



THE UNITED STATES ARMY SOCIAL MEDIA HANDBOOK





Letter from the Chief of Public Affairs

Thank you for the effort you put into telling the U.S. Army's and our Soldiers' stories every day. Each of you invests an extraordinary effort into researching, covering and publishing news and content for the American public and the global community, providing important coverage on topics that tell the U.S. Army's story.

Speed Matters —

You now operate in a faster paced newsroom than your predecessors did. You no longer have the luxury of a 24-hour window to research, report and air news due to social media and mobile devices enabling breaking news to appear in a matter of hours, even minutes after an event occurs.

Critical Response Time —

Traditional media outlets are leveraging the ability to seek out information and report real time. These outlets are looking for an immediate response to query (RTQ) and are pressured to publish as soon as possible. These factors mean you have to be ready to respond to any number of contingencies at any time.

More often than not, this means responding online and on social media platforms.

Conversations —

Communities are increasingly looking to you for information that directly impacts them, and looking for ways to interact with Soldiers. Social media gives you the ability to converse directly with your audiences at a level of personal interaction never before imagined, creating a meaningful dialogue with individuals and groups. You are increasingly able to build a strong community support structure based on social media engagement.

Best Practices and Tools —

You have to make the most of opportunities to expand your knowledge base and add to your social media toolkit. This handbook is only a primer to the basic operation of social media assets. In it you will find the basic requirements for setting up and maintaining various social media platforms.

Command Analysis —

Remember that social media is not a one-size-fits-all

effort. Your unit may need to focus on one platform or several platforms. It is your responsibility to provide your commander a balanced analysis to determine what is the end-state for a particular line of effort and what return on investment is expected.

Training/Innovation —

You have to make the most of the training that is available to you, both formal training at the Defense Information School, and informal training you seek out on your own. Social media evolves at such a fast pace that it is critical to take the initiative to seek out these opportunities, and when you find these opportunities, share them with your peers. The Online and Social Media Division maintains a list of free social media training and resource websites that we distribute via CPA Sends to help staff stay current on social media best practices and current trends.

I am proud of the work I see from public affairs professionals out in the field. However, we can and must continue to improve, grow and keep up with technology.

I encourage you to continue looking for opportunities to help tell the U.S. Army's story. Thank you again for everything you do.

MALCOLM B. FROST
Brigadier General, U.S. Army
Chief of Public Affairs

Table of Contents

Seven Basic Social Media Tips	2
Social Media Summary	3
Steps to Creating Effective Communication Platforms	4
Checklist for Establishing an Official Army Social Media Account	6
Official U.S. Army Social Media Account Requirements	7
Social Media Directory	8
Maintaining an Official Social Media Account	9
Using Social Media for Crisis Communications	11
Impersonations	13
Social Media Scams	16
Checklist for Operations Security for Official Army Pages	17
Operations Security	18
Social Media for Soldiers, Staff and Families	20
Social Media in Garrison, Training and while Deployed	22
U.S. Army Leaders on Social Media	23
Facebook Quick Reference Guide	24
Twitter Quick Reference Guide	30
Instagram	35
Enclosure	
Example Unit Policy	37

Page Resource Guide

All resources discussed on each page of the U.S. Army Social Media Handbook are hyperlinked in the text and listed at the bottom of each page in a page resource guide box.

Seven Basic Social Media Tips

Your online interactions are a reflection of the U.S. Army as well as your professionalism.

It is critical that Soldiers act responsibly and understand that [U.S. Army standards of conduct](#) apply to all aspects of their lives, 24 hours a day, seven days a week.

Here are seven tips to help guide you when using social media:

- Be aware of the image you present.**
Do not discredit yourself, your family, your organization or your Army by using inappropriate language or content. Only post or discuss issues related to your professional expertise or personal experience. Remember, your behavior online is reflective of your Army's image.
- Ensure information you post or share is releasable.**
It is imperative that you are aware of potential security violations when posting online. It is never acceptable to post classified, For Official Use Only (FOUO) or pre-decisional information on an official or personal account. It is your responsibility to be aware of the classification and releasability of the material you post.
- Live the U.S. Army values.**
Online misconduct is punishable under the Uniform Code of Military Justice (UCMJ). [ALARACT 122/2015, Professionalization of Online Conduct](#), reinforces AR 600-20 and defines cyber misconduct as "the use of electronic communication to inflict harm.; examples include, but are not limited to: libel, slander, harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermines dignity and respect."
- Do not use trademarked or copyright protected material.**
Posting or sharing music, logos, songs, or other information that is protected by copyright, trademark, or any other restriction is illegal. Restricted materials can only be shared with express permission from the owner.
- Do not misrepresent your identity.**
Misrepresentation of your identity by disguising yourself or impersonating others is prohibited and is punishable under the UCMJ.
- Be cautious with the personal information you share.**
Criminals and adversaries can easily piece together information you share, potentially harming you, your loved ones, fellow Soldiers, or our mission. Safeguard yourself and those close to you by not posting personal contact information or sharing plans and schedules. Turn off electronic functions such as GPS or geotagging and always optimize your security settings.
- If you feel threatened or feel that you or a member of your Family needs help.**
Ask for help if you or a Family member have fallen victim to a scam, impersonation, or feel threatened. Contact the local civil authorities or the [U.S. Army Criminal Investigation Command for assistance](#) and to report a scam, impersonation or threat.

Page Resource Guide

AR 600-20 Army Command Policy

ALARACT 122/2015 Professionalization of Online Conduct

U.S. Army Criminal Investigation Command: Report a Crime

www.apd.army.mil/pdf/files/r600_20.pdf

<https://www.milsuite.mil/book/docs/DOC-215026>

www.cid.army.mil/reportacrime.html

Social Media Summary

Why use social media?

Soldiers have always been the U.S. Army's best and most effective messengers. Social media allows Soldiers to tell their story in an authentic and intimate manner. By interacting with Soldiers, Family members, Department of the Army Civilians and the public on social media platforms, the U.S. Army enables communities to be built that increase confidence and create an environment where our audience goes for trusted information.

Social media enables the U.S. Army Family around the world to stay connected and tell the U.S. Army's story. Every time an organization or member of the U.S. Army Family joins social media, it increases the timely and transparent dissemination of information. It ensures that the U.S. 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 U.S. Army's story and it allows America to connect with its Army. The U.S. Army uses social media to tell the U.S. Army's story, but it also uses social media to listen.

"And the choice we face, I mean anybody who has a message they want to have heard anywhere in the world, isn't whether or not that is the media environment we want to operate in. That's the media environment we've got. The question we all face now is, 'How can we make best use of this media? Even though it means changing the way we've always done it.'"

Clay Shirky, Social Media Theorist

Messages posted to social media platforms have the potential to reach millions of users in an instant. These individuals have the ability to not only respond with direct feedback to the author of the message, but also to the followers/audience of the author and their own peers. In his [TED Talk](#), Shirky says that social media is

the biggest change in communications since the invention of the printing press. Not only can an idea be transmitted from the author to the audience, but it also spawns two-way communication among a network of individuals. Social media has empowered the world and enabled any person with an Internet connection or a smart phone to become part of the conversation and voice their opinion on a topic instantly.



A [Pew Research Center poll](#) conducted in 2015 found:

- Approximately **64 percent** of adults in the U.S. own a smart phone.
- More than **68 percent** of these use the devices to monitor breaking news.
- More than **67 percent** use their phone to share event pictures, videos, or commentary.

What regulations, policies, or guidelines cover an official social media account?

All official accounts must be operated within Department of Defense (DoD) and [U.S. Army guidelines](#). The following documents should be thoroughly reviewed to ensure accounts are maintained accordingly. Developing a unit policy based on these documents is a good step towards ensuring Public Affairs staff and Soldiers in the unit have a guideline to reference.

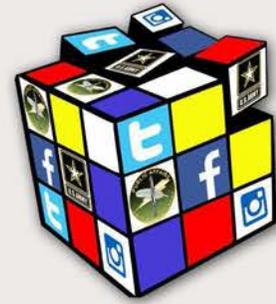
- [DoD Instruction 8550.01 – DoD Internet Services and Internet-based Capabilities](#).
- Secretary of the Army's Delegation of Authority Approval of External Official Presences

Page Resource Guide

Clay Shirky's TED Talk	www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history
Pew Research Poll	www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/
Regulations and policies	www.army.mil/e2/rv5_downloads/socialmedia/Registration_Checklist.pdf
DoDI 8550.01 Internet Services and Internet-based Capabilities	http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf

Steps to Creating Effective Communication Platforms

Social media is a powerful communications tool. When used correctly, social media can help an organization reach an enormous audience. Social media can help organizations engage in the conversation while at the same time promote awareness of the organization's main communication priorities. But not all U.S. Army organizations use social media effectively. Suboptimization of social media can be attributed to organizations rushing into social media before determining what the organization aims to achieve with social media platforms. Using social media effectively is a process, and it requires strategy, goals, manpower and foresight. The checklists on the following pages will help you as you develop your organization's social media account.



Step 1:

Determine if you need a social media account. What effects do you plan to achieve with your social media account? Who is the audience you are trying to reach and why? How do you represent your leaders? Do you need a personal, public figure, or organization page? Make sure you have a way forward, the manpower to effectively manage your social media account, and a set of goals.

Developing a social media outreach plan requires a lot of thought, so make sure you know how you plan to use social media as part of your overall communication plan.

Step 2:

Review all of the U.S. Army social media content available. This handbook is a great start, but there are many materials at your disposal.

The U.S. Army maintains a [SlideShare site](#) where there are dozens of Social Media Roundups. These are brief, 10-15 slide presentations that discuss various social media topics.

Be sure to also review the other documents on the site. This will help you understand the policies surrounding social media use.

Additional resources can be found at the top of the [U.S. Army Social Media Directory](#).

Step 3:

Once you have done your research and are ready to set up a social media account, be sure to do so in accordance with the DoD and U.S. Army guidance.

Step 4:

It is important to provide up-to-date unit contact information on your social

media platforms. Facebook pages and YouTube channels are required to provide a government email address and other official contact information as applicable for the unit. However, since some platforms like Twitter allow less space for this information, it is sufficient to provide just an email address.

Step 5:

Each social media account must have a terms of use statement that informs visitors of what is authorized when interacting on the platform. This terms of use statement should include a general disclaimer, privacy and security disclaimers, a copyright and trademark disclaimer, moderated account disclaimer and a Freedom of Information Act notice. For an example of a terms of use statement, review the [U.S. Army's terms of use statement](#) on the U.S. Army's official

Page Resource Guide

U.S. Army Slideshare

www.slideshare.net/usarmysocialmedia

U.S. Army Social Media Directory

www.army.mil/media/socialmedia/

U.S. Army's terms of use statement (Facebook)

www.facebook.com/USArmy/info/?tab=page_info

Facebook page and the [DoD Social Media user agreements](#).

Step 6:

Once the page is complete, register it with the U.S. Army. The registration process is quite simple. Ensure you meet the submission guidelines listed at the [U.S. Army Social Media Directory](#). Type in your information then click the “submit” button. Qualifying accounts will be registered and forwarded to the appropriate platform for verification as an official account.

Step 7:

The process is not over once you are up and running. Make sure you post relevant, quality content and keep your social media account active.

Step 8:

After you have done the basic research, set up your social media account and submitted it for registration you should work with your team to develop a social media strategy. This helps your organization, refine its focus. During this phase of the planning process, it’s also helpful to look at how other U.S. Army organizations are using social media. The [U.S. Army Social Media Directory](#) provides links to all of the U.S. Army’s registered social media sites. The [DoD also maintains an extensive registry](#) of military social media accounts. Both the DoD and U.S. Army sites enable account managers to research successful examples.

Check out these [Facebook](#), [Twitter](#) and [Instagram](#) tips on effective posting and effective audience engagement. For example:

- Be consistent in the quality and types of posts you create. Use high-quality photos or videos of Soldiers doing their jobs. Avoid grip and grin photographs.
- Ensure your photos, videos and text reflect U.S. Army Values, current published communication priorities and your organization’s intent.
- Use a content calendar, for example: Motivation Monday; Technology Tuesday; What is Happening Wednesday; Throwback Thursday; Feature Friday; Sneak Peek Saturday; and Soldier Sunday.
- If it has been a week since an event has occurred, it’s time to forecast the next event not post photos from the old event.
- It is ok to post the same message on different platforms. But vary the wording, photos and videos to make the posts feel different to your audience.
- Use social media as a way to have a conversation with your audience. Respond to comments on your posts to help guide the tone and direction of the conversations. It lets your audience know you’re listening.
- Remember to keep the bottom line up front. Post short and informative content. Make sure what you want your audience to know is easily identifiable.
- Every element of your profile — your photo, header and biography — should reflect your organization’s identity and personality.
- Create a unique personality that entertains yet educates your audience.
- Use platform analytics to review post performance, peak audience engagement periods and identify effective TTPs you can employ.

Page Resource Guide

[DoD Social Media user agreements](#)
[U.S. Army Social Media Directory](#)
[Department of Defense Social Media Registry](#)
[Facebook page posting tips and best practices](#)
[Twitter content strategy](#)
[Instagram Help Center](#)

www.defense.gov/socialmedia/user-agreement.aspx
www.army.mil/media/socialmedia/
www.defense.gov/Sites
www.facebook.com/business/a/page-posting-tips
<https://business.twitter.com/basics>
<https://help.instagram.com/#>

Checklist for Establishing an Official Social Media Account

- Get command approval.**
See the [Secretary of the U.S. Army Memorandum, Delegation of Authority - Approval of External Presences](#) memo.
- Review official social media policies, guidelines, resources and required training.**
Before you get started with social media, it is important to understand DoD and U.S. Army social media policy. U.S. Army social media resources can be found at the top of the [U.S. Army Social Media Directory](#) and on the [U.S. Army's Slideshare](#) account.
- Determine your audience.**
Identify your intended audience and research their social media habits. This includes Soldiers, Families, veterans, U.S. Army civilians and the general public. Your stakeholders, politicians, community leaders, and criminals, imposters, adversaries or enemies are also watching.
- Determine your strategy and goals.**
What do you want to achieve/communicate? It could include distributing command information, connecting to a community, building esprit de corps, etc. Define your tactics that support those goals and how to measure success.
- Determine staffing.**
Ensure you have appropriate staffing and resources (personnel, equipment, connectivity, SOP's) to meet the requirements needed to maintain the platform. Identify primary and alternate social media managers and how alternate managers to take over established duties.
- Research and select social media platforms.**
Determine whether you can efficiently and effectively maintain and manage a social media account. Your audience's demographic will determine what platforms are most effective for reaching them in a meaningful manner. A person's age group, occupation, military affiliation, nationality and education influences what platforms he or she will be active on.
- Select your name and branding.**
Consider using a name that is easily remembered and logical. Avoid nicknames, callsigns, acronyms or mottos the public may not know. Use the official U.S. Army logo and other branded graphics to develop a cohesive identity that supports Department of the Army efforts. For more information on branding visit the [U.S. Army Branding Portal](#) or [Create](#) page.
- Draft content strategy.**
After identifying your audiences, selecting the platforms and approving branding, begin drafting a posting strategy based on your audience's engagement patterns.
- Develop policies, SOPs and training.**
The organization's social media team must develop organization-specific social media policies, procedures and training materials. Ensure the material is readily available and provide training to individuals at all levels of your organization, including Family Readiness Groups.

Page Resource Guide

Secretary of the U.S. Army Memorandum	http://armypubs.army.mil/epubs/Active_Collection_1.html
U.S. Army Social Media Directory	www.army.mil/media/socialmedia/
U.S. Army Slideshare	www.slideshare.net/usarmysocialmedia
Social Media and Operations Security Training Course	https://ia.signal.army.mil/login.asp
Social Network Class	http://iaseapp.disa.mil/eta/sns_v1/sn/launchPage.htm
Enterprise Army Branding Portal	www.usarmybrandportal.com
Army.mil Create	www.army.mil/Create

Official U.S. Army Social Media Account Requirements

Found on the U.S. Army Social Media Directory

- Point of contact**
The account must list a valid .mil or .gov email address.
- Official URL**
The account must have a URL to an official U.S. Army website. Use your command's website or www.army.mil if your organization does not have a website.
- User Terms of Agreement**
A account must have a user terms of agreement statement listed on the social media platform. An example of the specific wording can be found at [GSA's Negotiated Terms of Service \(TOS\) Agreements](#) web page.
- Labeled as an official account**
In order for an organization to maintain an official social media account it must clearly identify that the account is "official" somewhere on the page in accordance with DoD and U.S. Army policy. An example of the specific wording can be found in the left-hand column of the [U.S. Army's Facebook](#) page at or at the top of the [U.S. Army's Twitter](#) account.
- Open to the public**
All official accounts must be open to the public. Private groups, accounts or feeds will not be registered on the U.S. Army's social media directory.
- Labeled Government Organization**
Only official accounts on Facebook can be registered and should be labeled as a "government organization." The use of a Facebook profile, community or group page for official purposes violates the government's terms of service agreement with Facebook.
- Approval**
Submit the social media account for registration and approval on the U.S. Army Social Media Directory.
- Security**
Ensure your security settings are maximized and include two-step verification if available by the platform. For tips on securing your social media account review the Social Networking Safety Tips published on the [U.S. Army Criminal Investigation Command's website](#).

Page Resource Guide

GSA TOS	www.digitalgov.gov/resources/negotiated-terms-of-service-agreements/
U.S. Army Facebook	www.facebook.com/USArmy
U.S. Army Twitter	www.twitter.com/USArmy
U.S. Army Social Media Directory	www.army.mil/media/socialmedia/
U.S. Army CID Social Networking Safety Tips	www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf

Social Media Directory

Registration

Registering organizational social media sites through the [U.S. Army Social Media Directory](#) is not just encouraged, it is required. According to DoD Instruction (DODI) 8550.01 – DoD Internet Services and Internet-based Capabilities, official online presences must be registered on the external official presences list, maintained by the assistant secretary of defense for public affairs. Once your social media site is reviewed, approved and registered on the directory your organization will be in compliance with DODI 8550.01. You can find registration information and submission guidelines at the [U.S. Army Social Media Directory](#).

Registering your social media presence is quite simple. Once you have reviewed the DoD and Army requirements for operating an official social media presence and your social media site meets all of the submission requirements, use the upper right side of the [U.S. Army Social Media Directory](#) to submit your link. Once submitted, the U.S. Army Office of the Chief of Public Affairs' (OCA) Online and Social Media Division (OSMD) will review the submission to ensure it has all the elements required of official social media sites.

Once sites are approved for inclusion, your official social media site will be added to the directory. Qualifying accounts will be sent to the platforms as appropriate for consideration for verification. When a social media manager leaves their position with your organization, be sure to [email OSMD](#) to update the U.S. Army's social media contact list.

Directory

The U.S. Army's Social Media Directory includes links to thousands of official U.S. Army social media sites on Facebook, Twitter, Flickr, YouTube, Instagram and other platforms. It allows users to search for social media sites stored in the directory. Each entry has an icon for each social media site the organization maintains. This makes it easier to search for all of the social media presences belonging to a specific U.S. Army organization.

Audits

OSMD conducts periodic audits of the Social Media Directory to ensure units are complying with applicable guidelines, SOPs, policies and regulations. Units are notified of violations found during the audits and may be removed from the directory if the violations are not corrected.



Page Resource Guide

DoD Social Media Registry
U.S. Army Social Media Directory
Online and Social Media Division email

www.defense.gov/Sites
www.army.mil/media/socialmedia/
usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil



Maintaining Official Social Media Account

Enforce organizational posting policy and monitor comments

Have an [organizational social media policy](#) ([Enclosure](#)). However, just because a posting policy is in place with organizational requirements, terms of participation and posting guidelines, this does not mean everyone will abide by them. Make sure to review wall posts and comments on your page frequently and remove those that violate the policy or terms of usage. Keep in mind that social media does not take a break for the weekend. In some instances, weekend activity on Facebook can be busier than during the week, so have a plan to monitor and engage the organization's wall every day, even on days off, holidays and weekends.

Interact with audiences

Social media is more than just a platform to push command messages; it is a social community. Platforms such as Facebook and Twitter help people bridge geographical gaps to connect, talk and interact. Using social media can be valuable to a communication strategy, but it needs to be more than a sounding board for organizational messages. Social media should be used to facilitate the conversation, engage the population and keep people interested in the discussion to bring America closer to its Army. Each organization's audience will have unique social media usage patterns. Developing a content strategy and using platform analytics

will identify how often and what times you should post content. For example, OSMD publishes three to four posts per day on Facebook and five or more on Twitter. The U.S. Army Flickr and Instagram accounts are reserved for the best images. Analytics show that the U.S. Army's audience engages with Facebook content primarily during the day, and with Twitter content in the evening. An interesting note is that overall engagement rates mirror prime time television schedules.

Listen to the audience

Pay attention to the tone of comments made on your account and evaluate how your messages can shape those responses. Social media managers can use previous responses to tailor organizational messages to better engage with an audience. Ask for feedback and suggestions, and then act on user responses. Becoming a trusted resource that interacts with stakeholders builds a stronger relationship than an organization that is perceived to direct communication one-way, solely at their audience.

Mix it up

Balance the messages. It is important to post command messages and organizational information, but try to keep the page entertaining enough for people to want to follow. Do not be afraid to have fun by posting

Page Resource Guide

U.S. Army Social Media Policy Template www.slideshare.net/USArmySocialMedia/social-media-policy-draft-for-us-army-units
 Example Organization Policy Template [Enclosure](#), page 37

interesting links, asking trivia questions, or posting history, family oriented themes or National and U.S. Army observances. Try posting a photo of the day or asking a weekly question. Social media is social, so it is important not to fall into the trap of talking at your audience, instead of with your audience. The ratio of news, command messages and entertainment will vary based on your commander's intent, your organization's mission and your audience's demographics. For example, the U.S. Army's audience on Facebook has a stronger engagement rate with photos and videos depicting dynamic, motivational, training or deployment events. However, our Twitter audience responds well to breaking news and trending topics.

Engage with your audience

Once a social media account grows to a certain size, the population will likely use it as a resource and forum to ask questions. It is important to spend time responding to questions to establish a valued relationship with users. One-on-one conversations will show the community that their voices are being heard. Sometimes that interaction is as simple as thanking them for sharing a memory or thought. Other times it requires researching a topic for an answer, possibly referring the audience to other organizations and providing links to resources. Again, your commander's intent, your organization's mission and your audience's demographics will drive your interaction.

Measuring performance

Ten 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 is about trends and human feedback. Social media sites like [Facebook](#), [Twitter](#), [Google](#) and [YouTube](#) provide their own free analytic tools that allow administrators to track views, impressions, comments and engagement. Some analytic tools provide graphs and charts, but ultimately the presentation of information depends on the platform. These

different presentations make for a richer statistical analysis. Additionally, using free analytic tools can help a unit demonstrate the usefulness of a social media platform, and even highlight the success of a specific social media campaign. Some platforms, like Instagram, do not offer native analytics.

U.S. Army Facebook analytics example



Facebook and Twitter provide robust native analytic reports that account managers can utilize to determine the best time of day to post, the best day of the week to post and what type of content users prefer. This also allows managers to provide feedback to leaders on the effectiveness of specific posts and identify trends in the social media community. The analytic reports are free and provide a reliable resource that public affairs offices can use to illustrate the impact of a social media campaign.

U.S. Army Twitter analytics example



Page Resource Guide

Facebook: About Page Insights

www.facebook.com/help/336893449723054/

Twitter: Analytics

<https://analytics.twitter.com/>

Google: Analytics

www.google.com/analytics/

YouTube Analytics

www.youtube.com/analytics?o=U

Using Social Media for Crisis Communications



Officials answer questions during a press conference April 3, 2014, about the April 2 shooting incident at Fort Hood, Texas. (U.S. Army photo by Sgt. Ken Scar, 7th Mobile Public Affairs Detachment)

Crisis management

Using social media to communicate with stakeholders during a crisis has proven to be effective due to its speed, reach and direct access. In recent crises, 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 safely.

Build trust and credibility before a crisis

The time to start using social media and building your audience is not in the middle of a crisis. The best course of action during a crisis is to leverage existing social media accounts. If you have a regularly updated channel of communication before a crisis hits, then your audiences will know where to find information online. To build credibility, you need to establish a presence on social media platforms before a crisis even occurs. A large social media following does not happen overnight; be patient and execute your social media strategy. The better you are at providing relevant information and engaging your audience, the faster your following will grow. Establish partnerships with law enforcement, disaster response agencies, hospitals and news outlets, and invite them to participate in crisis response drills. If a real crisis occurs you can rely on these partnerships to assist you during your response.

Promote your social media account as the official source for information

During a crisis it is important that you highlight your social media efforts. Make sure the public, media and coordinating agencies are aware of where you will be releasing information. Announcing the details of a release, or directing your audience to a website where they can download the release, gives you the opportunity to have your message heard first and is an effective counter to rumors that can take hold and spread.

Post cleared information as it becomes available

Social media moves information quicker than ever, so when a crisis hits, do not wait for a formal press release. When you have solid, approved/cleared information, post it. This includes information about negative news items, as well. You can continue to post updated information as it becomes available. Not posting updates quickly during a crisis, or not keeping the community informed, may damage the organization's credibility. Rumors spread faster than ever with social media. Posting accurate information first, and providing subsequent updates, builds credibility and puts your message at the forefront of your audience's mind.



North Carolina National Guard Soldiers, assigned to 882nd Engineers Company (Vertical), 505th Engineers Battalion, assess the damage of a road in Eastover, S.C., October 13, 2015. The North Carolina National Guard has been ready to support the South Carolina Emergency Management Division and other state and federal partner agencies as South Carolina recovers from the effects of severe flooding throughout the state. (U.S. Army National Guard photo by Sgt. Brian Godette, 382nd Public Affairs Detachment)

Monitor content and conversations

Use search engines and other monitoring tools to track discussions on various topics. Google and other search engines have systems you can set up that email you news reports on particular topics. There are also websites that track hashtags, create usage reports and provide snapshots of current social media posts. Understanding where conversations are originating and the overall sentiment on social media is critical to the strategies and tactics you may use in crisis communications.

Answer questions

Be prepared to engage and answer your audience's questions. Anticipate likely questions the public may have and prepare responses ahead of time. Research current government and corporate crisis communication efforts and how

the public responds to them. Look for how you can apply what you learn to your organization. The best way to stop rumors is to be the first to release accurate information.

Share information

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

Analyze results

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

Impersonations

Imposter, unofficial, fan and parody accounts

The practice of impersonating Soldiers for financial gain is common. When imposter accounts are identified, it is important to report the accounts to the host platforms. Twitter allows users to create parody, satire, newsfeed, commentary, and fan accounts that mimic organizations, if they indicate that they are “unofficial” or “fan” accounts.

Identifying an imposter

If you suspect you have identified an imposter account you should confirm the account is not registered on the [U.S. Army Social Media Directory](#).

Imposters are damaging not only to an individual’s reputation, but also to the U.S. Army’s. It is important to know the warning signs of a scam or the common identifiers associated with an imposter account.

- The account is not registered and/or verified.
- The account has very few photos.
- Photos are posted in the same date range.
- The account has few followers or comments.
- The account name and photos do not match.
- There are obvious grammatical errors.
- Key information is missing.

Official accounts will not send friend requests. If you receive a request from an account claiming to be a senior leader, report it.

The individuals or groups establishing imposter accounts can be clever - using different user names, close spellings, personal photos, official photos, and even changing the nametape on Soldier’s uniforms. Remember, anyone in the U.S. Army Family is vulnerable.

Twitter parody example



Staff Sergeant Salvatore Giunta, Medal of Honor Recipient, was impersonated on Twitter before being awarded the Medal of Honor. It is important to be aware that [Twitter allows parody and fan accounts](#). After notifying Twitter the account was marked as a “tribute” or “fan” account.

Facebook imposters search example



Imposters regularly attempt to impersonate the U.S. Army’s Chief of Staff on social media platforms.

Page Resource Guide

U.S. Army Social Media Directory
Twitter parody and fan account policy

www.army.mil/media/socialmedia/
<https://support.twitter.com/articles/106373#>

Reporting imposters

Imposter accounts are violations of terms of use agreements. Most social media platforms have a reporting system that allows users to report an individual who is pretending to be someone else.

Soldiers, especially leaders, are prime targets for identity thieves who will use images posted online to create the fake accounts. It is good practice to search sites regularly for imposters.

Report 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 your local public affairs office or OSMD for assistance.

If a high-level U.S. Army official, such as a general officer, is impersonated, contact [OSMD via email](#) to request assistance with imposter accounts.



Facebook reporting system

Suggest Friends
Unfriend
Share Profile
Report/Block This Person

What You Can Do

Select an option below if you would like to unfriend or block this person:

Unfriend [redacted]
Stefanie will not be able to post on your wall

Block [redacted]
Blocking means you won't be able to see or contact each other on Facebook

Additionally, you may report this profile as the following:

This profile is pretending to be someone or is fake

Inappropriate profile photo

Inappropriate Wall post

My friend is harassing or bullying me

Is this your intellectual property?

Continue **Cancel**

Facebook also has a [web form](#) where individuals that do not have an account can report an imposter.



Twitter reporting system

Dear Twitter, someone is impersonating me!

Please fill out all the fields below so we can review your report.

I am being impersonated.

My company is being impersonated.

Not what you need help with? [Choose another topic](#)



Flickr reporting system

YAHOO! HELP

Report abuse in Flickr

If a photo or someone is violating our [Terms of Use](#) or [Community Guidelines](#), you can report it.

Report a photo for abuse

- Click on the image to open it.
- Scroll down to the "Additional info" section.
- Click **Flag this photo**.
- Click **Mark for review**.

Report a member for abuse

- Scroll to the bottom of the member's page.
- Click **Report abuse**.
- Fill out the form accordingly.
- Click **Send**.

Did you know? Using the "Report abuse" link sends us the specific page URL directly, enabling us to locate that content quickly and expedite any necessary action.



Instagram reporting system

(There is also an in-app reporting option)

Report an Impersonation Account on Instagram

If someone created an Instagram account that's pretending to be you or someone you know, use this form to file a report.

Which of the following best describes your situation?

Someone created an account for my business or organization

Someone created an account pretending to be me or a friend

Someone created an account pretending to be someone I represent (ex: my friend)

Send

Page Resource Guide

Online and Social Media Division email

Facebook

Facebook (non account holder)

Twitter

Flickr

Instagram

usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil

www.facebook.com/help/?faq=12256

www.facebook.com/help/contact/295309487309948

<https://support.twitter.com/forms/impersonation>

www.help.yahoo.com/kb/SLN7389.html/

<https://help.instagram.com/contact/636276399721841>

Always document the impersonator

- Take screenshots of the fake account and copy the URL to reference when you report the account. This helps clarify what account you are referencing and it records the imposter's actions. It is also good to document the accounts in order to track the volume of imposter accounts.
- Note when you report the account and when the platform takes it down.
- Keep a record of the accounts so you can track trends.
- Use reverse image searches to find fake accounts. These searches allow you use a jpeg or other image file to search the Internet and identify web addresses where the image appears. There are several resources you can use for this, such as [Google](#), [TinEye](#), [ImageBrief](#) and [Image Raider](#). This is not an exhaustive list and new sites and features are regularly added.
- Use search engine alerts to notify you of specific words, alternate spellings of names or organizations, hashtags or phrases being used online. There are many free resources available that allow you to automate your searches and create automated reports. [Google Alerts](#), [Yahoo! Alerts](#), [Talkwalker Alerts](#), [Social Mention](#), [IFTTT](#), [HashAtIt](#), [Hashtagifyme](#) and [Hashtags](#) are just a few websites that scour social media platforms and other websites for the words, phrases or topics you designate.



LinkedIn reporting system

LinkedIn and/or SlideShare Notice of Inaccurate Profile Information * Required

Name

Email Address

Instructions:

This Notice should be used if you believe that content in a member's LinkedIn and/or SlideShare account is inaccurate. For more information on our false profile policy, please visit [our Help Center](#).

LinkedIn relies on the integrity of its members in providing true and accurate information in their accounts, and does not control or vet user-generated content for accuracy. Submitting a Notice will not necessarily result in the removal of the account or information. LinkedIn and/or SlideShare will use this Notice, including your contact information, to investigate your claim.

What information is inaccurate or false?

Link to the inaccurate account or content: *
Copy and paste the URL of the account from your browser

Please explain how you know this account or other information to be inaccurate or false: *

Attach any files that are relevant to your request:
 No file selected.

Digital Signature

By submitting this Notice and entering my signature below, I confirm that I have read and understand the contents of the Notice of Inaccurate Profile Information form.

Typing your full name in this box will act as your digital signature: *

In order to answer your question or troubleshoot a problem, a LinkedIn representative may need to access your account, including, as needed, your messages and settings.



Google+ reporting system

Google+ Help GOOGLE+ HELP FORUM

Report impersonation

The page I'm reporting is:

Pretending to be me

Pretending to be someone else, not me

Falsely representing a company or organization

Page Resource Guide

Google Reverse Image Search	https://images.google.com/
TinEye	www.tineye.com/
ImageBrief	www.imagebrief.com/search#/landing
Image Raider	www.imageraider.com/
Google Alerts	https://www.google.com/alerts
Yahoo! Alerts	https://policies.yahoo.com/us/en/yahoo/privacy/products/alerts/
Talkwalker Alerts	www.talkwalker.com/alerts
Social Mention	www.socialmention.com/
IFTTT	https://ifttt.com/
HashAtIt	www.HashAtIt.com
Hashtagifyme	www.Hashtagify.me
Hashtags	www.hashtags.org
LinkedIn	https://help.linkedin.com/app/ask/path/TS-NFPI
Google+	https://support.google.com/plus/troubleshooter/1715140?hl=en

Social Media Scams

Common identifiers of scams

- A person asking for money
- Claims of supposed lack of support/services
- Communication only via social media/email
- Common spelling, grammatical or language errors

Types of scams

The [Federal Bureau of Investigation Internet Crime Complaint Center \(IC3\)](#) has identified current and ongoing Internet trends and scams. The following are scams that OSMD has identified that particularly affect military members:

- [Romance Scams](#)
- Identity Theft
- Internet Extortion
- Phishing/Spoofing
- Spam
- Third Party Receiver of Funds

Most of the reports OSMD receives are romance scams. CID receives hundreds of allegations a month from victims who state they became involved in an online relationship with someone, on a legitimate dating website or other social media website, who claims to be a Soldier. The “Soldier” then begins asking for money for various false service-related needs. Victims can lose tens of thousands of dollars, with a very low possibility of recovery.

These scams pose a unique challenge in the fight against imposters and identity thieves because they often require a dating profile in order to conduct a search for fake accounts. Because of this, it is difficult for organizations to monitor for impersonators using Soldier or key leaders’ information in a romance scam.

In addition, it is not possible to remove dating site profiles without legitimate proof of identity theft or a scam. If you suspect fraud on a dating site, take a screenshot of any advances for money or impersonations and report the account on the platform immediately.

Where to report scams

- Local law enforcement agencies
- U.S. Army Criminal Investigation Division
- [Department of Justice Computer Crime and Intellectual Property Section \(DOJCIPS\)](#)
- [Financial Fraud Enforcement Task Force](#)
- IC3
- [Federal Trade Commission’s Identity Theft Website](#), by calling 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261, or write to: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Tips to reduce vulnerability

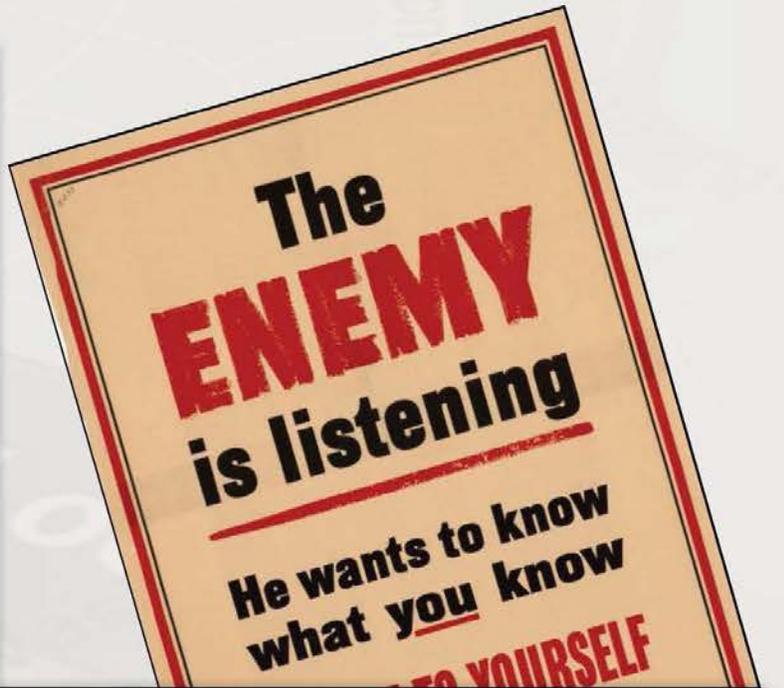
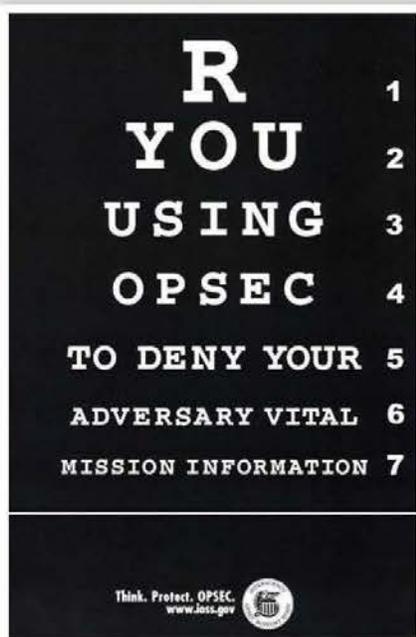
- Register official unit and senior leader accounts at the [U.S. Army Social Media Directory](#).
- Ensure privacy settings on all professional and personal accounts are set to the maximum.
- Go to [CID’s Security Tips, USA.Gov’s Online Safety](#), or the [FBI’s Common Fraud Schemes](#) for how to maximize security settings and configure accounts.

If you need further assistance

If you have identified and reported a suspected scam and need further assistance with reporting, [email OSMD](#) for assistance and include the URL the scam is being operated from, screenshots and any other proof of the imposter or account.

Page Resource Guide

Romance Scams	www.cid.army.mil/romancescam.html
Financial Fraud Enforcement Task Force	www.stopfraud.gov/report.html
IC3 Reporting	www.ic3.gov/complaint/default.aspx
Federal Trade Commission	www.ftc.gov/idtheft
CID Security Tips	www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf
CID: Romance Scams	www.cid.army.mil/romancescam.html
USA.Gov Online Safety	www.usa.gov/online-safety
FBI Common Fraud Schemes	www.fbi.gov/scams-safety/fraud/internet_fraud
U.S. Army Social Media Directory	www.army.mil/media/socialmedia/
Online and Social Media Division email	usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil
DOJCIPS	www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime



Checklist for Operations Security for Official U.S. Army Pages

- Designate managers:** Assign staff responsible for posting content to the official online account and make sure those individuals are current on all OPSEC training.
- Content submission:** Ensure all content is submitted to and approved by the commander or the organization's release authority prior to posting.
- Posted content:** Ensure all content is posted in accordance with the organization's public affairs guidance, and U.S. Army and DoD policies, instructions and regulations.
- Monitor:** Regularly check your social media account and make sure external social media users are not posting sensitive information on your official account.
- Training:** 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 Family members. It is 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 accounts within your organization for OPSEC violations. Never stop working to protect OPSEC. Once the information is out there, you can not get it back.

Making Potentially Dangerous Social Media Posts Safer

Dangerous	Safer
My Soldier is in the 82nd Airborne at Bagram Air Field, Afghanistan.	My Soldier is deployed to Afghanistan.
My Soldier will be leaving Kuwait and heading to Afghanistan in three days.	My Soldier deployed this week.
My Soldier is coming back at noon on Dec. 12, 2015.	My Soldier will be home this winter.
My family is back in Edwardsville, Ill.	I'm from the Midwest.

Operations Security

Safe social networking

Social media has become a big part of our Army lives. It helps organizations share information and keeps audiences connected. We depend on social media, but it can be extremely dangerous if you are not careful. Do you know what information you can post about your job? Did you know people can use social media to steal your identity? Did you know you can be at risk, even if you do not use social media? Operations security (OPSEC) and personal privacy concerns should be paramount when using social media both personally and professionally.

Training

ALARACT 289/2013, [Army Operations Security \(OPSEC\) Training for External Official Presence \(EOP\) Operators](#) states that all commanders will ensure that those personnel who publish information on external online presences receive mandatory annual OPSEC training.

Social media managers are required to take two OPSEC courses. The first, [OPSEC for EOP Operators](#), is accessed using the Information Assurance Training Center's website. Second is the [DISA Social Networking Class](#), found at the Defense Information Systems Agency's website.

OPSEC in daily interactions

Since social media use is so commonplace in our day-to-day interactions, it is



When a device is updated or patches installed, the equipment may revert to default settings, potentially enabling devices to embed Global Positioning System locations into photographs or insert map locations in social media posts. Ensure that Soldiers and PAO staff are educated on GPS technology present in devices and the security risks associated with the technology.

easy to become complacent. To maintain OPSEC, it is important to remain vigilant at all times. Sharing seemingly trivial information online can be dangerous to loved ones and fellow Soldiers. America's enemies scour blogs, forums, chat rooms and personal websites to piece together information that can harm the U.S. and its Soldiers. Never accept a friend request from someone you do not know, even if they know a friend of yours. Do not share information that you do not want to become public. Someone might target you for working in the DoD, so be cautious when listing your job, military organization, education and contact information. Providing too much information in your profile can leave you exposed

to people who want to steal your identity or sensitive operational information. Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but more can be done by adjusting your privacy settings.

Geotagging safety

Geotagging is the process of adding geographical identification to photographs, videos, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything posted on the Internet. Some smartphones and digital cameras automatically embed geotags into pictures and many people unknowingly upload photos to the Internet that contain location information.

Page Resource Guide

[OPSEC for EOP Operators](#)
[DISA Social Networking Class](#)

https://iatraining.us.army.mil/iaseapp.disa.mil/eta/sns_v1/sn/launchPage.htm

A variety of applications are capitalizing on users' desire to broadcast their geographic location. The increased popularity of location-based social networking is changing the way we view security and privacy on an individual level and creating OPSEC concerns at Army level. One Soldier exposing his/her location can affect the entire mission. Deployed Soldiers, or Soldiers conducting operations in classified areas, should not use location-based social networking services. These services will bring the enemy right to the Army's doorstep.

CID Security Flyers

Criminal Investigation Command's (CID) Computer Crime Investigative Unit publishes [cyber crime prevention flyers](#) and cyber crime alert notices to provide a comprehensive view on Internet safety.

Online Misconduct

[Online misconduct](#) is a term that describes unacceptable or improper behavior through the use of technology. There are mechanisms for reporting online misconduct. While there is no Federal criminal statute called "online bullying," misuse of online communications, sending harassing or intimidating communications and images, or other online misconduct may violate existing Federal

laws under the United States Code and may also be a violation of the UCMJ.

Social Networking Safety Tips

[Social networking sites](#) allow people to interact with others and find people with similar interests or backgrounds. These sites enjoy worldwide popularity, underscoring the need to understand potential risks associated with the use of these sites. A person's online activities may inadvertently expose excessive information about their identity, location, relationships and affiliations, creating an increased risk of identity theft, stalking, or targeted violence.

Twitter

Assume that once something is posted to [Twitter](#), and by extension the Internet, no amount of effort will eliminate it. The Internet does not forget. There are sites that collect Twitter content and keep copies of Tweets on searchable servers. Because of this, anyone, whether they have a Twitter account or not, can see your Tweets.

Facebook

[Facebook](#) has many options available that allow various levels of access to your account. Consider setting trusted contacts, limit who can look you up, set login

alerts, and enable two-step verification when logging in.

Google+

[Google+](#) collects content and data from across all its product lines, including YouTube, Gmail, Google Maps, Google News. The company is very effective making connections from your single, unified profile. Therefore, profile settings on Google products should be monitored and set accordingly.

LinkedIn

When configuring [LinkedIn](#) for maximum safety, users must decide for themselves how to balance privacy, security and safety against the value of building a successful business network. Regardless of how effectively and completely you control LinkedIn settings, there is no way to completely hide a LinkedIn profile.

Page Resource Guide

CID Security Flyers	www.cid.army.mil/cciu2can.html
Online Misconduct	www.cid.army.mil/documents/CCIU/2can/OnlineMisconduct.pdf
Social Networking Safety Tips	www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf
Twitter	www.cid.army.mil/documents/CCIU/2can/CPFFTwitter.pdf
Facebook	www.cid.army.mil/documents/CCIU/2can/CCPFFacebook.pdf
Google+	www.cid.army.mil/documents/CCIU/2can/CCPFGooglePlus.pdf
LinkedIn	www.cid.army.mil/documents/CCIU/2can/CCPFLinkedIn.pdf

Social Media for Soldiers, Staff and Families



Online Conduct - Think, Type, Post

The U.S. Army defines online conduct as the use of electronic communications in an official or personal capacity that is consistent with [U.S. Army Values](#) and standards of conduct. It is important that all Soldiers know that once they have logged on to a social media platform, they still represent the U.S. Army.

Online **misconduct** is a term that describes unacceptable or improper behavior through the use of technology. While there is no Federal criminal statute called “online bullying,” misuse of online communications, sending harassing or intimidating communications and images, or other online misconduct may violate existing Federal laws under the United States Code.

“**Think**” about what message is being communicated and who could potentially view it.

“**Type**” messages that are consistent with U.S. Army Values.

“**Post**” if the message demonstrates dignity and respect for self and others.

[ALARACT 122/2015, Professionalization of Online Conduct](#), defines cyber misconduct as “the use of electronic communication to inflict harm. Examples include, but are not limited to: harassment, bullying, hazing, stalking, discrimination, retaliation, or any other types of misconduct that undermine dignity and respect.” The U.S. Army is a values-based organization where everyone is expected to do what is right by treating all persons as they should be treated – with dignity and respect, as outlined in [AR 600-20, Army Command Policy](#), paragraph 4-19 4–19. Treatment of persons.

Members of the U.S. Army community should **report incidents** to their chain of command or family support services for resolution. Additional avenues for reporting and information include the Equal Opportunity (military), Equal Employment Opportunity (civilians), SHARP, the Inspector General, and Law Enforcement offices.

More information can be found at the [Online Conduct - Deputy Chief of Staff, Army G1](#).

Joining networks

Social media helps individuals with similar interests connect and interact. Soldiers are authorized to utilize a variety of platforms as long as their involvement does not violate unit policy or the basic guidelines of the UCMJ.

Setting guidelines

Leaders should communicate social media expectations with their Soldiers. It is important to outline unit policy, making sure Soldiers know what they can and cannot do on social media. A [Example Organization Policy \(Enclosure\)](#) can be customized to each unit.

Follow the UCMJ

Soldiers using social media must abide by the UCMJ at all times, even when off duty. Commenting, posting or linking to material that violates the UCMJ or basic rules of Soldier conduct is prohibited, including talking negatively about supervisors or releasing sensitive information.

Page Resource Guide

U.S. Army Values	www.army.mil/values/
CID Cyber Misconduct	www.armyg1.army.mil/docs/CyberMisconductFlyer.pdf
ALARACT 122/2015	https://www.milsuite.mil/book/docs/DOC-215026
AR 600-20 Army Command Policy	www.apd.army.mil/pdf/files/r600_20.pdf
Online Misconduct: Awareness and Reporting	www.cid.army.mil/documents/CCIU/2can/OnlineMisconduct.pdf
Online Conduct - Army G1	www.armyg1.army.mil/ONLINECONDUCT.asp
Example Organization Policy	Enclosure, page 37

Social media and Army Families

Social media is becoming a valuable tool for keeping Families and Soldiers connected, which is vitally important to unit well-being. Family Readiness Groups (FRGs) are key organizations. FRG social media sites have streamlined the process of finding out what is happening at an installation. They also provide discussion sections where the FRG, Soldiers and Families can post information and photos about installation news and activities. OCPA recommends FRG site be configured as closed groups for maximum safety.

Security and safety

- Do not reveal sensitive or personal information, such as addresses, schedules and event locations.
 - Do not post when you are going on vacation or leaving the house
 - Ask, “What could a person do with this information? Could it compromise the safety of myself, my Family or my unit?”
 - Geotagging reveals your location to other people within your network. Smartphones can embed GPS coordinates into photographs and other data. Turn off the GPS function on smartphones and digital cameras. Always make sure to check that the geotagging is not reset after updating operating software.
 - Closely review photos or videos before posting to ensure sensitive or personal information is not released.
 - Talk to your Family about OPSEC. Be sure they know what can and cannot be posted.
 - Look closely at all privacy settings. Set security options to allow visibility only to individuals you know.
 - Platform security and privacy settings change frequently. Routinely check and update settings to be as restrictive as possible.
 - Utilize two-step verification when possible to prevent unauthorized access in the event your password is compromised.
- Passwords should be at least 14-characters long and contain at least two: numbers, special characters, upper-case characters, and lower-case characters.
 - Change passwords every 60 days.
 - Do not share passwords.

For more [tips](#) and [home computer security](#) visit the [CID Cyber Lookout Program](#).

Duty status-whereabouts unknown (DUSTWUN), missing in action (MIA) wounded in action (WIA) and killed in action (KIA)

Social media is a major part of our daily interactions, so when Soldiers are killed or missing in action, it is hard to turn off the flow of information distributed through social media platforms. While it is difficult to prepare for tragedy, it is important to know that social media can play a role (good or bad) in the handling of DUSTWUN, MIA, WIA or KIA situations.

In a DUSTWUN, MIA, WIA or KIA situation, members of the media may look at unit, Soldier and Family member Facebook profiles to find out more about the Service member. In a captivity situation, captors may also turn to Facebook to pull information for interrogation purposes. It is vitally important that you and your Family set privacy settings as restrictive as possible.

In accordance with DoDI 1300.18, Department of Defense (DoD) Personnel Casualty Matters, Policies, and Procedures, details about Soldiers killed or missing in action cannot be released until 24 hours after the next of kin has been notified and after the information has been [released by the DoD](#). It is important that all friends, Family and fellow Soldiers know that information about individuals killed in action must not be released before the next of kin is notified. Always follow unit and Army protocol when it comes to DUSTWUN, MIA, WIA or KIA situations.

Page Resource Guide

Social Networking Safety Tips
Home Computer Security
CID Cyber Lookout Program
DoD News Releases

www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf
www.cid.army.mil/documents/CCIU/2can/HomeSecurityPractices.pdf
www.cid.army.mil/cciu2can.html
www.defense.gov/releases

Social Media in Garrison, Training and While Deployed

Connecting your audiences

More and more commanders are leveraging social media not just in garrison, but also in training and deployment environments to keep the public informed, Families connected, and to address negative news stories and inaccurate reports.

The accounts below are examples of effective social media use that an organization or individual can emulate, taking strategies and tactics from, to build a new account or energize an existing account.



2nd Stryker Brigade Combat Team, 2nd Infantry Division

www.facebook.com/lancerbrigade

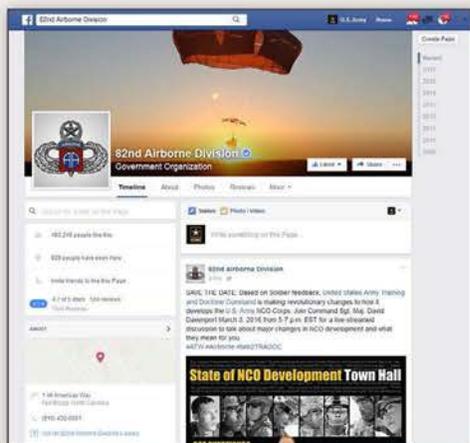
The 2nd Stryker Brigade Combat Team, 2nd Infantry Division regularly posts videos and photographs taken in garrison, training and deployed environments. By using hashtags, linking to partner nations' social media accounts and providing a range of topics that engage a variety of audiences, their account has the ability to tell the Army's story to a wide demographic.



25th Infantry Division

www.facebook.com/25thid

When it comes to using social media to complement a unit's outreach strategy, 25th Infantry Division utilizes a comprehensive program that provides a mix of training, history, command information, community interest, and Morale, Welfare and Recreation posts. Their use of graphic elements compliments the narrative in their posts, and helps draw their audience into the posts. They also share external sources of information in their news feed, further exposing those audiences to the 25th ID account.



82nd Airborne Division

www.facebook.com/82ndAirborneDivision

The 82nd Airborne Division provides a conduit for information flow to their Soldiers and highlights their activities as a critical component in our nation's ability to respond to a global crisis. The unit selects dynamic content that encompasses regional military operations, award ceremonies, military and unit history, military competitions, and the daily life of Service members. This provides a critical window for Family members, media and interested parties. They actively post photos and videos loaded directly to the social media platform, helping drive awareness and a continued engagement momentum with current and new audiences.

U.S. Army Leaders on Social Media

Reaching out

Social media allows a leader to communicate directly with a large number of individuals while simultaneously retaining a one-on-one tone. But this takes commitment, a plan and follow-up. An effective social media presence is about daily interactions, commenting on responses, and conducting scheduled analysis of efforts. Some of the U.S. Army's highest-ranking leaders have tapped into social media platforms to communicate and connect with the population at large. By reaching out through social media, U.S. Army leaders are engaging with 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. Remember to be authentic, post regularly, post relevant content, use photos and videos, and use a mix of native and shared content.

Acting Secretary of the U.S. Army Patrick J. Murphy

The Acting Secretary of the U.S. Army, Patrick J. Murphy, is a vocal supporter of social media. He encourages engagement and interaction with his audience by directly participating on his platforms, posting messages to organizations, responding to comments on his accounts, sharing relevant content from other accounts and highlighting key topics regarding the U.S. Army trending in the news.

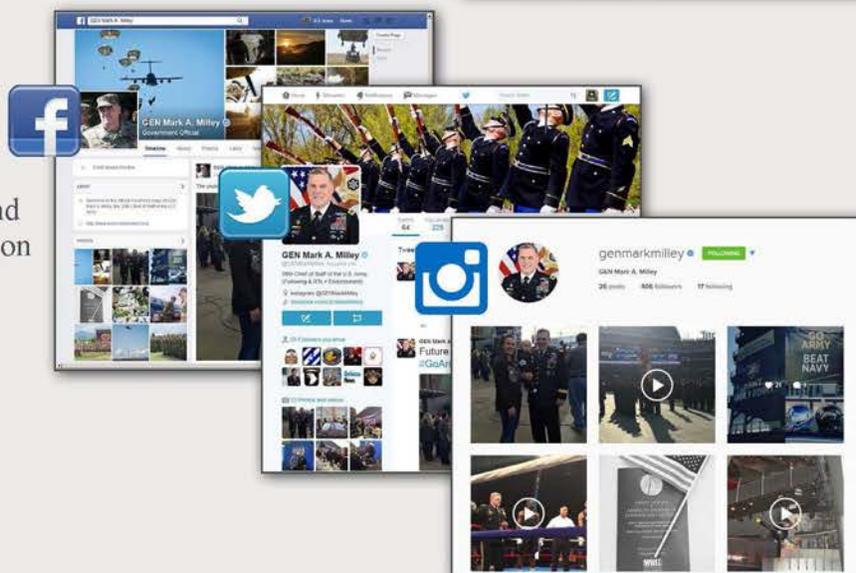
Facebook: [Under Secretary of the Army Patrick Murphy](#)
Twitter: [@PatrickMurphyPA](#)
Instagram: [PatrickMurphyPA](#)



Chief of Staff of the U.S. Army Gen. Mark A. Milley

Gen. Mark A. Milley uses social media to engage with various U.S. Army audiences by posting, commenting, Tweeting and responding to people who engage on his sites.

Facebook: [GEN Mark A. Milley](#)
Twitter: [@GENMarkMilley](#)
Instagram: [genmarkmilley](#)



Page Resource Guide

Hon. Murphy:	www.facebook.com/MurphyforPA/timeline www.twitter.com/PatrickMurphyPA www.instagram.com/patrickmurphy/
Gen. Milley:	www.facebook.com/GENMarkMilley/ www.twitter.com/GENMarkMilley www.instagram.com/genmarkmilley/

Facebook Quick Reference Guide



Organizational:

- **Do not** use military slang or acronyms in organizational posts.
- **Do schedule posts** throughout the day to avoid spamming your audience.
- **Do not** be too promotional or appear self congratulatory.
- **Do not** use boilerplate messages or press releases, unless necessary.
- **Always** provide some sort of lead, description or call to action when posting a link - do not post just the link.
- **Do not** use copyright protected material.
- **Do not** endorse companies or products.
- **Do not** consider the number of like or fans indicating successful key engagement.
- **“Like”** other organizations, and similar content.

Leaders:

- **Do** be authentic.
- **Do not** use social media slang in professional posts.
- **Do not** post too many times a day (you will lose followers).
- **Disable geotagging** in programs or applications.
- **Do not** remove a comment or post because you do not like it. If it is not a violation of your comment policy, or Facebook’s community rules, leave it!
- **Do** respond to comments made to your posts and reinforce positive dialogue.
- **Remember** you do not control what happens to a message once it is posted.
- **Start** with a strategy – How does social media fit into your overall communication goals?
- **Tag** other accounts in posts.
- **List** links to your organization and other platforms on your information tab.

All Users:

- **Do not** violate endorsement or copyright rules.
- **Post often**, ideally three times a week or more.
- **Distribute your posts** throughout the day, nights and weekends.
- **Evaluate which time** works best to post.
- Try to **tag at least one** appropriate page in each post
- **Engage with** your audience, ask questions when possible.
- **Respond to** questions in a timely manner.
- Post a **comment policy** and enforce it.
- **Spell and grammar check** every post prior to posting.
- **Mix it up** when posting photos, questions, videos, shares, etc.
- **Ask yourself:** Would I share that with my friends?
- Add a **unique touch**; create relationships with your audience.
- **Set defaults** to show only your posts but allow comments.
- **Welcome** participation, collaboration and feedback.
- **Track metrics** and evaluate how content performs over time.
- **Engage** audiences on other accounts.
- **Identify/find** subject **matter experts** to answer questions that people ask on your page.
- **Avoid using automated posting services** to post same content to multiple sites.
- **Post** native videos.

Page Resource Guide

Facebook scheduling
U.S. Army Slideshare

<https://www.facebook.com/help/389849807718635>
www.slideshare.net/USArmySocialMedia/social-media-roundupgeotagging-safety

Good Posts



#USArmy Soldiers, assigned to the Virginia National Guard, fire an M2 machine gun during pre-deployment training at Fort Pickett, Va., July 14, 2015.

U.S. Army photo by Sgt. 1st. Class Terra C. Gatti, The National Guard

DO:

- Create a list of unique topics that need special approval to post, like host nation sensitivities.
- Check every post for potential safety violations.
- Have someone check hashtags, proofread your posts for grammar and spelling errors before posting.
- Always post a caption to provide context for a photograph or video.

Bad Posts



Virginia National Guard soldiers fire a M2 heavy machine gun during pre-deployment training at Ft. Pickett, Va., July 14, 2015. 30 Soldiers assigned to the 29th Infantry Division will deploy from Fort Bragg, N.C. to Afghanistan, Sept. 25, 2015 and are expected to return May 15, 2016.

DON'T

- Violate Security, Accuracy, Propriety or Policy.
- Violate AP Style or DoD Captioning Style Guides.
- Forget to leverage hashtags (#) and tag other social media accounts.
- Fire and forget - your audience looks for feedback to their comments.



DO:

- Use quality photos with a concise, 5Ws caption.
- Use one photo and a link to where the audience can find more is ideal.



DON'T

- Use a large number of photos.
- Assume your audience understands what is happening in the photos.

Good Posts

Bad Posts

U.S. Army Fort Leonard Wood
February 26 at 1:11pm · 🌐

A #FortLeonardWood commander recently provided the commencement address at a graduation ceremony for aspiring area leaders.



Garrison commander inspires new area leaders
A Fort Leonard Wood commander recently provided the commencement address at a graduation ceremony for aspiring area leaders.
ARMY.MIL | BY MRS. MARTHA YOSHIDA (LEONARD WOOD)

U.S. Army Fort Leonard Wood
February 26 at 4:00pm · 🌐

Faces of the Fort Friday: A closer look into the lives of #FortLeonardWood community members.

"I joined the Army because I was ready for a different set of challenges. I was in college at the time and had been there for three years, so joining the Army was kind of a decision to take a step back and start over. I was working as a janitor, and the head facilities guy had mentioned to me that West Point was a great institution. I Googled it, liked what I saw and started the a... See More



DO:

- Keep posts concise and the main point up front so it is seen on desktop and mobile devices.
- [Link to](#) an external article or site for in-depth explanations.
- Think about posts as deep headlines that gets people to read the articles.
- Leverage hashtags and links to other social media accounts.

DON'T

- Try to fit an entire article into a post, causing your audience to move on the next post.
- Bury the news peg and assume your audience will click on the "See More" link.
- Forget to leverage hashtags (#) and tag other social media accounts.

U.S. Army shared 101st CAB, Wings of Destiny's photo
Published by Matthew MacRoberts [P] · February 2 at 7:03pm · 🌐

A #USArmy Soldier, assigned to the 101st Airborne Division (Air Assault), performs maintenance on a helicopter at U.S. Army Fort Campbell, Ky., Jan. 28, 2016.

U.S. Army photo



DO:

- Add unknown information to a share.
- Localize the news peg for your audience.

US Army Fort Benning shared U.S. Army Garrison Fort Benning's photo
7 hrs · 🌐

U.S. Army Armor School US Army Infantry School, Ft Benning, Georgia
316th Cavalry Brigade 14th Combat Support Hospital 199th Infantry Brigade 198th Infantry Training Brigade 194th Armored Brigade Fort Benning MWR US Army Airborne School, Fort Benning Airborne and Ranger Training Brigade

Briant Wells Field House open for combatives training evenings and Saturdays



MON 1800-1930 Gi Jiu-Jitsu class; TUE 1800-1930 No Gi Jiu-Jitsu class; WED 1800-1930 Wrestling or Kick Boxing class (based on demand); THUR 1800-1930 No Gi Jiu-Jitsu class; FRI 1800-1930 Gi Jiu-Jitsu class; SAT 0900-1300 open mat

DON'T

- Just tag accounts in a share.
- Just add a hashtag to a share.
- Repeat the same information.

Facebook Quick Start Page

Account Name	URL
U.S. Department of Defense (DOD)	www.facebook.com/DeptofDefense
NATO	www.facebook.com/NATO
U.S. Coast Guard	www.facebook.com/UScoastguard
U.S. Navy	www.facebook.com/USNavy
United States Air Force	www.facebook.com/USairforce
U.S. Marine Corps	www.facebook.com/marines
U.S. Department of Veterans Affairs	www.facebook.com/VeteransAffairs
Secretary of Defense Ash Carter	www.facebook.com/SECDEF
Under Secretary of the Army Patrick Murphy	www.facebook.com/MurphyforPA
GEN Mark A. Milley	www.facebook.com/GENMarkMilley
General Frank J. Grass	www.facebook.com/GeneralGrass
LTG Jeffrey W. Talley	www.facebook.com/LTGJeffreyWTalley
U.S. Army	www.facebook.com/USArmy
U.S. Army Central	www.facebook.com/usarmycentral
U.S. Army Training and Doctrine Command	www.facebook.com/USArmyTRADOC
U.S. Army Forces Command (FORSCOM)	www.facebook.com/FORSCOM
U.S. Army Europe	www.facebook.com/USArmyEurope
U.S. Forces Korea (Official Page)	www.facebook.com/myusfk
The National Guard	www.facebook.com/TheNationalGuard
U.S. Army Reserve Command - Fort Bragg, NC	www.facebook.com/USArmyReserveCommand
3d U.S. Infantry Regiment (The Old Guard)	www.facebook.com/oldguard/
I Corps	www.facebook.com/1stCORPS
III Corps and Fort Hood	www.facebook.com/forthood
XVIII Airborne Corps	www.facebook.com/XVIII.Airborne.Corps
1st Cavalry Division	www.facebook.com/1stCavDiv
1st Infantry Division	www.facebook.com/1stInfantryDivision
3rd Infantry Division	www.facebook.com/3rd.Infantry.Division
4th Infantry Division	www.facebook.com/4thID
7th Infantry Division	www.facebook.com/7thInfantryDivision
U.S. Army Fort Drum & 10th Mountain Division	www.facebook.com/drum.10thmountain
25th Infantry Division	www.facebook.com/25thid
82nd Airborne Division	www.facebook.com/82ndAirborneDivision
101st Airborne Division (Air Assault)	www.facebook.com/101st
GOARMY.COM	www.facebook.com/GoArmy
U.S. Army Cadet Command (ROTC)	www.facebook.com/cadetcommand
West Point - The U.S. Military Academy	www.facebook.com/WestPointUSMA
Army Medicine	www.facebook.com/OfficialArmyMedicine
U.S. Army Chaplains Corps	www.facebook.com/ArmyChaplainCorps
NCO Journal	www.facebook.com/NCOJournal
Soldiers Magazine	www.facebook.com/SoldiersMag

Twitter Quick Reference Guide



Organizational:

- **Do** keep the 140 character limit - do not break Tweets into multiple sections.
- **Do** use photos or native videos in every Tweet, and remember these use approximately 24 characters.
- **Do** remember that once a message posts you do not control what happens to it.
- **Do not** mix professional and personal accounts on the same device.
- **Do** include a link to your official website and the disclaimer “Official Twitter page of... (Following, RTs and links ≠ endorsement)” in your profile information.
- **Do not** cluster all of your Tweets close to the same time.
- **Do** Tweet breaking news related to your unit.
- **Do** live Tweet events.
- **Do not** be too promotional.

Leaders:

- **Do** be authentic.
- **Do not** Tweet too many times in a day.
- **Do not** follow imposters or those religious or political affiliated organizations.
- **Do not** obsess about your number of followers.
- **Do not** add location to Tweets.
- **Do not** use automated Tweets with no engagement (“I just posted a photo to Facebook”).
- **Do** Tweet Army senior leader quotes.
- **Do** engage with your Twitter audience by asking questions and Retweeting their answers.
- **Do** check your direct messages and mentions daily and respond.
- **Do not** post Tweets directly to other platforms.

All Users:

- **Do not** violate endorsement or copyright rules; seek guidance if in doubt.
- **Do** be creative by posting different types of information.
- **Do** use Twitter to communicate during a crisis.
- **Do** follow other Army and DoD Twitter accounts.
- **Do** check often for new Twitter accounts and acknowledge, follow, share, etc.
- **Do** Retweet/Quotetweet content from other accounts while also adding your organization’s words.
- **Do** tag other accounts.
- **Do** listen to what your followers are talking about.
- **Do** create a voice and be authentic.
- **Do** become the go-to resource for timely news and information.
- **Do** focus on Tweeting exceptional content.
- **Do** mix up your Tweeting times.
- **Do** edit your Tweets and avoid typos.
- **Do** brand your page.
- **Do** list your Twitter page on your Facebook page about section.
- **Do** limit the number of hashtags (#) in posts - know how they are used on the platform.
- **Do not** Tweet with unprofessional Twitter language (“lol” “2 be” “OMG”).
- **Do not** let your Twitter account become stagnant (go more than a day without Tweeting).

Elements of a Tweet

Public tag of Twitter user Handle/Tag Hashtag

USArmy U.S. Army
 .@2ndCAB Soldiers participate in Operation
 #AtlanticResolve http://goo.gl/J0oJe cc: @CNN
 5 Jul

Retweet and public reply Handle/tag Shortened URL

USArmy U.S. Army
 RT @FightingFirst: Soldiers conduct convoy operations with
 @USArmyReserve Soldiers Dec. 16, 2016 http://goo.gl/J0oJe
 5 Jul

<p>Corrected Tweet</p> <p>USArmy U.S. Army CT: @usfor_a:... http://goo.gl/J0oJ 5 Jul</p>	<p>Modified Tweet</p> <p>USArmy U.S. Army MT: @usfor_a:... http://goo.gl/J0oJ 5 Jul</p>	<p>A corrected Tweet is a correction of the record when there is an error in an earlier Tweet. Modified Tweets credit the original source, allowing for localization.</p>
---	--	---

Quote Tweet

Malcolm Frost @Malcolm_Frost · Dec 13
 .@USArmy broadcasters & journalists ensure Public Affairs tells the #USArmy story; an ever-growing critical mission

U.S. Army Racing @ARMYRACING
 Today's #Army #career of the day is 46R Public Affairs Broadcast Specialist. Check it out ht.ly/UKQtw

U.S. Army @USArmy
 .@FightingFirst Soldiers fire an M109 Paladin during a range at @usarmycentral's Camp Buehring, Kuwait, Dec 13, 2015

0:39

Post videos natively and use a call to action where appropriate. Use a period before the @-sign when tagging at the beginning to make it a public Tweet.

GoArmy @GoArmy · Feb 24
 #POTD: A #USArmy paratrooper from @173rdAbnBde awaits signal from the jumpmaster to exit a Black Hawk helicopter.
 grafenwoehr.com

Strong action photo Tweeted with other accounts tagged and using hashtags conversationally.

Good Tweets



U.S. Army @USArmy · Dec 15

A #USArmy Soldier qualifies with a M16A2 during #AtlanticResolve in Lithuania, Dec. 8, 2015

DO:

- Use hashtags (#) in every Tweet.
- Leverage established hashtags already being used by other organizations or units before creating a new one.



U.S. Army @USArmy · Dec 15

A #USArmy Soldier participates in a sleep study to measure performance after resting, Dec. 8, 2015

DO:

- Coordinate hashtag use with to maximize engagement potential.
- Use trending hashtags.



U.S. Army @USArmy · Dec 15

.@wrair experts discuss effects of sleep deprivation on #USArmy Soldier performance <http://go.usa.gov/ckKp7>

DO:

- Use links to articles and websites in Tweets to drive viewers to more information.
- Use URL shorteners, preferably the General Services Administration (GSA) site for [government URLs](http://go.usa.gov/).



U.S. Army @USArmy · Dec 15

.@USNationalGuard Soldiers use a water bucket to fight a forest fire in California, April 11, 2015

DO:

- Include critical information and maximize character use.

Bad Tweets



U.S. Army @USArmy · Dec 15

A #USArmy #Soldier qualifies with a #M16A2 during #Exercise #SniperShot at #FortBliss, #Texas, Dec. 8, 2015

DON'T

- Use more than two or three hashtags.
- Forget to explain or advertise hashtags early and often.
- Use general hashtags.



U.S. Army @USArmy · Dec 15

A U.S. Army Soldier participates in a sleep study to measure #performance after resting, Dec. 8, 2015

DON'T

- Forget to research hashtags for association to inappropriate content or conflicts with Army Values.



U.S. Army @USArmy · Dec 15

.@wrair experts discuss effects of sleep deprivation on #USArmy Soldier www.army.mil/xyz23456waytoolong.gov

DON'T

- Forget to use the government link shortener to manage long URLs.



U.S. Army @USArmy · Dec 15

.@USNationalGuard #Soldiers #FireFighters #California

DON'T

- Solely post hashtags or tags to accounts.

Good Tweets



U.S. Army @USArmy · Dec 15

A @USArmyReserve Soldier conducts land navigation training at Fort Bragg, N.C., Dec. 8, 2015

DO:

- Tag other accounts to leverage their audience engagement.

Bad Tweets



U.S. Army @USArmy · Dec 15

A U.S. @ArmyReserve Soldier conducts land navigation training at Fort Bragg, N.C., Dec. 8, 2015

DON'T

- Assume you know the correct account information for a tag in your Tweet.



U.S. Army @USArmy · Dec 15

The #USArmy Infantry is more effective with Stryker than w/out for delivering battlefield lethality <http://go.usa.gov/p7>



DO:

- Use a photo or video to generate interest in a Tweet.



U.S. Army @USArmy · Dec 15

(1/3) #USArmy Infantry is more effective with Stryker than w/out for delivering lethality to the battlefield. The next



U.S. Army @USArmy · Dec 15

(2/3) round of Stryker modernization will include main gun upgrades and armor improvements to better protect



U.S. Army @USArmy · Dec 15

(3/3) the Soldiers inside the vehicle.

DON'T

- Break a Tweet that is more than 140 characters into multiple sections.



U.S. Army @USArmy · Dec 15

A #USArmy Soldier conducts airborne operations at Joint Base Elmendorf-Richardson, AK, Dec. 8, 2015



RETWEETS
96

LIKES
249



U.S. Army @USArmy · Dec 15

I posted a photo to Facebook fb.me/LinkToFacebookPost

DO:

- Add unknown information to a Tweet.
- Use a different photo or video to cross promote messages on various platforms.
- Localize Tweet to your audience.

DON'T

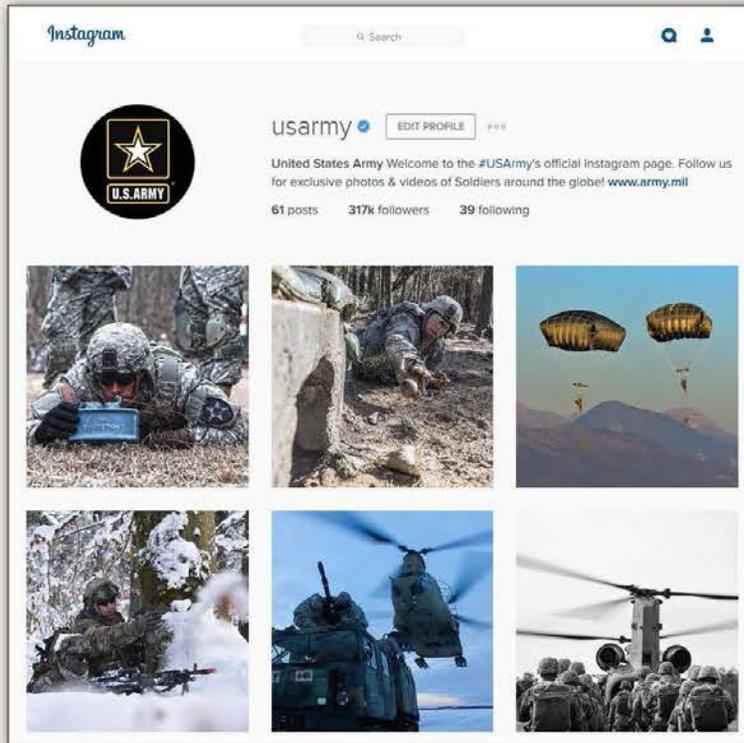
- Use automation tools to Tweet.

Page Resource Guide

Twitter Quick Start Page

Account Name	Account	Hashtag
U.S. Dept of Defense	@DeptofDefense	#SecDef
DoDNews	@DoDNews	#DoD
The Joint Staff	@thejointstaff	
U.S. Central Command	@CENTCOM	
NATO	@NATO	
US Mission To NATO	@USNATO	
USCG (Official)	@USCG	
U.S. Navy	@USNavy	#USNavy, #NavyWeek
U.S. Air Force	@usairforce	#AirForce
U.S. Marines	@USMC	
U.S. Army	@USArmy	#USArmy
Patrick J. Murphy	@PatrickMurphyPA	#SecArmy
GEN Mark A. Milley	@GENMarkMilley	
Lt. Gen. Talley	@jeffreywtalley	
MG Jeffrey Snow	@USAREC_CG	
Gary Volesky	@GVolesky	
BG Malcolm Frost	@Malcolm_Frost	
John Kirby	@statedeptspox	
FORSCOM	@FORSCOM	
U.S. Army TRADOC	@TRADOC	
U.S. Army Europe	@USArmyEurope	#StrongEurope
US Army Africa	@USArmyAfrica	#AfricanHorizons
U.S. Army Pacific	@USARPAC	
National Guard	@USNationalGuard	
U.S. Army Reserve	@USArmyReserve	
I Corps	@I_Corps	
1st Cavalry Division	@1stCavalryDiv	
3rd ID and FSGA-HAAF	@3rd_Infantry	
4th Infantry Div.	@4thInfDiv	
7th Infantry Division	@7thID	
Fort Drum & 10th Mtn	@drum10thmtn	
82nd Airborne Div	@82ndABNDIV	
GoArmy	@GoArmy	#ArmyTeam
Army ROTC	@armyROTC	
US Military Academy	@WestPoint_USMA	#USMA
Army Medicine	@ArmyMedicine	#PerformTriad
Soldier 4 Life	@csaSoldier4Life	#SoldierForLife
Army Chaplain Corps	@ArmyChaplains	
The Old Guard	@The_Old_Guard	
ARCIC	@AdaptingTheArmy	#AOC #F2025

Instagram Quick Reference Guide



Organizational:

- **Do** understand your audience's likes, dislikes and what drives them to engage on other accounts.
- **Do** create a running theme or include unit identity in photos/videos.
- **Do** research peak engagement times and post accordingly.
- **Do** tell a story using photographs/videos but be picky in image selection.
- **Do** look for unusual or different ways to illustrate a topic.

Leader:

- **Do** be authentic
- **Do** coordinate with other leaders that have an authentic, established connection with your audience.
- **Do** look for strategies to build engagement and follow-up plans to encourage retainment.
- **Do** interact with audience to create loyal followers.
- **Do** be creative: creativity sparks engagement.
- **Do** create a personal feel in the account.
- **Do** follow other users and engage with other posts, allowing their audience to be exposed to your content.
- **Do** amplify strategies/efforts on established social media platforms.
- **Do** post photos/videos that are relevant to your audience.

All users:

- **Do not** violate endorsement or copyright rules.
- **Do** be timely; do not wait to post photos or videos.
- **Do not** post snapshots or substandard images.
- **Do not** be a one-way channel of information; learn to listen, reply to and invite comments.
- **Do not** overuse hashtags or neglect hashtag research before posting.
- **Do not** post advertisements or PDF documents.
- **Do not** overlook the caption: the photo/video may be the focus but the caption provides context.
- **Do not** over process using filters; photo/video manipulation rules still apply.
- **Do not** create different hashtags for different platforms.
- **Do** provide a "scoop" by posting behind the scene photos/videos.
- **Do** share content about your organization posted by other users.
- **Do** customize your biography, incorporating the required elements for official online accounts.
- **Do** use [link shorteners like Go.USA.Gov](#); remember many government networks block commercial short links.
- **Do** post timely content - remember social media is about the here and now.
- **Do** establish a dialogue with your audience.

Instagram Quick Start Page

Recommended list of accounts to follow:

Account Name	Account	Hashtag
deptofdefense	www.instagram.com/deptofdefense/	#DoD
usarmy	www.instagram.com/usarmy/	
uscg	www.instagram.com/uscg/	#USCG
usnavy	www.instagram.com/usnavy/	
usairforce	www.instagram.com/usairforce/	#AirForce
marines	www.instagram.com/marines/	
us.nationalguard	www.instagram.com/us.nationalguard/	#NationalGuard
patrickmurphypa	www.instagram.com/patrickmurphypa/	
genmarkmilley	www.instagram.com/genmarkmilley/	
commandant.usmilitaryacademy	www.instagram.com/commandant.usmilitaryacademy/	
usarec	www.instagram.com/usarec/	
jbmhh	www.instagram.com/jbmhh/	
walterreedarmyresearch	www.instagram.com/walterreedarmyresearch/	#wrair
ameddhistory	www.instagram.com/ameddhistory/	
future_soldier_center	www.instagram.com/future_soldier_center/	
peoacwa	www.instagram.com/peoacwa/	
westpoint_usma	www.instagram.com/westpoint_usma/	
usamu1956	www.instagram.com/usamu1956/	
armyfifeanddrum	www.instagram.com/armyfifeanddrum/	
fortjacksonpao	www.instagram.com/fortjacksonpao/	#FortJackson
30thmed	www.instagram.com/30thmed/	
strikebct	www.instagram.com/strikebct/	
173rdairbornebrigade	www.instagram.com/173rdairbornebrigade/	
35th_ada	www.instagram.com/35th_ada/	
usarmyoldguard	www.instagram.com/usarmyoldguard/	
53rdibct	www.instagram.com/53rdibct/	
82ndcab	www.instagram.com/82ndcab/	
louisvilleusace	www.instagram.com/louisvilleusace/	
providerpao	www.instagram.com/providerpao/	
94thaamdc	www.instagram.com/94thaamdc/	
armyfifeanddrum	www.instagram.com/armyfifeanddrum/	
usarmyalaska	www.instagram.com/usarmyalaska/	
charlestoncorps	www.instagram.com/charlestoncorps/	
artilleryredlegs	www.instagram.com/artilleryredlegs/	#fieldartillery

Enclosure

EXAMPLE UNIT POLICY ([Download document](#))

U.S. ARMY SOCIAL MEDIA POLICY TEMPLATE

OFFICIAL UNIT PAGES

PURPOSE. To establish U.S. Army policy that provides guiding principles for the effective use of public-facing social networking sites, multi-media sites, blogs and wikis for (UNIT).

APPLICABILITY. This policy applies to unit Commanders, Soldiers and individuals who have administrative rights to post content on (UNIT)'s official social media pages. While Soldiers and individuals affiliated with the U.S. Army are welcome to participate in social media, we expect everyone who participates in the online space to understand and to follow these simple but important guiding principles. These rules might sound strict and contain a bit of legal-sounding jargon but please keep in mind that our overall goal is simple: to participate online in a respectful, relevant way that protects our rapport with the American public and, of course, follows the letter and spirit of established regulations.

GUIDING PRINCIPLES.

- a. **Obtain Approval for Social Media Presence.** Per a 3 Dec 2013 Secretary of the Army memorandum titled "[Delegation of Authority – Approval of External Official Presences](#)", commanders of all Army Commands, Army Service Component Commands and Direct-Reporting Units have the authority to approve the establishment of External Official Presences (EOPS), which includes social media sites.
- b. **Designate Page Administrator(s).** U.S. Army units should designate administrator(s) for official public-facing social media pages. At a minimum, page administrator(s) assume responsibility for maintaining social media pages by means of implementing [branding](#), posting content, monitoring user feedback and responding to users. The frequency of posts and engagement should be determined by page administrators based on (UNIT)'s resources. Administrator(s) also reserve the authority to provide administrative access to other users, if necessary.
- c. **Complete Training.** Soldiers, Commanders and social media page administrators should, at a minimum, have completed OPSEC Level I Training. Other recommended training courses include the [Defense Information Systems Agency course](#), [Information Assurance Training and Certification](#) and [OPSEC Support Staff \(IOSS\) courses 3500 and 1500](#).
- d. **Content Approval.** Release authority is a critical component of maintaining official social media pages. Administrators should establish a method to ensure thorough content review before posting – being mindful of [operations security](#), the [Uniform Code of Military Justice](#), For Official Use Only (FOUO) documents, the [Freedom of Information Act \(FOIA\)](#), etc. Content that should NOT be posted on official pages include, but is not limited to: unit/personnel rosters; information, other than authorized releases, about casualties prior to official confirmation that next of kin have been notified; information regarding events or incidents currently under investigation.
- e. **Enforce Operations Security.** While social media use is touted as a means of being transparent, security is paramount when it comes to sharing information using online platforms. Any information that may compromise operations security, or [OPSEC](#), should not be discussed on social media pages maintained by Army units. Page administrators should monitor pages for any potential OPSEC violations and determine the best course of action (screen capture and delete content; report violations to (UNIT)'s chain of command; educate social media users on what constitutes appropriate post, etc.)
- f. **Comply with Established Regulations and Policy.** To the extent that resources are available, ensure social media use complies with applicable mandates, such as [Section 508 of the Rehabilitation Act of 1973](#), [Department of Defense Instruction 8550.01](#), [U.S. Army Standard Operating Procedure](#), [U.S. Army Delegation of Authority](#), [Responsible Use of Internet-Based Capabilities](#), the [Hatch Act](#) and [Records Management](#).
- g. **Moderate Pages.** All discussion boards and comments should be closely monitored by page administrators, but there should be a balance as not to over moderate pages and online exchanges between users. Allow users connected to your pages to fight your battles for you, as well, when possible. They are, by virtue of their nature, not the official (UNIT) responders and, as such, carry with them a different level of credibility.
- h. **Address Negative Comments.** Do not stray from negative comments. An open forum comes with certain risk of negativity and to shy from it will potentially tarnish credibility. However, responses must be vetted / approved and accurately express the U.S. Army's position without editorializing or straying from the facts. Only delete or block comments or users when a clear pattern of malicious,

Enclosure Cont'd

EXAMPLE UNIT POLICY (Download document)

derogatory behavior is apparent and they are in violation of the terms of participation. Keep a log of all malicious material which has been deleted.

- i. **Be Mindful of Copyright, Trademarks, Litigation & Personal Information.** Social media posts and content must respect copyright, privacy, fair use, financial disclosure, and other applicable laws. Always give people proper credit for other's work and make sure you have the right to use something with attribution before you publish it online. Do not publish or report on conversations that are meant to be pre-decisional or internal to the U.S. Army unless given permission by your chain of command. As a standard practice, avoid commenting on anything related to legal matters, litigation, or any parties the U.S. Army may be in litigation with. Lastly, always protect sensitive information, such as protected acquisition and personally identifiable information.
- j. **Register Official Pages.** All official U.S. Army social media pages should be registered by submitting links and contact information via the U.S. Army Social Media Directory located at <http://www.army.mil/socialmedia>. The U.S. Army's Online and Social Media Division (OSMD) will manually review each submission and publish the sites that adhere to the established guidelines posted on the Social Media Directory webpage (http://usarmy.vo.llnwd.net/e2/rv5_downloads/socialmedia/Registration_Checklist.pdf). If OSMD has any issues or questions with link submissions, they will contact the individual who submitted the link(s).

(UNIT) Social Media Policy

TERMS OF PARTICIPATION.

Welcome, this is the official U.S. Army (Facebook, Twitter, YouTube, Vimeo, Flickr, Blog, etc.) for (UNIT) where you will find the most recent information and news about (UNIT). It is our goal to provide the public with information and news about (UNIT) and allow for an open forum of discussion about (UNIT) topics.

If you are looking for our official web page please visit (OFFICIAL UNIT .MIL) or <http://www.army.mil>.

Please feel free to express your opinion about the U.S. Army in an objective and respectful way that allows for a continued information relationship.

Participants are asked to follow the posting guidelines below.

(UNIT) reserves the right to remove any posts in violation of the posting guidelines.

POSTING GUIDELINES.

Posts will be removed if they violate the guidelines listed below:

- No graphic, obscene, explicit or racial comments or submissions nor do we allow comments that are abusive, hateful or intended to defame anyone or any organization.
- No solicitations or advertisements. This includes promotion or endorsement of any financial, commercial or non-governmental agency. Similarly, we do not allow attempts to defame or defraud any financial, commercial or non-governmental agency.
- No copyrighted or trademarked images or graphics. Imagery posted on the Facebook wall should be owned by the user.
- No comments or photos that suggest or encourage illegal activity.
- No documents of any kind should be posted on this page.
- You participate at your own risk, taking personal responsibility for your comments, your username and any information provided.

Also, the appearance of external links on this site does not constitute official endorsement on behalf of the U.S. Army or Department of Defense.

For more information, visit the Department of Defense Social Media user agreement at: <http://www.defense.gov/socialmedia/user-agreement.aspx>



Online and Social Media Division
Office of the Chief of Public Affairs
1500 Pentagon, Washington, DC

USARMY.PENTAGON.HQDA-OCPA.MBX.OSMD-INQUIRY@MAIL.MIL