of this request.

Unit Commander Approval

Name: _____
Signature: _____
Date: _____

TNNG JPAO Approval

Name: _____
Signature: _____
Date: _____

Attachment 3

References

Handling Dissident and Protest Activities Among Members of the Armed Forces, DoD Directive 1325.06. <http://www.dtic.mil/whs/directives/corres/pdf/132506p.pdf>

Joint Ethics Regulation DoD 5500.7-R.
http://www.dod.mil/dodgc/defense_ethics/ethics_regulation/jer1-6/doc

National Guard Recruiting and Retention Social Media Guidebook.
<http://www.slideshare.net/thenatlguard/army-national-guard-recruiting-and-retention-social-media-guidebook>

Navigating the Social Network: Air Force Guidance to effective Social Media use.
<http://www.af.mil/shared/media/document/AFD-120327-048.pdf>

Online Social Media Guidance. <http://www.usmc.mil/usmc/Pages/SocialMediaGuidance.aspx>

Political Activities by Members of the Armed Forces, DoDD 1344.10.
<http://www.dtic.mil/whs/directives/corres/pdf/134410p.pdf>

Responsible and Effective Use of Internet-based Capabilities, DTM 09-026.
<http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026/pdf>

Social Media and the Air Force, Version 2.
<http://www.af.mil/shared/media/document/AFD-091210-043.pdf>

U.S. Army Social Media Handbook, Version 3.
<http://www.slideshare.net/USArmySocialMedia/army-social-media-handbook-2012>