



DEPARTMENT OF THE ARMY  
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND  
501ST MILITARY INTELLIGENCE BRIGADE  
UNIT 15282  
APO AP 96205-5282

IADK-Z

01 OCT 2016

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Brigade Policy Letter #28 – Social Media Policy

1. References:

- a. INSCOM Policy Memorandum #31, INSCOM Public Affairs Program (Public Release of Information and Social Media Web Site Management).
- b. United States Forces Korea (USFK) Command Policy Letter #5, Operations Security (OPSEC).
- c. The United States Army Social Media Handbook, Version 3.2, March 2014.
- d. Office of the Chief of Public Affairs, Online and Social Media Division, Memorandum (Standardizing official U.S. Army external official presence (social media), 10 Jan 2014.
- e. AR 360-1 (The Army Public Affairs Program) 25 May 2011.
- f. AR 530-1 (Operations Security (OPSEC)) 19 Apr 2007.
- g. AR 340-21 (The Army Privacy Program) 5 July 1985.
- h. Alaract 289/2013 (Army Operations Security (OPSEC) Training for External Official Presence (EOP) Operators) 29 Oct 2013.
- i. Defense Media Activity (Guide to Keeping Your Social Media Account Secure) [http://www.defense.gov/documents/WEB\\_Guide\\_to\\_Keeping\\_Your\\_Social\\_Media\\_Accounts\\_Secure\\_2015.pdf](http://www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf).
- j. U.S. Army Records Management and Declassification Agency (Privacy Act Overview training) <https://www.rmda.army.mil/privacy/docs/Privacy-Act-Overview-Training.pptx>.

2. This memorandum provides guidance on the establishment, maintenance, and use of unit social media platforms to include but not limited to Facebook, Twitter, Flickr,

IADK-Z

SUBJECT: Brigade Policy Letter #28 – Social Media Policy

YouTube, etc. The establishment of the 501st Military Intelligence Brigade's Social Media program is to use social media to enhance our communication with current and former unit Soldiers, Family Members, Civilians, veterans, and the local community while keeping well within the bounds of the Army Privacy program, Operations Security (OPSEC), DoD Standards, Army Regulations, and INSCOM policies.

3. The use of Social Networking Sites (SNS) has dramatically increased over the past decade. Many of our Soldiers, Family Members, and DoD personnel use these sites to communicate with loved ones, share their story, and obtain information. As leaders begin to utilize these tools to enhance communication and share the unit story, it is vital to monitor threats to operation security (OPSEC) and ensure users (Soldiers, Family Members, and DoD personnel) are aware of the risks associated with social media and what precautions to take.

4. This policy applies to all individuals who have administrative rights to post content on official social media pages of units under the 501st MI BDE.

5. Responsibilities:

a. Unit Commanders will:

(1) Accept responsibility for unit Social Media Program.

(2) Appoint individuals to serve as the Unit Public Affairs Representative (UPAR) to act as administrators on unit social media sites.

(3) Ensure UPARs receive proper training through the US Army's Social Media link (<http://www.army.mil/media/socialmedia/>) and proper annual OPSEC and Privacy Act training, UPARs should work closely with unit OPSEC officers to ensure posts and published unit information are within INSCOM's and DoD guidelines. Additionally, UPARs must also take the "Army OPSEC Training for EOP Operators" at <https://iatraining.us.army.mil/> and the Defense Information Systems Agency's social networking class: [http://iase.disa.mil/eta/sns\\_v1/sn/launchPage.htm](http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm).

(4) Ensure official unit Social Media Sites are registered through the U.S. Department of Defense (<http://www.defense.gov/socialmedia/>), adhering to INSCOM's Policy Letter #31 and all requirements posted on the US Army's Social Media link (<http://www.army.mil/media/socialmedia/>).

(5) Develop a social media strategy to ensure 1) UPARs and other administrators understand the commander's vision and unit's message to the public, 2) UPARs and other administrators are aware of content posting approval guidelines, and

IADK-Z

SUBJECT: Brigade Policy Letter #28 – Social Media Policy

to ensure site remains active (recommend at least one post a week) with relevant content to engage the public/audience.

(6) Educate Soldiers, Family Members, and DoD Civilians on the importance of OPSEC when utilizing social media.

b. Unit Public Affairs Representative will:

(1) Must take the "Army OPSEC Training for EOP Operators" at <https://iatraining.us.army.mil/> and the Defense Information Systems Agency's social networking class: [http://iase.disa.mil/eta/sns\\_v1/sn/launchPage.htm](http://iase.disa.mil/eta/sns_v1/sn/launchPage.htm). Be knowledgeable of INSCOM Policy #31 and U.S. Army Social Media guidance (<http://www.army.mil/media/socialmedia/>).

(2) Must take the "Privacy Act Overview" training at <https://www.rmda.army.mil/privacy/docs/Privacy-Act-Overview-Training.pptx>. Be knowledgeable and keep a copy of the Army's Personally Identifiable Information (PII) User's Guide (<https://www.rmda.army.mil/privacy/docs/Army-PII-Users-guide.pdf>).

(3) Follow OPSEC guidelines when posting information on a social media site (public forum). UPARs and site administrators should familiarize themselves with INSCOM Policy #31 for complete listing and details of information requiring higher approval prior to release. When in doubt contact unit OPSEC officer and obtain approval in writing prior to posting information or pictures.

(4) UPARs and site administrators are responsible for documenting and removing any OPSEC violations. Take a 'screenshot' of the violation for record and remove the post or picture. Immediately notify the unit OPSEC Officer and unit commander.

(5) Negative comments often appear on social media sites and public online forums, do not automatically delete these comments. Deleting all negative comments can potentially tarnish credibility and reduce followers. Only delete or block comments/users when a comment/posting is in direct violation of the posting guidelines and terms of participation, or are clearly malicious or derogatory in nature. All deletions should be recorded, take a 'screenshot' and keep record as to why deletion occurred. For more information on DoD Social Media User Agreement, visit <http://www.defense.gov/socialmedia/user-agreement.aspx>.

(6) If you suspect that your unit social media site has been targeted by a phishing campaign or has been hacked, notify the unit OPSEC officer and unit commander. Report any suspected phishing or hacking to [ocpa.osmd@us.army.mil](mailto:ocpa.osmd@us.army.mil)

IADK-Z

SUBJECT: Brigade Policy Letter #28 – Social Media Policy

and see specific guidance for addressing these issues at each social media site at [http://www.defense.gov/documents/WEB\\_Guide\\_to\\_Keeping\\_Your\\_Social\\_Media\\_Accounts\\_Secure\\_2015.pdf](http://www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf).

c. Unit Operation Security Officer will:

(1) Be aware of the unit's social media sites and administrators.

(2) Occasionally monitor site for suspicious activity.

(3) Review and approve/deny UPAR's social media posting or informational release request. Forward to Brigade or INSCOM for further review if needed.

---

6. Policy:

a. All official and unofficial unit social media sites, including spouse's and FRG groups/pages will be made aware to the commander of their presence. All official unit pages must be approved by unit commander and registered in accordance with DoD social media guidelines.

b. Administrators for unit social media sites must be documented, trained in OPSEC, and unit OPSEC officer must be aware of their role.

c. It is highly encouraged for each unit with an active social media site has at least a timeline/posting guidance and/or social media strategy.

d. Social media is a valuable tool, connecting Families, Soldiers, and communities. As our FRGs utilize social media sites to distribute information and provide a platform for Families and Soldiers to connect, it is important to stay vigilant and remember OPSEC at all times.

(1) Family Readiness Groups should and are encouraged to provide all FRG members with the U.S. Army Social Media OPSEC presentation and the FBI Briefing on Identity Theft located on the U.S. Army's Slide Share (<http://www.slideshare.net/usarmysocialmedia>).

(2) FRGs should refrain from posting 1) specific unit movement, 2) when/if a family is going on vacation or leaving the house vacant, 3) gossip, or 4) information concerning MIA/KIA prior to release by DoD.

e. Soldiers using social media must abide by the Uniform Code of Military Justice (UCMJ) at all times. Commenting, posting or linking to materials that violates UCMJ or

IADK-Z

SUBJECT: Brigade Policy Letter #28 – Social Media Policy

basic rules of Soldier conduct is prohibited. Social media provides the opportunity for Soldiers to speak freely about their activities and interests. However, Soldiers are subject to UCMJ even when off duty, so talking negatively about supervisors or elected officials or releasing sensitive information may result in adverse action as appropriate.

7. Point of contact for this memorandum is SFC Karim B. Clarke, Public Affairs Officer at DSN: 754-9811, or email [karim.b.clarke.mil@mail.mil](mailto:karim.b.clarke.mil@mail.mil).



DERRICK S. LEE  
COL, MI  
Commanding

DISTRIBUTION:

A