OFFICE OF THE CHIEF OF PUBLIC AFFAIRS

U.S. Army Social Media Handbook

January 2011

Online and Social Media Division
Office of the Chief of Public Affairs
1500 Pentagon
Washington, D.C.

Table of contents

Letter from the Chief of Public Affairs

Team-

You already know that communicating your organization's messages is important. Today, it takes more than press releases to successfully communicate. Being an effective Army communicator today relies on proactive planning, nesting messages, engaging audiences on a variety of platforms, monitoring what is being said both online and in traditional media, and taking a proactive role in telling the Army's story.

As part of that, we need to make sure we use all the tools at our disposal to keep our Soldiers and the general public informed.

Social media is another set of tools that helps us spread the Army message faster than ever. These tools not only help us to respond to a 24-hour news cycle, but also help us lead conversations and participate in the stories. By reaching out to the online community, we're able to be where more and more people get their news, and by doing so, we're better serving our warfighters.

Social media is a powerful communication tool, but it goes beyond just using the tools. It is important to understand the tools and their overwhelming benefits and sometimes dangerous ramifications. It is also important to develop a strategy and execute that strategy while keeping operations security in mind.

I advise you to embrace social media, read through the regulations at the back of this handbook and develop a strong fundamental knowledge of these tools.

I asked the experts in my Online and Social Media Division to create this handbook to help you use these tools as effectively as possible. If you have any questions, contact them at ocpa.osmd@us.army.mil. Stay abreast of the latest things going on in social media by subscribing to our weekly 'Social Media Roundup' by sending a request to that email address.

Our Soldiers and their Family members are the strength of our nation. Nine years of persistent conflict have shaped our shared experiences, which can be told through the social media platforms to assist those new to our Army Family. This builds resiliency in the force and makes our Army strong. Soldiers have always been and always will be our greatest story tellers, and social media tools allow us to tell their story more effectively.

Best of luck as you push forward with your social media endeavors.

//original signed//
STEPHEN R. LANZA
MG, USA
Chief of Public Affairs

Social Media Summary

WHAT IS SOCIAL MEDIA?

Social media represents a shift in the way we as a culture communicate. By using Internet-based platforms like Facebook, Twitter, Flickr and YouTube, social media provides new ways to connect, interact and learn. People no longer look for the news, the news find them. And in the world of social media, the perception of truth can be just as powerful as the truth itself. The Internet moves information quickly, whether for good or bad. Social media, with a variety of available platforms, can instantaneously connect users within a global network, making the transfer of information even more pervasive. Today, social media is so widespread and transparent that you may already be involved even if you are not actively participating. Social media is highly effective tool to use when reaching out to large communities and audiences. But with this substantial ability to connect with the masses, comes risks. Using social media to spread information is becoming the standard. More and more units are using social media to communicate, so it's more important that ever to understand the risks associated with using the various platforms.

ARMY SOCIAL MEDIA

The Army recognizes that social media has the ability to communicate with larger audiences faster and in new ways. It has become an important tool for Army messaging and outreach. The Army uses a variety of social media platforms designed to support a range of media from text, audio, pictures and videos; all of which is generated and maintained by organizations and individuals within the Army Family. The Army understands the risks associated social media and has worked hard to develop training to help Soldiers and family members use social media responsibly.

WHY USE SOCIAL MEDIA?

Soldiers have always been the Army's best and most effective messengers. Today, Army social media enables the Army Family around town, around the country and around the world to stay connected and spread the Army's key themes and messages. Every time a member of the Army Family joins Army social media, it increases the timely and transparent dissemination of information. It ensures that the Army's story is shared honestly and directly to Americans where they are and whenever they want to see, read or hear it. Social media allows every Soldier to be a part of the Army story. By starting a discussion on Facebook, or commenting on a Soldier's story on a blog, all Soldiers can contribute to the Army story. Social media is a cheap, effective and measureable form of communication. The Army uses social media to tell the Army's story, but it also uses social media to listen.

WHAT DOES THE DOD SAY ABOUT SOCIAL MEDIA?

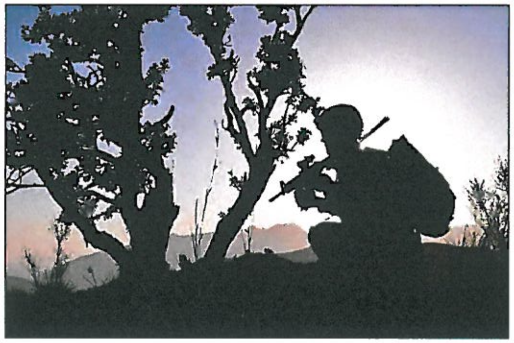
On February 25, 2010, the DoD issued a Directive-Type Memorandum (DTM) providing guidelines for military use of social media and acknowledged "that Internet-based capabilities are integral to operations across the Department of Defense." DTM 09-026 Responsible and Effective Use of Internet-based Capabilities outlined how the NIPRNET should be configured to allow access to Internet-based capabilities across all DoD components. All service branches are using social media at different levels, but this DTM clearly indicates that use of social media in the DoD is authorized.

Social Media for Soldiers and Army Personnel

Members of the Army Family are experiencing a special time in their lives. They have a lot to share with Family, friends and others. Social media is an opportunity to instantly reach out and connect regardless of time, space or distance. The Army encourages members of the Army Family to use social media to connect and tell their stories, but it also advises everyone to do this in a safe and secure manner.

OPSEC AWARENESS

The primary concern when using social media is maintaining operations security. It's important to know that social media is a quickly evolving means of distributing information and that means OPSEC is more important than ever before. All Army leaders should communicate with their Soldiers about the risks of using social media and incorporate social media into their regular OPSEC training.



JOINING SOCIAL NETWORKS

Soldiers will naturally seek out involvement in social media platforms if they haven't already. Social media helps individuals with similar interests connect and interact. Soldiers are authorized to use and belong to a variety of social media platforms as long as their involvement does not violate unit policy and the basic guidelines of the Uniform Code of Military Justice.

LAY OUT THE GUIDELINES

Leaders must engage their Soldiers on social media use. All leaders must communicate social media expectations with their Soldiers. It is important to outline unit policy and make sure all Soldiers know what they can and cannot do when using various social media platforms.

"Our adversaries are trolling social networks, blogs and forums, trying to find sensitive information they can use about our military goals and objectives. Therefore, it is imperative that all Soldiers and Family members understand the importance of practicing good operations security measures."

-Sgt. Maj. of the Army Kenneth O. Preston

FOLLOW THE UCMJ

Soldiers using social media must abide by the Uniform Code of Military Justice at all times. Commenting, posting, or linking to material that violates the UCMJ or basic rules of Soldier conduct is prohibited. Social media provides the opportunity for Soldiers to speak freely about what they're up to or what their interests are. However, Soldiers are subject to UCMJ even when off duty, so talking negatively about supervisors, or releasing sensitive information is punishable under the UCMJ. It's important that all Soldiers know that once they log on to a social media platform, they still represent the Army.

MAINTAINING OPSEC

Sharing what seems to be even trivial information online can be dangerous to loved ones and the fellow Soldiers in the unit -- and may even get them killed. America's enemies scour blogs, forums, chat rooms and personal websites to piece together information that can be used to harm the United States and its Soldiers. The adversary -- Al Qaeda and domestic terrorists and criminals for instance -- have made it clear they are looking.

Social Media for Soldiers and Army Personnel (Cont.)

When using social media, avoid mentioning rank, unit locations, deployment dates, names, or equipment specifications and capabilities.

GEOTAGGING AND LOCATION -BASED SOCIAL NETWORKING

The Army is always working to protect itself against security breaches, but with new technologies come new risks. Today, more than ever, it is vitally important that Army leaders, Soldiers and Army civilians understand what kind of data they are broadcasting and what they can do to protect themselves and their families. Geotagging photos and using location-based social networking applications is growing in popularity, but in certain situations, exposing specific geographical location can be devastating to Army operations. Soldiers should never tag photos with geographical location when loading to photo sharing sites like Flickr and Picasa. Soldiers should not use location-based social networking applications when deployed, at training or while on duty at locations where presenting exact grid coordinates could damage Army operations. While Soldiers are engaged in Army operations, they should turn off the GPS function of their smartphones. Failure to do so could result in damage to the mission and may even put families at risk.

DO NOT VIOLATE COPYRIGHT AND TRADEMARK

Soldiers cannot include any 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 copyrighted material unless they are authorized to do so by the copyright or trademark owner.

SECURITY ITEMS TO CONSIDER

- Take a close look at all privacy settings. Set security options to allow visibility to "friends only."
- 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?"
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly, make sure they don't give away sensitive information.

Social Media Standards for Army Leaders

SOCIAL MEDIA FOR LEADERS

Social media has improved the way we connect and communicate as a culture, but it presents some interesting dilemmas for Army leaders.

ONLINE RELATIONSHIPS

Social media is about connecting, so it's only natural that Army leaders may interact and function in the same social media spaces as their subordinates. How they connect and interact with their subordinates online is up to their discretion, but it is advised that the online relationship function in the same manner as the professional relationship.

SHOULD SOLDIERS "FOLLOW" THOSE IN THEIR COMMAND?

This is also left to the discretion of the Army leader. Ultimately, it depends on how that leader uses social media. If the leader is using social media as a way to receive command and unit information along with installation updates, then following members in a leader's command is appropriate. But if the leader is using social media as a way to keep in touch with family and friends, it may not make sense to follow people in the leader's chain of

LEADER CONDUCT ONLINE

When in a position of leadership, conduct online should be professional. By using social media, leaders are essentially providing a permanent record of what they say, so, if you wouldn't say it in front of a formation, don't say it online. If a leader comes across evidence of a Soldier violating command policy or the UCMJ on social media platforms, then that leader should respond in the same manner they would if they witnessed the infraction in any other environment.

SELF PROMOTION

Using rank, job, and/or responsibilities in order to promote oneself online for personal or financial gain is not appropriate. Such actions can damage the image of the Army and an individual command.

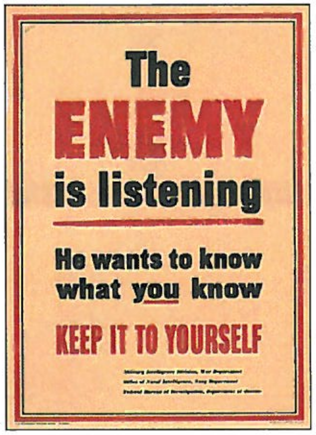
PAID SUBMISSIONS

Treat requests from non-governmental blogs for a blog post as a media request and coordinate with your public affairs officer. It is against Army regulations to accept compensation for such posts.

POLITICAL DISCOURSE

Everything a leader says and does is more visible and taken more seriously. Leaders have a greater responsibility to speak respectfully and intelligently about issues they don't intend to reflect on a command or the Army.

Checklist for Operations Security 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.

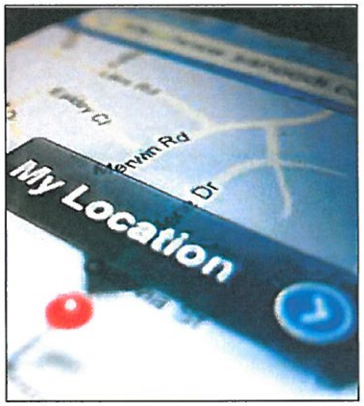
□ Make sure all content is posted in accordance with organization Public Affairs guidance and Army regulations.

□ Monitor your social media presence and make sure external social media users are not posting sensitive information on your official presence. 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. It's important to keep them just as informed and up-to-date as the Soldiers 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 OPSEC. Once the information is out there, you can't get it back.



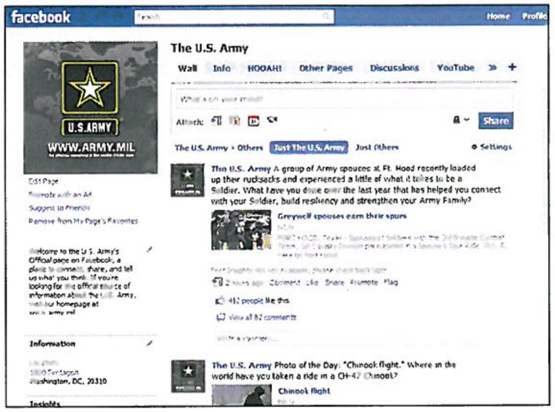
Making dangerous social media posts safer

Dangerous	Safer
My Soldier is in XYZ at ABC Camp in ABC City, Afghanistan.	**My Soldier is deployed to Afghanistan.**
My Soldier will be leaving Kuwait and heading to Iraq in three days.	**My Soldier 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.**

Establishing and Maintaining Army Social Media Presences

MANAGING A SOCIAL MEDIA PRESENCE

Today, the Army understands that social media has increased the speed and transparency of information. It's determining which events make the news and it's setting agendas. More and more Army organizations are using social media for strategic online engagement. Social media is used in garrison environments, operational environments and in Family Readiness Groups. Developing a successful social media presence does not happen overnight. It is a detailed process that requires extensive planning and detailed execution. It all starts with stating the missions, messages and themes of an organization.



The U.S. Army

The U.S. Army A group of Army spouses at Ft. Hood recently loaded up their rucksacks and experienced a little of what it takes to be a Soldier. What have you done over the last year that has helped you connect with your Soldier, build resiliency and strengthen your Army Family?

Greywolf spouses earn their spurs

The U.S. Army Photo of the Day: "Chinook flight." Where in the world have you taken a ride in a CH-47 Chinook?

Chinook flight

Washington, DC, 20310

DEVELOPING A STRATEGY

Once the direction of an organization is established, it's then possible to develop a social media communication strategy. This strategy must be detailed and provide input into all the social media platforms supported by an organization. Language should be conversational, fun and engaging. Asking questions is a good way to get people involved and encourage them to comment. The purpose of using social media platforms is to place your units messages in the social media space. Units should want to find a balance that keeps people coming back to the pages, but also gets the message out. This can be accomplished by mixing the doses of messages with items the audience may find interesting. In today's modernizing Army environment, social media plays an increasingly important role. Social media is not a fad, if the Army ignores it, it will not go away.

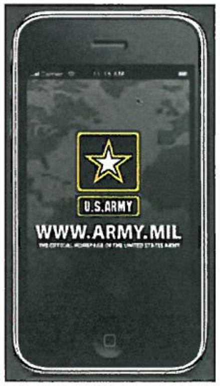
REGISTRATION

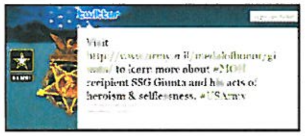
DTM 09-026 requires that all official social media presences be registered with the DoD. Since social media use is so prevalent in today's society, it's important to register and indicate that the presence is official. To register a social media presence with the Army, social media managers should visit: www.army.mil/socialmedia/. Registering on the Army's social media directory also provides other benefits. Once a site is approved, it appears on the Army social media directory. Ads that appear on Facebook are also removed from official Army Facebook presences. Registration ensures that a command presences are included in any USG/DoD Terms of Service (ToS) Agreements. Official use of social media platforms must be in compliance with Army public affairs policy. Content posted to an official social media presence must be either already in the public domain or must be approved for release by the commanding officer. Commands are ultimately responsible for content posted on their platforms.

MEASURMENT

Just 10 years ago, the success and reach of a news story could be measured by the size of a newspaper's circulation or the number of clicks on a website. Today, measurement is about more than just numbers. It's about trends and human feedback. Social media sites like Facebook, Twitter, Flickr and YouTube allow for administrators to track views, impressions and comments. Many sites provide their own analytics tools. By using numbers in conjunction with comments and reader feedback, it's now easier than ever to determine how organizational messages are received and how the audience is responding to the content. Nearly all of the most popular social media platforms offer analytics tools for users. Some of these tools provide graphs and charts, but it ultimately depends on the platform. The different representations of information make for a richer and more depth statistical analysis. Using the analytics tools of each platform can help a unit demonstrate the usefulness of a social media platform, and even highlight the success of a specific social media campaign.

Establishing and Maintaining Army Social Media Presences (Cont.)





Visit http://www.army.mil/medalofhonor/giunta/ to learn more about #MOH recipient SSG Giunta and his acts of heroism & selflessness. #USArmy

ENFORCE POSTING POLICY AND MONITOR COMMENTS

It's good to have a posting policy, but just because a posting policy is in place doesn't mean everyone is going to follow it. Make sure to review wall posts frequently and remove posts that violate the posting policy. Keep in mind that social media doesn't take a break for the weekend. In some instances, weekend activity on Facebook can be busier than the week, so watch the organization's wall every day, even on days off, holidays and weekends.

ENGAGE THE AUDIENCE

Social media is more than just a platform to push command messages, it's a social community. Platforms like Facebook and Twitter, help people bridge enormous geographical gaps to connect, talk and interact. Using social media can be incredibly valuable to a communication strategy, but it needs to be more than just a sounding board for organization messages. It's important to use social media to facilitate the conversation, engage the population and keep people interested in what's being discussed.

LISTEN TO THE AUDIENCE

By watching the wall on a Facebook site, or by reading the comments on a blog post, social media managers can get a feel for what the online community wants to hear about. Sometimes, it's useful to talk to an audience directly. Ask for feedback and suggestions, and then act on that feedback. A social media presence accomplishes very little if the online audience is not interested in what's being said. Listening to an audience can mean the difference between maintaining a successful social media presence or an irrelevant one.

MIX IT UP

Balance the "fun" with the "medicine." It's important to put out command messages and organizational information, but it's also good to keep the page entertaining enough for people to want to follow it. Don't be afraid to have fun by posting interesting links or asking trivia questions. Try posting a photo of the day, or asking a weekly question. Social media is social, so it's important that social media managers don't fall into the trap of talking at their audience.

ANSWER QUESTIONS

Social media communities grow quickly, so it's important to note that once a social media presence grows to a certain size, the population will use it as a resource and possibly ask questions. It's important to spend time responding to questions asked in social media platforms. The community will value this interaction and the one-on-

PROMOTE ORGANIZATIONAL SOCIAL MEDIA PRESENCES

It's important to tell the social media community that you're out there. Attach links to social media platforms at the bottom of press releases and after official emails from your office. The more you get the word about out a social media presence, the faster the community that follows it will grow.

POST CONTENT TO SOCIAL MEDIA PLATFORMS OFTEN

A static social media presence is ineffective. Static pages are boring and visitors to the page lose interest quickly. If content on the page is not regularly updated, people will stop coming by to view the page. Carefully select links to stories, unit videos and photos related to the organization's mission. Social media platforms are designed to support various forms of content, take advantage of that. Once information is cleared by a release authority, post it. Social media moves information quicker than ever, so don't wait for a press release. If the information is there, use it.

BUILD A COMMUNITY

A large social media following doesn't happen over night, so relax and execute the social media strategy. The better an organization is at providing good information and engaging its social media audience, the faster the following will grow.

Using Social Media for Crisis Communications

CRISIS MANAGEMENT

Using social media to communicate with stakeholders during a crisis has proven to be an especially effective due to its speed, reach and direct access. In recent crisis, social media has helped distribute command information to key audiences and media while also providing a means for dialogue among the affected and interested parties.

YOU CAN'T FORCE TRUST

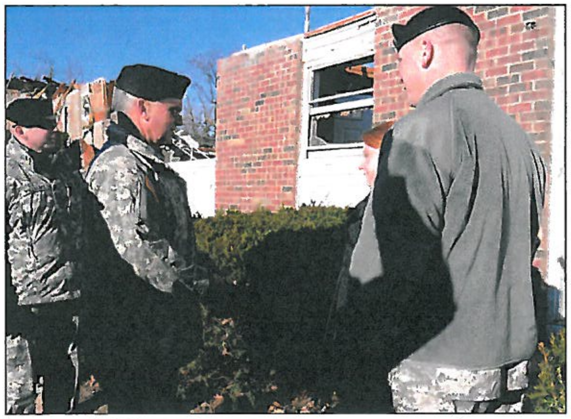
The best course of action is to leverage already existing social presences. It is important to have a regularly updated channel of communication open between the organization and the key audiences before the crisis hits so they not only know where to find you online, but know that they can trust the information they get.

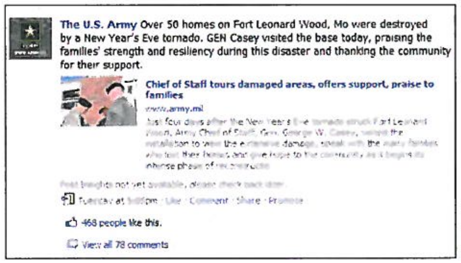
MONITOR CONTENT POSTED BY USERS

Monitor social media sites so the command understands what information the users need. Staff appropriately to answer questions as best as possible and ensure that your audience knows the organization is listening to them and are actively engaged in the crisis.

POST CLEARED INFORMATION AS IT COMES IN

When a crisis hits, there's no need to wait for a formal press release. When you have solid information that an organization's audiences want to know, post it. If the organization needs to put out updated information at a later time be sure to post it as well, but playing it too cautious and waiting for everything to play out will damage the organization's credibility





The U.S. Army Over 50 homes on Fort Leonard Wood, Mo were destroyed by a New Year's Eve tornado. GEN Casey visited the base today, praising the families' strength and resiliency during this disaster and thanking the community for their support.

Chief of Staff tours damaged areas, offers support, praise to families

www.army.mil

Just four days after the New Year's Eve tornado struck Fort Leonard Wood, Army Chief of Staff, Gen. George W. Casey, visited the installation to view the extensive damage, speak with the many families who lost their homes and give hope to the community as it begins its intense phase of reconstruction

Post Insights not yet available, please check back later.

Tuesday at [illegible] · Like · Comment · Share · Promote

468 people like this.

View all 78 comments

USE MOBILE DEVICES

Keep your social presences up to date by using mobile devices. The myriad of mobile devices available today allow you to update social sites without being tied to your computer at a desk. Crisis happen all the time, so be prepared. Whether the installation is on lock-down, you're waiting out a storm, or you're at a remote site at the scene, mobile devices allow you to share quick updates immediately. Make sure to ensure your mobile devices are continuously charged. Be creative in finding power solutions that work for your situation.

ANSWER QUESTIONS

Answer questions as often as possible. Avoid just posting information on a social media presence. Be prepared to receive questions. Respond back as quickly as possible through the most appropriate means of communication.

MONITOR CONVERSATIONS

Listen to what the audience is talking about and be prepared to engage. This is the best way to stop rumors before they run rampant. Use search engines and other monitoring tools to track discussion on the topic.

Using Social Media for Crisis Communications (Cont.)

SHARE INFORMATION

Share critical information with a network of trusted social media sites, such as other Army command sites, government and official non-governmental sites like the American Red Cross. The social media community is large and it's possible to reach a lot of people through an extended network in the social media space.

ENCOURAGE PEOPLE ON THE SCENE TO SEND INFO

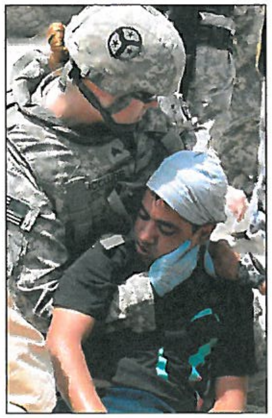
Organizations can do this by having individuals on the scene ether use their personal accounts or feed you information to post on the official command social sites. No matter how the information is submitted, the command site should promote this content when appropriate.

PROMOTE SOCIAL MEDIA PRESENCES

Make sure to advertise the organization's social media presences on outgoing press releases, e-mail signatures, links on the home page and in conversations with reporters. The social media presence isn't helpful if people don't know about it, so the organization should be aggressive when sending out information. Make sure the public knows that the organization's social media presences are a good resource for information.

ANALYZE RESULTS

Once the crisis is over, analyze what happened. Evaluate metrics and track user feedback. It's important to evaluate how a social media presence performs during a crisis so adjustments can be made for the future.



Checklists for Establishing an Official Social Media Presence

PRIOR TO ESTABLISHING AN OFFICIAL SOCIAL MEDIA PRESENCE, CONSIDER THESE ITEMS

□ **Study Army social media policy and read Army resources**

- Before you get started with social media, it's important to understand Army social media policy. Army social media resources can be found at: www.slideshare.net/usarmysocialmedia.

□ **Determine your goals**

- What do you want to achieve/communicate? It could include distributing command information, connecting to a community, building espirit de corps, etc.

□ **Determine your audience**

- Identify the audience you intend to communicate with. This can include Soldiers, Army Families, Veterans, civilians and the general public. Don't forget, your audience will also include stakeholders, politicians, community leaders and adversaries or enemies.

□ **Research and select social media platforms**

- Identify the social media platforms that will be suit the needs of your organization. Not all platforms will work for some organizations, so make sure you understand what can be achieved with each platform. Look at what other organizations are doing to get ideas.

□ **Select your name and branding**

- Read the Army's SOP for naming social media platforms. The SOP provides detailed naming and branding procedures. Check out this site for more: www.usarmybrandportal.com.

□ **Draft content strategy**

- After identifying your audiences, selecting the platforms and approving branding, begin drafting a posting strategy. This helps refine your organization's social media goals. For an example of a social media strategy, go to this website: http://slidesha.re/hlovpN

□ **Determine site management strategy**

- Identify social media managers on your team. Make sure contingency plans are in place to allow for other members to fill in on established duties if necessary.

□ **Develop policies and training**

- The social media team is responsible for developing organization-specific social media policies to include posting and commenting policies. Also make sure to develop training materials to help educate and train individuals in your command about social media and its uses. To view the Army's social media training resource, visit: www.slideshare.net/USArmySocialMedia.

Checklists for Establishing an Official Social Media Presence (Cont.)

REQUIREMENTS FOR AN OFFICIAL PUBLIC FACING COMMAND SOCIAL MEDIA PRESENCE (THIS MEANS A PUBLIC SITE, NOT ONE BEHIND A FIREWALL)

□ **Commanding officer or Public Affairs Officer approval**

- A presence must be approved by the release authority before it can be registered. Delegation of Authority-Approval of External Official Presences: http://slidesha.re/chQWAs

□ **The point of contact must include a valid .mil address when submitting for approval**

□ **The presence must have a URL to an official Army website**

- Your command's website or the Army.mil if your organization does not have a website

□ **The presence must post disclaimer text**

- The disclaimer identifies the page as an official Army social media presence and disclaims any endorsement. An example can be found here: http://on.fb.me/eulvUR.

□ **The presence must be clearly identified as "official"**

- Site must identify that the presence is "official" somewhere on the page. An example can be found in the left-hand column of the Army's Facebook page: www.facebook.com/USarmy.

□ **The presence must be unlocked and open to the public**

- This mostly applies to Twitter, but also means that "private" Facebook groups should not be registered on the Army's social media directory. All official presences are open to the public.

□ **Only official presences on Facebook can be registered and should be labeled as "Organization-Government"**

- The use of Facebook Profile, Community and Group pages for official purposes violates the government's terms of service agreement with Facebook.

□ **Submit the social media presence for approval and registration to www.army.mil/socialmedia/.**

□ **Set default view of your Facebook wall to show posts by only your organization.**

□ **Make sure YouTube channels are set up as a government presence. Step-by-step instructions can be found at this website:** https://forum.webcontent.gov/?page=TOS_YouTube

Army Branding

USING ARMY BRANDING

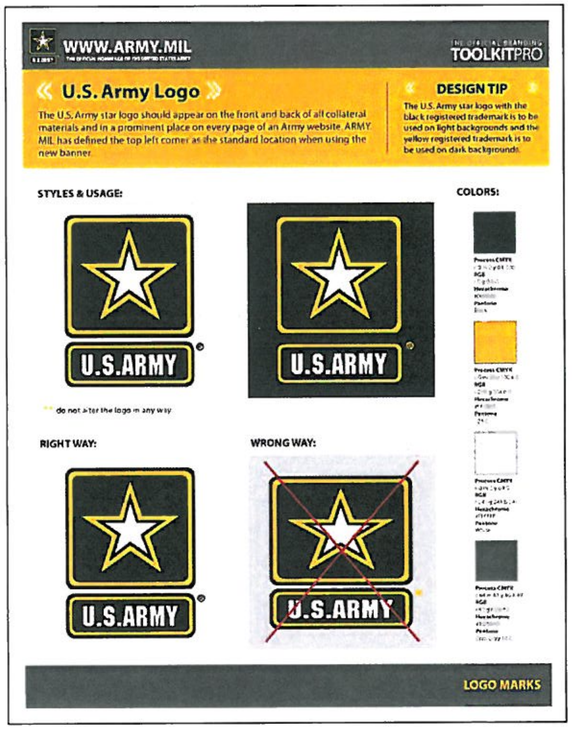
A Brand is not just a logo or an emblem. It's an organization's identity. So when using Army branding on social media sites, it's important to use the correct images. A brand represents the organization through distinctive visual elements, which uphold the integrity of the brand when used consistently and correctly across all communications.

STAYING ARMY STRONG

The U.S. Army Brand positioning conveys the heart and soul of the Brand in one statement. It's the core of the U.S. Army Brand and the underpinning of the U.S. Army's message of 'strength.' Army Strong is a unique brand of strength. Everyone is familiar with the tangible power of the U.S. Army: the Apaches, the Humvees, the weaponry, the push-ups. This campaign highlights the true strength of our Army — the strength that lies within each and every Soldier. It is harder to see, but it is this strength that makes the U.S. Army the preeminent land power on earth. So maintaining the same consistent branding across all Army sites (social media or otherwise) is vitally important.

BRANDING PORTAL

The U.S. Army Brand Portal (usarmybrandportal.com) provides Army brand elements such as Army logos, camouflage backgrounds, color palettes, typography, and released Army photography all in one place. The site also provides guidelines on how to use those elements together to ensure consistent Army branding. By visiting the site and getting the Army design elements and guidelines from the same place, people can ensure their use of Army branding is consistent with the Army's own designs.



WWW.ARMY.MIL

TOOLKITPRO

« U.S. Army Logo »

The U.S. Army star logo should appear on the front and back of all collateral materials and in a prominent place on every page of an Army website. ARMY.MIL has defined the top left corner as the standard location when using the new banner.

DESIGN TIP

The U.S. Army star logo with the black registered trademark is to be used on light backgrounds and the yellow registered trademark is to be used on dark backgrounds.

STYLES & USAGE:

** do not alter the logo in any way

RIGHT WAY:

WRONG WAY:

COLORS:

LOGO MARKS

U.S.ARMY

UNIT INSIGNIA EXAMPLES (HTTP://WWW.TIOH.HQDA.PENTAGON.MIL/)

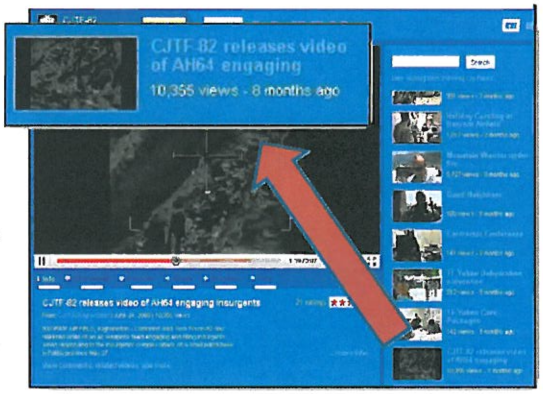
AIRBORNE
AA
1

Social Media Case Studies

Social media in an operational environment

SOCIAL MEDIA IN COMBAT

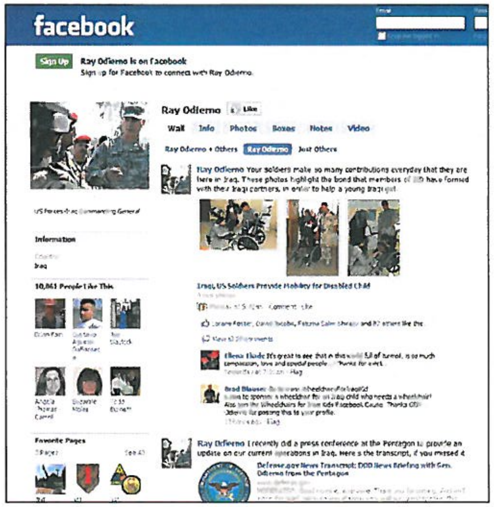
Operational units are finding opportunities for strategic online engagement on several platforms. Many deployed units maintain Facebook pages, Flickr sites and YouTube channels.


CJTF-82
CJTF-82 releases video of AH64 engaging
10,355 views - 8 months ago
Search

CJTF-82 releases video of AH64 engaging insurgents

CJTF-82

Combined Joint Task Force-82 in Afghanistan posted the video on the right to their YouTube channel of an air weapons team engaging and killing insurgents who were attacking a small patrol base in Paktia Province. While the Taliban claimed Americans had killed innocent civilians, this video allowed CJTF-82 to accurately portray the actual event to the media and the world.



Ray Odierno is on Facebook
Sign up for Facebook to connect with Ray Odierno.

Ray Odierno

Ray Odierno + Others | Ray Odierno | Just Others

US Forces-Iraq Commanding General

Information

Iraq

10,861 People Like This

Favorite Pages

Ray Odierno Your soldiers make so many contributions everyday that they are here in Iraq. These photos highlight the bond that members of have formed with their Iraqi partners, in order to help a young Iraqi girl.

Iraq, US Soldiers Provide Mobility for Disabled Child

Ellena Hude It's great to see that in this world full of turmoil, is so much compassion, love and special people... Thanks for everything.

Brad Blauser Wheelchairs for Iraqi Kids
to sponsor a wheelchair for an Iraqi child who needs a wheelchair! Also join the Wheelchairs for Iraqi Kids Facebook Cause. Thanks Odierno for posting this to your profile.

Ray Odierno I recently did a press conference at the Pentagon to provide an update on our current operations in Iraq. Here's the transcript, if you missed it.

Defense.gov News Transcript: DOD News Briefing with Gen. Odierno from the Pentagon

GEN. ODIERNO

When it comes to using social media to compliment his outreach strategy, General Odierno has been an ambitious and enthusiastic leader. An early advocate, General Odierno maintains a Facebook page that is both vibrant and informative. During his multiple tours in Iraq, Facebook was a ready source of information and an opportunity for discussion for his Facebook followers and other interested readers. His page also provided updates from theater, keeping family members connected during deployments. Now that he is at Joint Forces Command, he continues to use his Facebook page.

CONNECTING FROM BATTLE

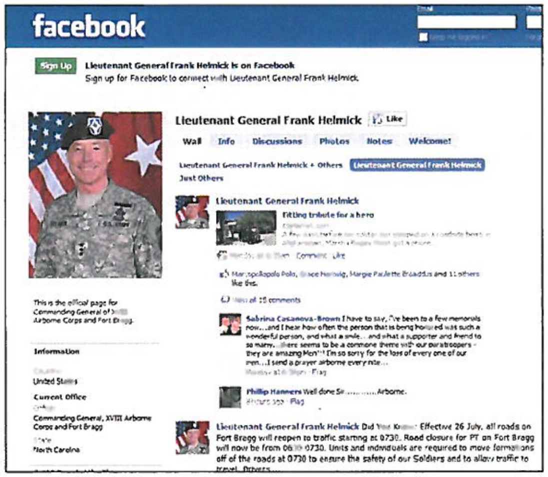
More and more commanders are seeing the value in using social media in combat. Social media can keep the public informed, it can keep Families connected and it can help address negative news stories and inaccurate reports.

Social Media Case Studies (Cont.)

Social media in a garrison environment

LT. GEN. HELMICK

Lt. Gen. Helmick at Fort Bragg has embraced social media, and his Facebook page is a good example of how to best use social media in a garrison environment. Lt. Gen. Helmick's Facebook page opens directly to his welcome page where he defines the purpose of the page and invites visitors to participate with him in discussions about Fort Bragg. His wall is populated with installation information and notifications about events and activities of interest to visitors to his page. The information is often supported with pictures and topic-specific video. Lt. Gen. Helmick often uses Facebook to solicit information from his visitors to help make Fort Bragg a better run installation. He asks for input on everything from the dining facility to traffic, and then he acts on those suggestions.



Lieutenant General Frank Helmick is on Facebook
Sign up for Facebook to connect with Lieutenant General Frank Helmick.

Lieutenant General Frank Helmick

Lieutenant General Frank Helmick + Others | Lieutenant General Frank Helmick | Just Others

This is the official page for Commanding General of XVIII Airborne Corps and Fort Bragg.

Information

United States

Current Office

Commanding General, XVIII Airborne Corps and Fort Bragg

North Carolina

Lieutenant General Frank Helmick
Fitting tribute for a hero

Marispolopolo Polo, Grace Hartwig, Margie Paulette Broaddus and 11 others like this.

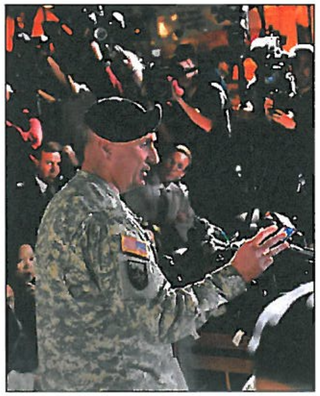
View all 15 comments

Sabrina Casanova-Brown I have to say, I've been to a few memorials now....and I hear how often the person that is being honored was such a wonderful person, and what a smile....and what a supporter and friend to so many... there seems to be a common theme with our paratroopers - they are amazing Men!!! I'm so sorry for the loss of every one of our men...I send a prayer airborne every nite....

Phillip Hanners Well done Sir.............Airborne.

Lieutenant General Frank Helmick Did You Know: Effective 26 July, all roads on Fort Bragg will reopen to traffic starting at 0730. Road closure for PT on Fort Bragg will now be from 0630-0730. Units and individuals are required to move formations off of the roads at 0730 to ensure the safety of our Soldiers and to allow traffic to travel. Drivers...

Social media in garrison crisis management



FORT HOOD SHOOTINGS

The 2009 crisis at Fort Hood illustrates the capability and capacity of social media to deliver news and information. After the shootings, people immediately went to the internet for information. People quickly turned to social media for information. Before the shootings, conversation surrounding Fort Hood was negligible, but on that day, mentions of Fort Hood skyrocketed on social media platforms like Twitter and Facebook. Even the media was aware that much of the most up-to-date information about the events at Fort Hood, which was sometimes speculation, was being conveyed by social media.

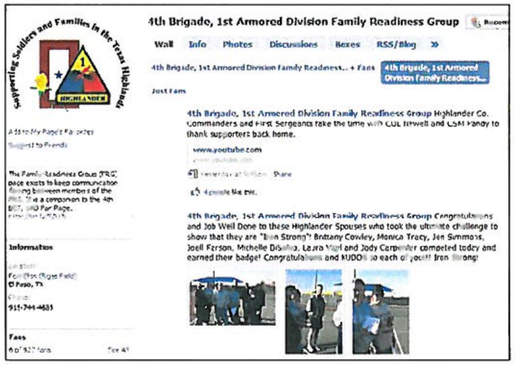
During those immediate hours of the shootings, traditional press conferences were used not so much to inform the media about what was going on, but rather to clarify what was being communicated on other forums, mostly social media forums that were quickly blasting unconfirmed information. On that day, Fort Hood found itself in a crisis that was both sudden and overwhelming. Any garrison might face a similar situation at any moment. More and more garrison commanders are understanding the need for a dynamic social media program for crisis communication as well as for a variety of everyday uses.

Social Media Case Studies (Cont.)

Social media and Family readiness

SOCIAL MEDIA AND FAMILIES

Social media is becoming an increasingly important tool for keeping Families and Soldiers connected with each other. The images on the right are screenshots of the Family Readiness Group Facebook page for the 4th Brigade, 1st Armored Division. This particular FRG page is full of information. It has announcements to keep Families up to date on activities of interest to them. Followers of the page are also very active. They often post additional information to the posted announcements. The interaction on this page, much like other FRG pages is dynamic, interesting and most of all informative. FRG Facebook pages have become the alternative to running from physical location to physical location trying to find out what's going on at an installation. FRG Facebook pages also include discussion sections where posts by the FRG and other individuals further advise each other about activities and information. The FRG, Soldiers and Families can also post photos to the pages. Ultimately, Social media is helping to keep families connected and that is vitally important to unit well being.



4th Brigade, 1st Armored Division Family Readiness Group

4th Brigade, 1st Armored Division Family Readiness... + Fans | 4th Brigade, 1st Armored Division Family Readiness...

Just Fans

Add to My Page's Favorites

Suggest to Friends

The Family Readiness Group (FRG) page exists to keep communication flowing between members of the FRG. It's a companion to the 4th BCT, 1AD Fan Page.

Information

Location:
Fort Bliss (Biggs Field)
El Paso, TX

Phone:
915-744-4635

Fans
6 of 927 fans See All

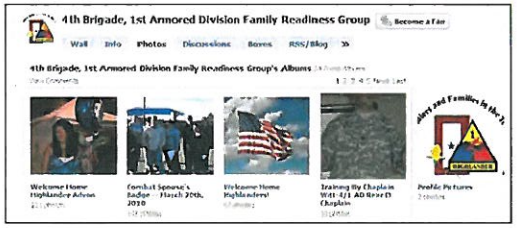
4th Brigade, 1st Armored Division Family Readiness Group Highlander Co. Commanders and First Sergeants take the time with COL Newell and CSM Pandy to thank supporters back home.

www.youtube.com

Yesterday at [illegible] · Share

4 people like this.

4th Brigade, 1st Armored Division Family Readiness Group Congratulations and Job Well Done to these Highlander Spouses who took the ultimate challenge to show that they are "Iron Strong"! Brittany Cowley, Monica Tracy, Jen Simmons, Joell Ferson, Michelle DiSalvo, Laura Vigil and Jody Carpenter competed today and earned their badge! Congratulations and KUDOS to each of you!! Iron Strong!



4th Brigade, 1st Armored Division Family Readiness Group

4th Brigade, 1st Armored Division Family Readiness Group's Albums

View Comments

1 2 3 4 5 Next Last

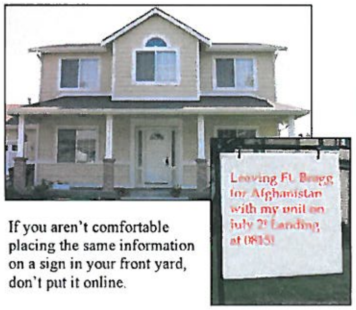
Welcome Home Highlander Advon

Combat Spouse's Badge -- March 20th, 2010

Welcome Home Highlanders!

Training By Chaplain With 4/1 AD Rear D Chaplain

Profile Pictures



Leaving Ft. Bragg for Afghanistan with my unit on July 2! Landing at 0815!

If you aren't comfortable placing the same information on a sign in your front yard, don't put it online.

WHAT CAN FAMILIES POST?

- Pride and support for service, units, specialties, and service member
- Generalizations about service or duty
- General status of the location of a unit ("operating in southern Afghanistan" as opposed to "operating in the village of Hajano Kali in Arghandab district in southern Afghanistan")
- Links to published articles about the unit or servicemember
- Any other information already in the public domain

Social Media Case Studies (Cont.)

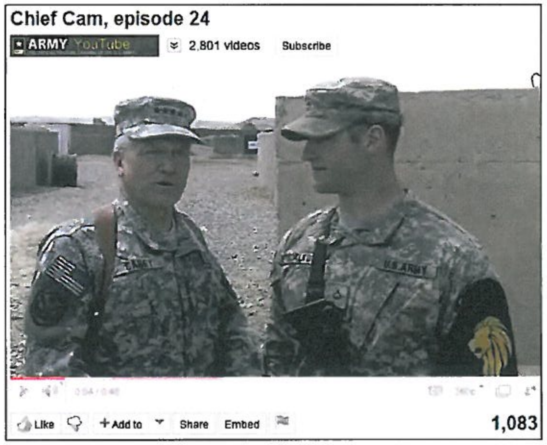
Army leaders and social media use

LEADERS IN ACTION

The previous case studies illustrate how leaders around the Army have used social media in garrison and operational environments, but social media use goes much deeper than that. Social media is about the daily interactions and some of the highest ranking leaders have tapped into social media platforms to communicate with the population at large.

CHIEF CAM

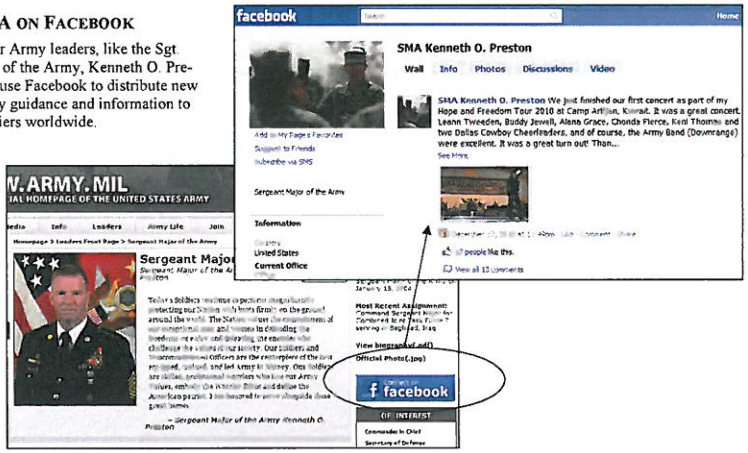
Army Chief of Staff, Gen. George W. Casey Jr. uses video to connect with the public. During his travels, Gen. Casey carries a flipcam and records interviews with Soldiers stationed around the world. He then posts these videos to YouTube.



Chief Cam, episode 24

SMA ON FACEBOOK

Other Army leaders, like the Sgt. Maj. of the Army, Kenneth O. Preston use Facebook to distribute new Army guidance and information to Soldiers worldwide.



SMA Kenneth O. Preston

SMA Kenneth O. Preston We just finished our first concert as part of my Hope and Freedom Tour 2010 at Camp Arifjan, Kuwait. It was a great concert. Leann Tweeden, Buddy Jewell, Alana Grace, Chonda Pierce, Kent Thomas and two Dallas Cowboy Cheerleaders, and of course, the Army Band (Downrange) were excellent. It was a great turn out! Than...

See More

17 people like this.

View all 13 comments

Add to My Page's Favorites

Suggest to Friends

Subscribe via SMS

Sergeant Major of the Army

Information

Country:
United States

Current Office

Homepage > Leaders Front Page > Sergeant Major of the Army

Sergeant Major

Today's Soldiers continue to perform magnificently protecting our Nation with boots firmly on the ground around the world. The Nation values the commitment of our exceptional men and women in defending the freedoms we enjoy and defeating the enemies who challenge the values of our society. Our Soldiers and Noncommissioned Officers are the centerpiece of the best equipped, trained, and led Army in history. Our Soldiers are skilled, professional warriors who live our Army Values, embody the Warrior Ethos and define the American patriot. I am honored to serve alongside these great heroes.

– Sergeant Major of the Army Kenneth O. Preston

January 15, 2004

Most Recent Assignment: Command Sergeant Major for Combined Joint Task Force 7 serving in Baghdad, Iraq

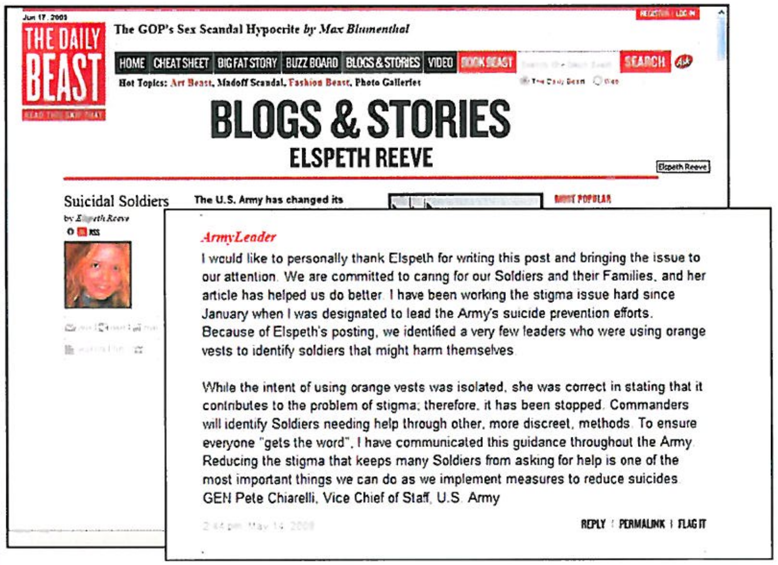
View biography(.pdf)

Official Photo(.jpg)

Social Media Case Studies (Cont.)

CONNECTING WITH THE PUBLIC

Maintaining a social media presence is not limited to simply engaging on your own platforms. Some Army leaders have taken it a step further. In the example below, when it came to the attention of Vice Chief of Staff of the Army Gen. Peter Chiarelli that a popular blog was reporting that Soldiers were wearing orange vests to identify them as suicidal, he was compelled to comment on the blog. By personally commenting on the blog, Gen. Chiarelli changed the narrative.



Jun 17, 2009
THE DAILY BEAST
The GOP's Sex Scandal Hypocrite by Max Blumenthal
HOME CHEATSHEET BIG FAT STORY BUZZ BOARD BLOGS & STORIES VIDEO BOOK BEAST SEARCH
Hot Topics: Art Beast, Madoff Scandal, Fashion Beast, Photo Galleries
BLOGS & STORIES
ELSPETH REEVE
Suicidal Soldiers
The U.S. Army has changed its
MOST POPULAR

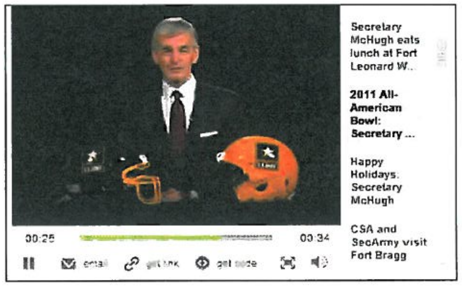
ArmyLeader

I would like to personally thank Elspeth for writing this post and bringing the issue to our attention. We are committed to caring for our Soldiers and their Families, and her article has helped us do better. I have been working the stigma issue hard since January when I was designated to lead the Army's suicide prevention efforts. Because of Elspeth's posting, we identified a very few leaders who were using orange vests to identify soldiers that might harm themselves.

While the intent of using orange vests was isolated, she was correct in stating that it contributes to the problem of stigma; therefore, it has been stopped. Commanders will identify Soldiers needing help through other, more discreet, methods. To ensure everyone "gets the word", I have communicated this guidance throughout the Army. Reducing the stigma that keeps many Soldiers from asking for help is one of the most important things we can do as we implement measures to reduce suicides.
GEN Pete Chiarelli, Vice Chief of Staff, U.S. Army

REACHING OUT

Leaders across the Army understand that social media in a new way to connect with various Army audiences. By reaching out through video, Facebook and blogs, Army leaders are engaging a new population of individuals who scour social media platforms for news rather than traditional media outlets. Social media helps bring the news to the user rather than forcing Army leaders to wait for the user to come to them.



00:25
00:34
email
get link
get code
Secretary McHugh eats lunch at Fort Leonard W...
2011 All-American Bowl: Secretary ...
Happy Holidays, Secretary McHugh
CSA and SecArmy visit Fort Bragg

Social Media Resources

The Department of Defense and the Army have dozens of social media resources available for social media managers, Soldiers and their Families.

POLICY RESOURCES

□ **DTM 09-026: Responsible and Effective Use of Internet-based Capabilities**
(http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf)

□ **AKO Social Media Portal**
(http://www.army.mil/suite/page/505262)

□ **Delegation of Authority—Approval of External Official Presences**
(http://www.slideshare.net/USArmySocialMedia/delegation-of-authority-social-media-use)

□ **Standardizing Official U.S. Army External Official Presences**
(http://www.slideshare.net/USArmySocialMedia/army-social-media-standard-operating-procedure-standardization)

OTHER SOCIAL MEDIA RESOURCES

□ **Army Social Media on Slideshare**
(http://www.slideshare.net/usarmysocialmedia)

□ **Army Social Media Directory**
(http://www.army.mil/socialmedia/)

□ **DoD Social Media Hub**
(http://socialmedia.defense.gov/)

□ **STRATCOM Social Networking training**
(http://www.stratcom.mil/snstraining/)

U.S. ARMY SLIDESHARE
THE OFFICIAL SLIDESHARE OF THE U.S. ARMY
U.S. Army
Search content from U.S. Army
Latest blog posts
Presentations (20)
DoD SOCIAL MEDIA HUB
Welcome to the Social Media Hub

Enclosure (1)

Department of the Army Standard Operating Procedure on standardizing official U.S. Army external official presences (social media)

DEPARTMENT OF THE ARMY
OFFICE OF THE CHIEF OF PUBLIC AFFAIRS
ONLINE AND SOCIAL MEDIA DIVISION
1500 ARMY PENTAGON
WASHINGTON DC 20301-1500

01 November 2010

SUBJECT: Standardizing official U.S. Army external official presences (social media)

1. References:
   a. Secretary of the Army Memorandum – Delegation of Authority – Approval of External Official Presences, 21 Oct. 2010
   b. Directive Type Memorandum DTM 09-026, Responsible and Effective Use of Internet Based Capabilities, 25 February 2010
   c. CIO/G6 Memorandum, Responsible Use of Internet Based Capabilities, 2010

2. The purpose of this memorandum is to standardize Army-wide External Official Presences (EOPs) (aka social media sites).

3. IAW Delegation of Authority memorandum (referenced above) commands are authorized to establish EOPs.

4. U.S. Army Family Readiness Groups may establish an official presence with the approval of their command. It is possible the unit's official page also serves the dual purpose as a platform for its Family Readiness Group to disseminate information, however, if the command elects to have separate pages they must adhere to the same standards.

5. All U.S. Army EOPs, to include pages on Facebook, Twitter, Flickr, YouTube, blogs and any other platform must adhere to the following standards:

   a. must be categorized as a government page
   b. include the Commander approved names and logos (i.e. 1st Brigade, 25th Infantry Division [Family Readiness]), not nickname nor mascot (i.e. not the "dragons")
   c. branding (official name and logos) across all social media platforms (i.e. Facebook, Twitter) are uniform
   d. include a statement acknowledging this is the "official [Facebook] page of [enter your unit or organizations name here] [Family Readiness]"
   e. Facebook pages must default to the "Just [your unit or organization's]" on the wall (Do this by selecting "edit page," then "manage permissions." Drop down under the "wall tabs page" and select "only post by page"). This results in command information being the first and primary thing on the wall, instead of spam and others comments.
   f. Facebook pages must include "Posting Guidelines" under the "Info Tab." Use the U.S. Army's Facebook policy as a reference and/or visit the DoD Social Media user agreement at: http://www.ourmilitary.mil/user_agreement.shtml
   g. be recent and up-to-date. Post must not be older than one month.
   h. adhere to Operations Security guidelines. FRSAs/FRG leaders should provide all page administrators and 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 slideshare site at www.slideshare.net/usarmysocialmedia.

Enclosure (1) Cont.

SUBJECT: Standardizing official U.S. Army external official presences (social media)
01 November 2010

   i. should not be used as a place for personal advertisement nor endorsement
   j. All pages must be registered through the U.S. Army at www.army.mil/socialmedia

6. 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.

7. For step-by-step instructions on how to set up pages, visit: http://socialmedia.defense.gov/learning-and-resources/training/social-media-guides/how-to-guides/ Further information, instruction, techniques, etc. can be found at www.slideshare.net/usarmysocialmedia

8. In order to sign up to receive weekly lessons, TTPs, etc. on how to manage social media pages, send an email to the email address below.

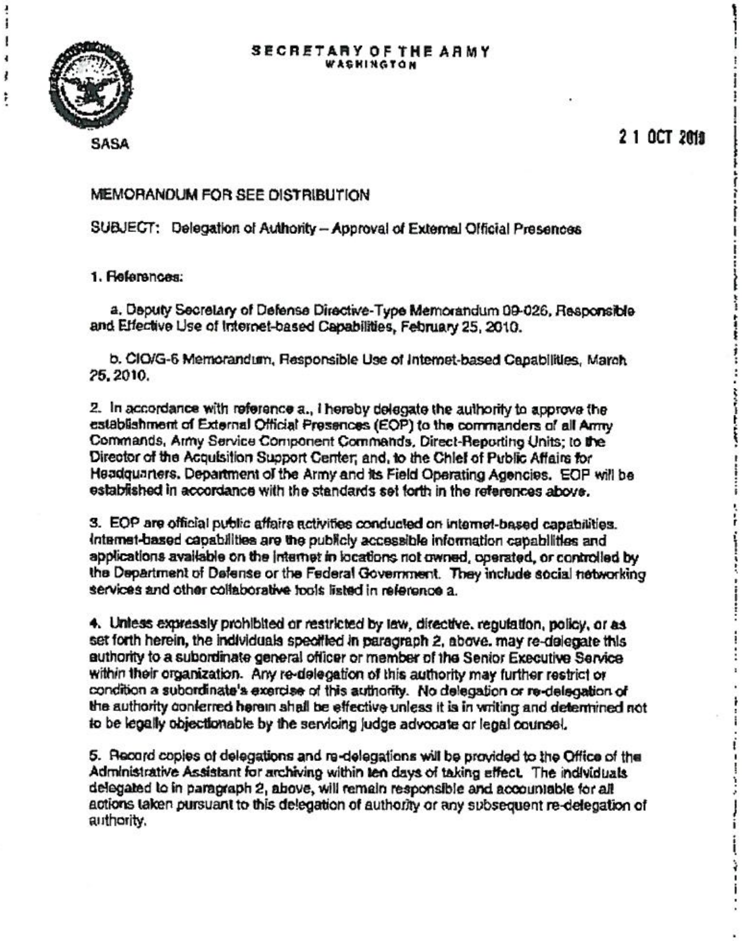
9. Use the platforms' help option to resolve questions, such as: http://www.facebook.com/help/ If questions are not resolved there, direct all questions and concerns to ocpa.osmd@us.army.mil.

10. POC for this memorandum can be reached at ocpa.osmd@us.army.mil

//original signed//
JUANITA A. CHANG
MAJ, CM
Director, Online and Social Media Division,
Office of the Chief of Public Affairs

Enclosure (2)

DEPARTMENT OF THE ARMY STANDARD OPERATING PROCEDURE ON STANDARDIZING OFFICIAL U.S. ARMY EXTERNAL OFFICIAL PRESENCES (SOCIAL MEDIA)



SECRETARY OF THE ARMY
WASHINGTON

SASA

21 OCT 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Delegation of Authority – Approval of External Official Presences

1. References:

a. Deputy Secretary of Defense Directive-Type Memorandum 09-026, Responsible and Effective Use of Internet-based Capabilities, February 25, 2010.

b. CIO/G-6 Memorandum, Responsible Use of Internet-based Capabilities, March 25, 2010.

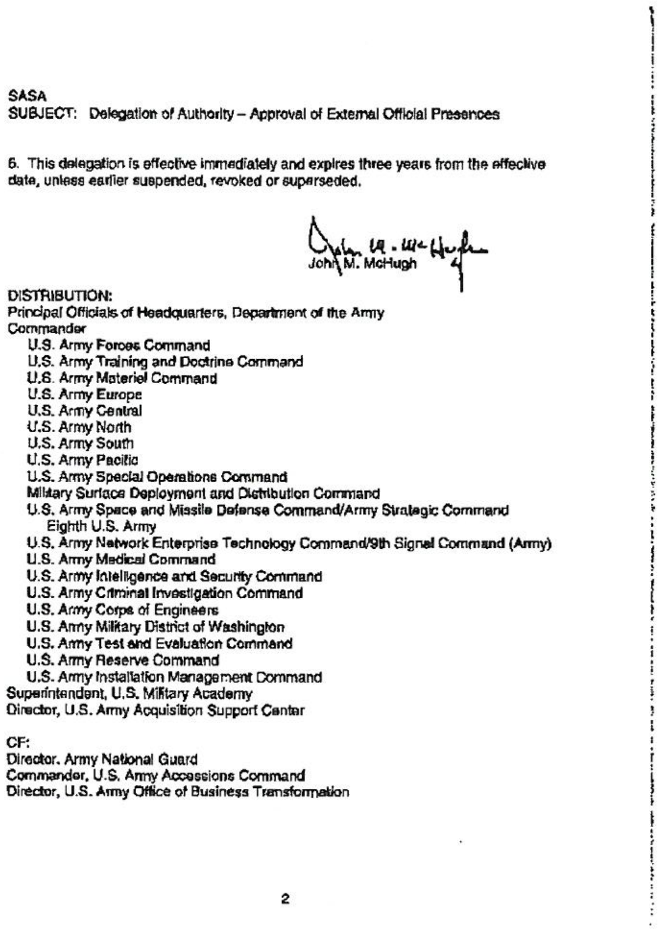
2. In accordance with reference a., I hereby delegate the authority to approve the establishment of External Official Presences (EOP) to the commanders of all Army Commands, Army Service Component Commands, Direct-Reporting Units; to the Director of the Acquisition Support Center; and, to the Chief of Public Affairs for Headquarters, Department of the Army and its Field Operating Agencies. EOP will be established in accordance with the standards set forth in the references above.

3. EOP are official public affairs activities conducted on internet-based capabilities. Internet-based capabilities are the publicly accessible information capabilities and applications available on the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. They include social networking services and other collaborative tools listed in reference a.

4. Unless expressly prohibited or restricted by law, directive, regulation, policy, or as set forth herein, the individuals specified in paragraph 2, above, may re-delegate this authority to a subordinate general officer or member of the Senior Executive Service within their organization. Any re-delegation of this authority may further restrict or condition a subordinate's exercise of this authority. No delegation or re-delegation of the authority conferred herein shall be effective unless it is in writing and determined not to be legally objectionable by the servicing judge advocate or legal counsel.

5. Record copies of delegations and re-delegations will be provided to the Office of the Administrative Assistant for archiving within ten days of taking effect. The individuals delegated to in paragraph 2, above, will remain responsible and accountable for all actions taken pursuant to this delegation of authority or any subsequent re-delegation of authority.

Enclosure (2) Cont.



SASA
SUBJECT: Delegation of Authority – Approval of External Official Presences

6. This delegation is effective immediately and expires three years from the effective date, unless earlier suspended, revoked or superseded.

John M. McHugh
John M. McHugh

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Europe
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Pacific
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
Eighth U.S. Army
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Reserve Command
U.S. Army Installation Management Command
Superintendent, U.S. Military Academy
Director, U.S. Army Acquisition Support Center

CF:
Director, Army National Guard
Commander, U.S. Army Accessions Command
Director, U.S. Army Office of Business Transformation

Enclosure (3)

DIRECTIVE-TYPE MEMORANDUM (DTM) 09-026—RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1010

February 25, 2010
Change 1, September 16, 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities

References: See Attachment 1

Purpose. This memorandum establishes DoD policy and assigns responsibilities for responsible and effective use of Internet-based capabilities, including social networking services (SNS). This policy recognizes that Internet-based capabilities are integral to operations across the Department of Defense. This DTM is effective immediately; it will be converted to a new DoD issuance ~~within 180 days~~. *This DTM shall expire effective March 1, 2011.*

Applicability. This DTM applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").
- All authorized users of the Non-Classified Internet Protocol Router Network (NIPRNET).

Definitions. Unless otherwise stated, these terms and their definitions are for the purpose of this DTM.

- Internet-based capabilities. All publicly accessible information capabilities and applications available across the Internet in locations not owned, operated, or controlled by the Department of Defense or the Federal Government. Internet-based capabilities include collaborative tools such as SNS, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps).
- external official presences. Official public affairs activities conducted on non-DoD sites on the Internet (e.g., Combatant Commands on Facebook, Chairman of the Joint Chiefs of Staff on Twitter).

Enclosure (3) Cont.

- official public affairs activities. Defined in DoD Instruction (DoDI) 5400.13 (Reference (a)).

Policy. It is DoD policy that:

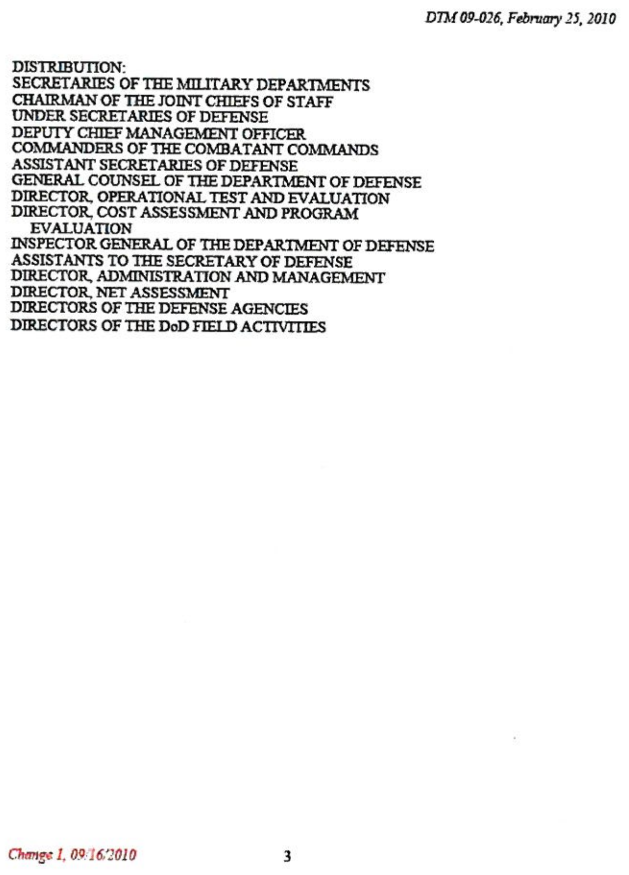
- The NIPRNET shall be configured to provide access to Internet-based capabilities across all DoD Components.
- Commanders at all levels and Heads of DoD Components shall continue to defend against malicious activity affecting DoD networks (e.g., distributed denial of service attacks, intrusions) and take immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve operations security or to address bandwidth constraints).
- Commanders at all levels and Heads of DoD Components shall continue to deny access to sites with prohibited content and to prohibit users from engaging in prohibited activity via social media sites (e.g., pornography, gambling, hate-crime related activities).
- All use of Internet-based capabilities shall comply with paragraph 2-301of Chapter 2 of the Joint Ethics Regulation (Reference (b)) and the guidelines set forth in Attachment 2.

Responsibilities. See Attachment 3.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

Attachments:
As stated

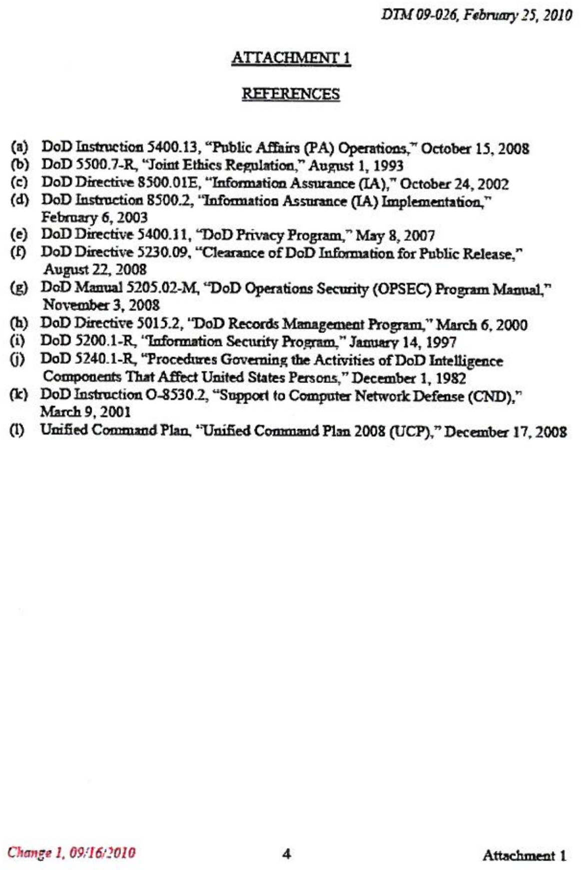
Enclosure (3) Cont.



DTM 09-026, February 25, 2010

DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM
  EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

Enclosure (3) Cont.



DTM 09-026, February 25, 2010

ATTACHMENT 1

REFERENCES

(a) DoD Instruction 5400.13, "Public Affairs (PA) Operations," October 15, 2008
(b) DoD 5500.7-R, "Joint Ethics Regulation," August 1, 1993
(c) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(d) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(e) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
(f) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(g) DoD Manual 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008
(h) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(i) DoD 5200.1-R, "Information Security Program," January 14, 1997
(j) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982
(k) DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001
(l) Unified Command Plan, "Unified Command Plan 2008 (UCP)," December 17, 2008

Enclosure (3) Cont.

ATTACHMENT 2

GUIDELINES FOR USE OF INTERNET-BASED CAPABILITIES

1. GENERAL. This attachment applies to the official and/or authorized use of Internet-based capabilities by DoD personnel and all authorized users of the NIPRNET. Examples include, but are not limited to:

a. SNS.

b. Image- and video-hosting web services.

c. Wikis.

d. Personal, corporate, or subject-specific blogs.

e. Data mashups that combine similar types of media and information from multiple sources into a single representation.

f. Similar collaborative, information sharing-driven Internet-based capabilities where users are encouraged to add and/or generate content.

2. OFFICIAL PRESENCES. External official presences shall comply with Reference (a) and clearly identify that the Department of Defense provides their content. In addition, external official presences shall:

a. Receive approval from the responsible OSD or DoD Component Head. Approval signifies that the Component Head concurs with the planned use and has assessed risks to be at an acceptable level for using Internet-based capabilities.

b. Be registered on the external official presences list, maintained by the Assistant Secretary of Defense for Public Affairs (ASD(PA)), on www.Defense.gov.

c. Comply with References (a) and (b) as well as DoD Directive (DoDD) 8500.01E, DoDI 8500.2, DoDD 5400.11, DoDD 5230.09, DoD Manual 5205.02-M, DoDD 5015.2, DoD 5200.1-R, and DoD 5240.1-R (References (c) through (j), respectively).

d. Use official DoD and command seals and logos as well as other official command identifying material per ASD(PA) guidance.

Enclosure (3) Cont.

e. Clearly indicate the role and scope of the external official presence.

f. Provide links to the organization's official public website.

g. Be actively monitored and evaluated by DoD Components for compliance with security requirements and for fraudulent or objectionable use (References (d), (g), and (i)).

3. OFFICIAL USE. 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. Use of Internet-based capabilities for official purposes shall:

a. Comply with References (b) through (j).

b. Ensure that the information posted is relevant and accurate, and provides no information not approved for public release, including personally identifiable information (PII) as defined in Reference (e).

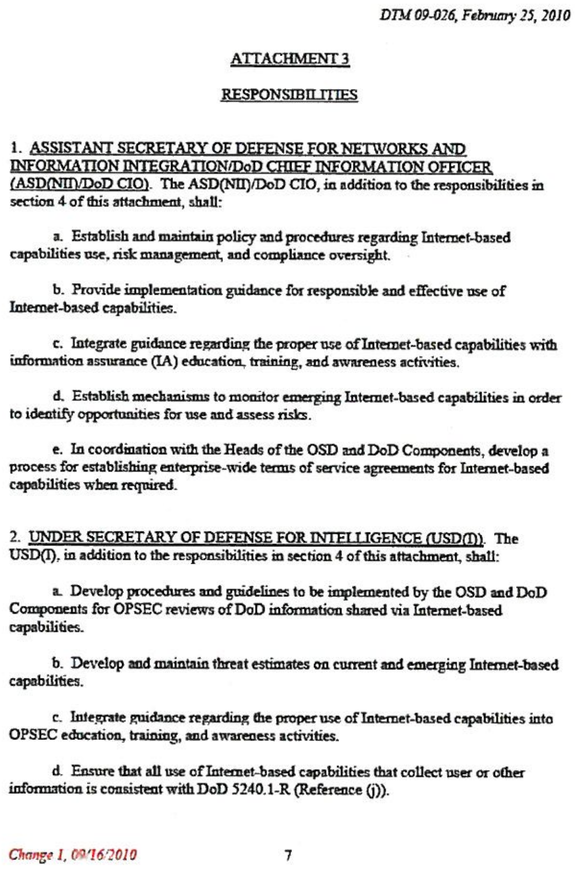
c. Provide links to official DoD content hosted on DoD-owned, -operated, or -controlled sites where applicable.

d. 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").

4. RECORDS MANAGEMENT. Internet-based capabilities used to transact business are subject to records management policy in accordance with Reference (h). All users of these Internet-based capabilities must be aware of the potential record value of their content, including content that may originate outside the agency.

5. LIMITED AUTHORIZED PERSONAL USE. Paragraph 2-301 of Reference (b) permits limited personal use of Federal Government resources when authorized by the agency designee on a non-interference basis. When accessing Internet-based capabilities using Federal Government resources in an authorized personal or unofficial capacity, individuals shall employ sound operations security (OPSEC) measures in accordance with Reference (g) and shall not represent the policies or official position of the Department of Defense.

Enclosure (3) Cont.



DTM 09-026, February 25, 2010

ATTACHMENT 3

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in section 4 of this attachment, shall:

a. Establish and maintain policy and procedures regarding Internet-based capabilities use, risk management, and compliance oversight.

b. Provide implementation guidance for responsible and effective use of Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities with information assurance (IA) education, training, and awareness activities.

d. Establish mechanisms to monitor emerging Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Heads of the OSD and DoD Components, develop a process for establishing enterprise-wide terms of service agreements for Internet-based capabilities when required.

2. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), in addition to the responsibilities in section 4 of this attachment, shall:

a. Develop procedures and guidelines to be implemented by the OSD and DoD Components for OPSEC reviews of DoD information shared via Internet-based capabilities.

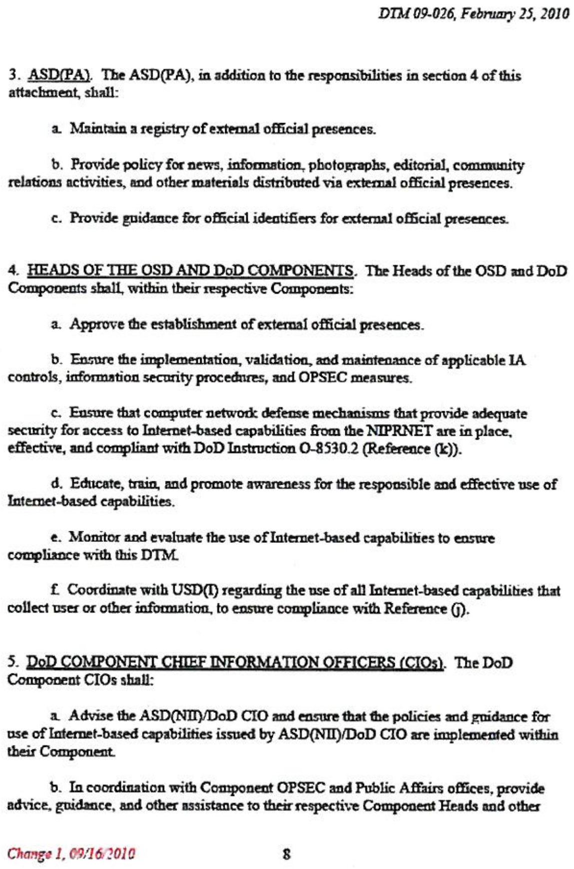
b. Develop and maintain threat estimates on current and emerging Internet-based capabilities.

c. Integrate guidance regarding the proper use of Internet-based capabilities into OPSEC education, training, and awareness activities.

d. Ensure that all use of Internet-based capabilities that collect user or other information is consistent with DoD 5240.1-R (Reference (j)).

Change 1, 09/16/2010 7

Enclosure (3) Cont.



DTM 09-026, February 25, 2010

3. ASD(PA). The ASD(PA), in addition to the responsibilities in section 4 of this attachment, shall:

a. Maintain a registry of external official presences.

b. Provide policy for news, information, photographs, editorial, community relations activities, and other materials distributed via external official presences.

c. Provide guidance for official identifiers for external official presences.

4. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall, within their respective Components:

a. Approve the establishment of external official presences.

b. Ensure the implementation, validation, and maintenance of applicable IA controls, information security procedures, and OPSEC measures.

c. Ensure that computer network defense mechanisms that provide adequate security for access to Internet-based capabilities from the NIPRNET are in place, effective, and compliant with DoD Instruction O-8530.2 (Reference (k)).

d. Educate, train, and promote awareness for the responsible and effective use of Internet-based capabilities.

e. Monitor and evaluate the use of Internet-based capabilities to ensure compliance with this DTM.

f. Coordinate with USD(I) regarding the use of all Internet-based capabilities that collect user or other information, to ensure compliance with Reference (j).

5. DoD COMPONENT CHIEF INFORMATION OFFICERS (CIOs). The DoD Component CIOs shall:

a. Advise the ASD(NII)/DoD CIO and ensure that the policies and guidance for use of Internet-based capabilities issued by ASD(NII)/DoD CIO are implemented within their Component.

b. In coordination with Component OPSEC and Public Affairs offices, provide advice, guidance, and other assistance to their respective Component Heads and other

Change 1, 09/16/2010 8

Enclosure (3) Cont.

Component senior management personnel to ensure that Internet-based capabilities are used responsibly and effectively.

c. Assist their respective Component Head to ensure effective implementation of computer network defense mechanisms as well as the proper use of Internet-based capabilities through the use of existing IA education, training, and awareness activities.

d. Establish risk assessment procedures to evaluate and monitor current and emerging Component Internet-based capabilities in order to identify opportunities for use and assess risks.

e. In coordination with the Component Public Affairs Office, assist their respective Component Head in evaluating external official presences' intended use.

6. COMMANDER, UNITED STATES STRATEGIC COMMAND (CDRUSSTRATCOM). The CDRUSSTRATCOM, in addition to the responsibilities in section 4 of this attachment, shall:

a. In accordance with Unified Command Plan 2008 (Reference (l)), direct the defense and operation of the DoD Global Information Grid (GIG).

b. Assess risks associated with the use of Internet-based capabilities, identify operational vulnerabilities, and work with the ASD(NII)/DoD CIO to mitigate risks to the GIG.

Frequently Asked Questions

Q: How do I get content on the Army's social media pages?

A: The Online and Social Media Division is always looking for content. You can email stories, photos or links to unit videos to ocpa.osmd@us.army.mil and we will work hard to feature them on our sites.

Q: What if my unit doesn't have money or enough people to manage a social media presence?

A: Facebook, Twitter, YouTube, Flickr and a variety of other social media platforms are free, so it is possible to have a social media team without a budget. Limited manpower does not limit your unit's ability to maintain a social media presence. Just keep it simple. Evaluate the platforms and determine which will work best for your manpower situation. It only takes one person to run a Facebook page and a Twitter account.

Q: Who can manage my unit's Facebook page

A: Currently, social media manager is not an Army military occupation specialty, so it is often viewed as an additional duty. Often times, 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 is motivated and the commander approves his/her managing the site, anyone can run a social media site as long as they work closely with the unit's public affairs shop in accordance with DTM 09-026

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: Can I delete comments on my unit's Facebook wall?

A: Every registered social media presence in the Army is required to have a posting policy in place. This posting policy should indicate what can and cannot be posted to a Facebook wall. If users violate these terms on your unit's wall, you are entitled to delete the comment and block the user if necessary. Keep in mind that Facebook is about facilitating the conversation so stick to your posting policy, but don't delete comments just because they express negative opinions about your organization.

Q: How can I increase the number of individuals who follow my unit on Facebook and Twitter

A: Be creative. There is no surefire way to increase followers on Facebook and Twitter, different techniques work for different organizations so it's important to think outside the box. Ask your followers to participate in the conversation, respond to them directly and ask them what they expect out of your social media presence. Look at what other organizations are doing. If they launch a successful campaign on Facebook, feel free to use their example and tailor it to your unit. Social media is still evolving so there is a lot of room to be creative. Don't be afraid to experiment and have fun.

Frequently Asked Questions (cont.)

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 them 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 breech and

Q: I've never been on Facebook (Twitter, YouTube, etc). How do I get started?

A: First, know that you're not alone. Fortunately most social media platforms are relatively easy to use. The best way to get started is to find someone you know who is savvy with social media to show you the ropes. You can also start your own personal social media accounts so that you can familiarize yourself with how they work. The Online and Social Media Division maintain Social Media resources for Facebook, Twitter, and Blogs that are available on Slideshare (http://www.slideshare.net/usarmysocialmedia) and is a good place to start. If you have any questions that you can't find answers to you can always call the Online and Social Media Division or your local public affairs officer.

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, 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/or 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. These official presences are listed in the U.S. Army Social Media Directory (lists only command presences, not family readiness groups) which can be found at: www.army.mil/media/socialmedia/ If you find an online presence that portrays itself as an official presence and the command is not sponsoring it, suggest that your command contact the administrator.

Q: I am turning over my duties as the social media manager. How should I transfer over our social media presence?

A: If you established your social media presences under a general command account, it will be very easy to simply turn over the login and passwords and teach the new social media manager how the platform works. If you have been using your personal account to relay information, you will need to introduce the new social media manager on the social platform to the audience. Make sure to give the new social media manager administrator privileges.

ONLINE AND SOCIAL MEDIA DIVISION
OFFICE OF THE CHIEF OF PUBLIC AFFAIRS
1500 Pentagon
Washington, D.C.
Ocpa.osmd@us.army.mil