146TH AIRLIFT WING

2021 SOCIAL MEDIA POLICY

146th AIRLIFT WING

A GUIDE TO ASSIST AIRMEN UTILIZING SOCIAL MEDIA

PROTECT YOURSELF ONLINE

GUIDANCE FOR ALL AIRMEN

When it comes to the rapidly ever-changing world of social media, Airmen must be vigilant regarding online safety and personal conduct when using social media. Now more than ever, Airmen using social media platforms must consider much more than account security and understand the ramifications of their online conduct.

The Air Force positively views personal social media sites and respects your rights as Americans to use them to express yourself. However, by the nature of your profession, you are always on the record and must represent the Air Force's core values.

This social media guide intends to help Airmen and employees from the 146th Airlift Wing protect themselves as they engage others via social media. Airmen must avoid anything that will discredit themselves or the Air Force and always use their best judgment. Inappropriate online conduct unbecoming of a United States service member, regardless of the medium used, can have serious consequences.

Within this guide, the 146th Airlift Wing's Public Affairs office has developed helpful tools and checklists to empower Airmen and assist with decision-making by clarifying Air Force policies. There is also a practical guide to help Airmen identify false information they encounter online. Also located within this guide is information to consider on how a post can be interpreted by the public. Learn to discern the difference between funny and distasteful content, and ultimately protect Airmen by assisting them in exercising their best judgment when in doubt if they should post something.

If you take nothing else away from this guide, remember this; you are an Airman 24 hours a day, 365 days a year. This includes the Air National Guard - which means you are always on duty, and your social media interactions can be subject to the Uniform Code of Military Justice. But, ultimately, you alone are responsible for what you post.

Suppose you have reviewed this guide in its entirety and still have questions about social media best practices. In that case, I invite you to visit our office any time or contact our work center to discuss. We are here to serve and protect our most valuable resource - our Airmen.

NICHOLAS C. G. CARZIS, MSgt. CA ANG
Superintendent Public Affairs
146th Airlift Wing

Additional resources for information found in this guide can be found on the Air Force Portal
E-pubs and at our office located inside the Wing Headquarters building 100 room 176.
Visit our website at https://www.146aw.ang.af.mil
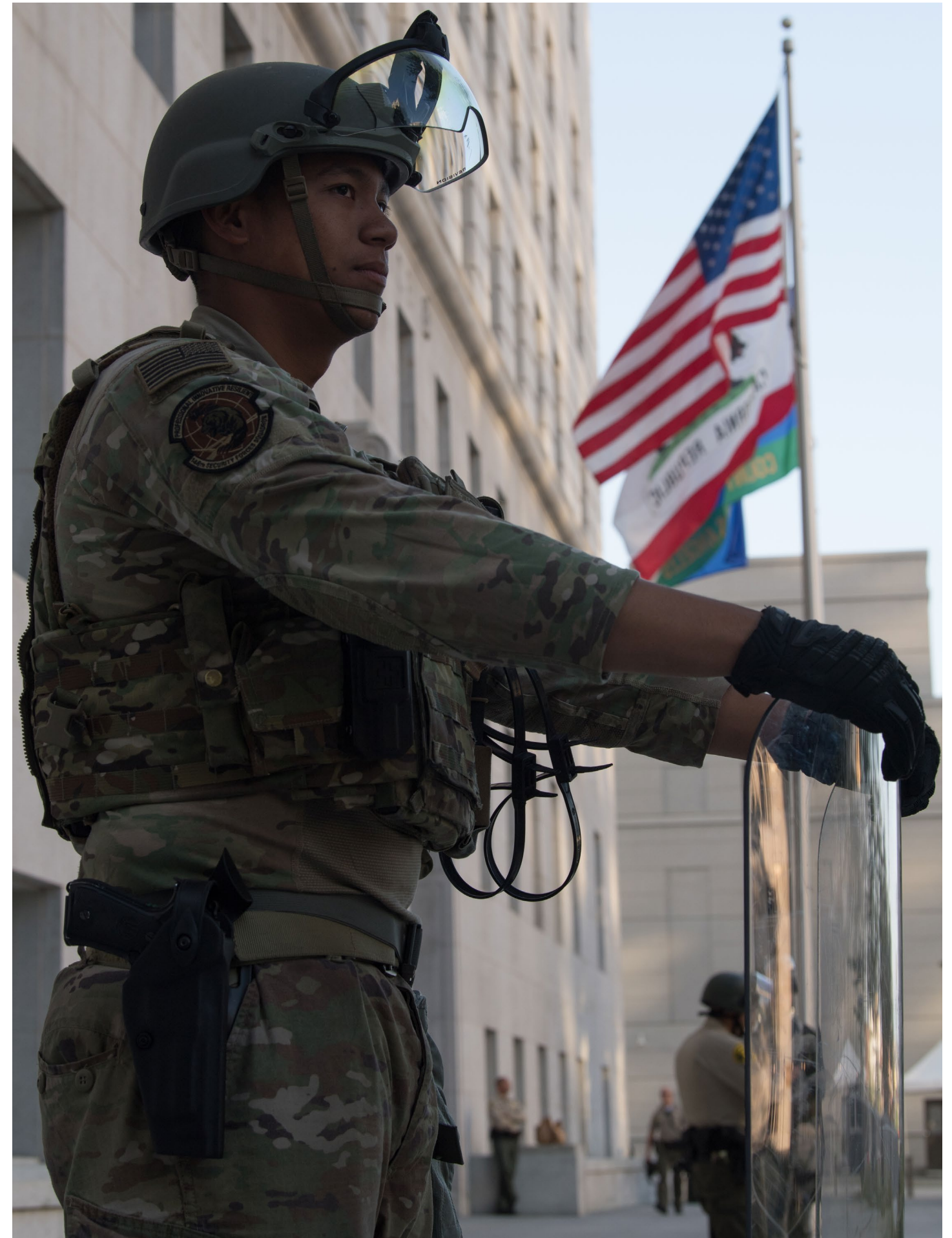
SETTING THE STANDARD

HOW SUPERVISORS CAN ASSIST AIRMEN WITH THEIR ONLINE CONDUCT

As a leader of Airmen, you are charged with always ensuring that you are demonstrating your best judgment and leading by example. Your online conduct is no exception.

Some supervisors may feel challenged when it comes to social media, whether because they don't use it themselves or don't understand the impact. However, today's Air Force supervisors face a new era of Airmen communicating almost exclusively on social media.

As a supervisor, you can help enforce and set the standard for online conduct within your organization. Here are some critical first steps to ensure your Airmen are successful regarding their online behavior.

WHERE TO START

TALK TO YOUR AIRMEN
As simple as it sounds, sometimes hearing information from the right source has a better chance of being communicated and received. Make a concerted effort to express the importance of appropriate online behavior with your Airmen.

ASK FOR HELP
Did you know your Public Affairs office has the ability to provide social media training for your squadron? It's true! You can leverage multiple dynamic speakers and presentations to help edify your concerns and message across to your Airmen by asking PA!

REPORT VIOLATIONS OF POLICY
If evidence of a violation of policy, Uniform Code of Military Justice (UCMJ), or civil law by one of your Airmen comes to your attention from social media, you should report it to your chain of command. Enforcing Air Force policy applies to online as well.

EMPHASIZE OPSEC OFTEN
Review OPSEC training and critical information lists with your Airmen, explain the impact and importance of protecting information, then ask them to ensure that their families and loved ones understand the concept of OPSEC to protect their families.

These four steps can dramatically increase efforts to ensure your Airmen are better protected and help preserve our Air Force culture. Supervisors should remember the key is to maintain the same relationship with them online as you do at work. Being clear about online conduct with them initially and providing as much information and training regarding online conduct will help support Airmen and answer their questions and concerns. This will edify your leadership's goals and keep them protected.

• • •

POLICY

YOUR ORGANIZATIONS POLICIES

The Public Affairs office is the primary office of responsibility regarding guidance and wing policy changes regarding social media and its use by Airmen within our organization. Therefore, the policies outlined within this guide are taken directly from the policy letter from the 146th Public Affairs office and Air Force Instruction 1-1.

We want our Airmen to understand the power of social media and its leverage in connecting others to the importance of our missions and its risks as a choice communication tool. There can be no misconception between where your responsibilities end as an Airman and your personal life begin. There is no discerning between your personal and military life. YOU ARE AN AIRMAN 24 hours a day.

Service members and employees must understand that they may be held accountable for their online activity if they violate any standards outlined within the policy. Compliance with the criteria discussed in this policy does not vary. It is not otherwise dependent on the method of communication used. The following Air Force standards must always be observed on and off duty regardless of the process of transmission.

• • • • •

FREEDOM OF EXPRESSION:

DO NOT: Post offensive and/or inappropriate online behavior that could discredit the military or you as a member. Use contemptuous words against elected officials, including the President, the Vice President, Congress, the Secretary of Defense, the Secretary of a military department, the Secretary of Homeland Security, or the Governor or legislature of any State/Commonwealth, in an official capacity.

DO: Use disclaimers that clearly define that the views you express are yours alone and do not reflect the views of the Air Force or our organization. (If it can be derived that you are a military member and a part of our organization, then you should use this practice). EXAMPLE: "The postings on this site are my own and don't necessarily represent Air Force positions, strategies, or opinions." Here's the bottom line: USE COMMON SENSE! If you don't want to read about it, see it in the news, or be asked about it by people you respect — don't say it, don't do it, don't post it. Don't go viral for the wrong reasons.

HARMFUL OR OFFENSIVE CONDUCT:

DO NOT: Post content in violation of federal or state laws, Air Force regulations and policies through inappropriate personal online activity, or any other form of communication. This includes posting defamatory, libelous, obscene, threatening, racially or ethnically hateful or otherwise offensive/illegal information or material. Online bullying, hazing, harassment, stalking, discrimination, retaliation or any other type of behavior that undermines dignity and respect.

DO: Report experiences of witnessing incidents of improper behavior. Reports can be made to your chain of command. Additional avenues you can report incidents or content that contains obscene, threatening, hateful, harassing, stalking, or discrimination include Equal Employment Opportunity offices, the Inspector General, Sexual Assault Prevention and Response offices, and the Office of Air Force Special Investigations.

OPSEC:

DO NOT: Post Classified, FOUO, CUI, or other official DoD information and documents on social media or any other non-DoD e-mail accounts. Don't post details about your unit's mission or security procedures, or announce locations and times of deployments.

DO: Closely review content before posting to ensure sensitive or personal information is not accidently released (e.g. troop locations, equipment, tactical unit details, and numbers of personnel. Familiarize yourself with OPSEC training and avoid posting content containing OPSEC hazzards in them.

PERSONAL SOCIAL MEDIA ACCOUNTS:

DO NOT: use your Air Force affiliation, official title, or position to promote, endorse or benefit any profit-making group or agency, or non-profit groups based solely on religious or political affiliations, IAW DODD 5500.07, and AFI 1-1, Air Force Standards, this includes appearing in, or preparing statements for inclusion in, advertisements designed for use by electronic or print media. Don't promote yourself for personal or financial gain.

DO: Differentiate between opinion and official information. Stay in your lane when talking about the Air Force or the DoD. Discussion of issues related to your career field or personal experiences are acceptable and encouraged, but you shouldn't discuss areas of expertise where you have no firsthand, direct experience or knowledge.

• • • • •

PERSONAL GAIN SINCERELY HELD BELIEFS:

DO NOT: Use the Air Force name or your title to endorse or promote products, political positions or religious ideologies.

DO: Clarify all individual expressions of sincerely held beliefs (conscience, moral principles, or religious beliefs) as your own.

POLICITAL ACTIVITY:

DO NOT: Solicit votes for or against a party, candidate or cause in an official capacity. Do not participate in any interview or discussion as an advocate for or against a party, candidate or cause this includes attendance in uniform at a rally (members may, however, express their personal opinions on political candidates and issues, make monetary contributions to a political campaign or organization and attend political events, in their personal capacity as a spectator when not in uniform. Commissioned officers may not make contemptuous words against the President, Vice President, Secretary of Defense, Deputy Secretary of Defense, Secretary of DAF or governor and legislature of any state in which he or she is located, or performing duty in. Don't express or imply Air Force endorsement of any opinions, products or causes.

DO: Express your political views on public issues/political candidates online outside of organized communication campaigns. Clearly present your views as your own and review participation guides found in AFI 51-508, Political Activities, Free Speech and Freedom of Assembly of Air Force Personnel.

DID YOU KNOW ABOUT THE HATCH ACT? : Rules governing political activities by government civilians are found in a federal law known as the Hatch Act. DOD civilians who violate the Hatch Act face adverse personnel actions, including suspensions and employment termination. See Hatch Act Guidance on Social Media, US Office of Special Counsel, February 2018.

You can find a copy of the wing's social media policy on our official app under resources or on the Public Affairs webpage by visiting our website at https://www.146aw.ang.af.mil under the resources tab. Additionally, you can always visit the Public Affairs work center to speak to one of our representatives or ask your local CSS for a copy of the newest policy letter.

● ● ● ● ●
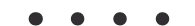
POLITICS & SOCIAL MEDIA CONTINUED:

You may generally express your personal views on public issues or political candidates via personal accounts on social media platforms, such as Facebook, Twitter, or personal blogs.

However, suppose personnel can be identified by a social media site as a DOD employee when expressing a personal opinion?

In that case, the posting must clearly and prominently state that the views expressed are those of the individual only and not of the Department of Defense.

While Airmen and DoD civilians may "follow," "friend," or "like" a political party or candidate running for partisan office, they should avoid posting links to "share" or "re-tweet" comments or tweets from the Facebook page or Twitter account of a political party or candidate running for partisan office. Such activity could be deemed as participation in political activities.

For more social media guidance for military members on social media and political activities, please review the Hatch Act.

UCMJ POLICY REVIEW

Improper or inappropriate online behavior by Airmen and DoD civilians shouldn't be tolerated. It should be reported if experienced or observed.

Airmen and Guardians using social media are subject to the UCMJ and Department of the Air Force regulations at all times, even when off duty. Commenting, posting, or linking to material that violates the UCMJ or Department of the Air Force regulations may result in administrative or disciplinary action, including administrative separation, and may subject D.A.F. civilians to appropriate disciplinary action.

Punitive action may include Articles 88, 89, 91, 92, 120b, 120c, 133, or 134 (General Article provisions for contempt, disrespect, insubordination, indecent language, communicating a threat, a solicitation to commit another offense, and pornography offenses), as well as other articles. Additionally, refer to AFI 1-1, Air Force Standards, Chapter 2 for information on how Airmen and Guardians should conduct themselves in the digital environment.

Applicable UCMJ and federal criminal law violations include Failure to obey order or regulation; Article 117. Provoking speeches or gestures; Article 134. General Article 18 U.S.C. § 2385. Advocating the overthrow of the Government.

ONLINE PROFILE PROTECTION

With whatever social media presence you have, a good standing practice is to limit the information you and your families post publicly. This includes addresses, birthdates, birthplaces, local towns, schools, etc. Small details can be aggregated over time to reveal significant information that could threaten you or your family. When posting, ask yourself what a person could do with this information? Could it compromise my safety or the safety of my family or my unit?

UPDATES

Keep your technology up to date (computer, phone, tablet, etc.). Whenever you get a software update at work or at home, run it. These are typically patches for recent security vulnerabilities.

TRACKING

Beware of tracking your location. Many social media platforms allow for "check in" and share your location, or automatically add location information to photos and posts.

PUBLIC WIFI

Avoid using public WiFi. With a public internet connection, you run the risk of being hacked. If you must use a public Wi-Fi connection, don't shop or go to your bank accounts on public Wi-Fi. Only go to sites that use a secure connection (indicated by an "HTTPS" in their web address). This means they use encryption to protect your information. Use a Virtual Public Network (VPN). This — often paid-for — service provides a more secure connection. If available, use two-factor authentication. Anyone trying to pretend to be you won't be able to access your accounts because they won't have your phone or computer.

LOOK OUT FOR BAD GUYS

Do not click links or open attachments unless the source can be trusted. Cyber criminals pretend to be people they are not in order to deceive you into performing actions that launch cyber-attacks, download viruses and install malware and spyware onto government or personal computers. Look for "HTTPS" on the web site address and the "lock" icon on the web page that indicate active security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

PRIVACY AND ACCOUNT SETTINGS

"Friends" and "followers" are considered relationships that can affect your security clearance, so make sure you only make connections with people you know well.
Sort "friends" into groups and networks, and set access permissions accordingly. Add "untrusted" people with the lowest permissions and accesses.

Verify, through other channels, that a "friend" request was actually from your friend. Beware of apps or plug-ins, which are often written by unknown third parties who might use them to access your data and friends. Applications may share your personal information with other users on Facebook AND external to Facebook. Check the settings of EACH application you use before "allowing access." Make sure only your family and friends (people you know WELL) can see your photos, full name, and other information. Assume that all the information you share will be made public (meaning, someone can find it on Google).

Don't accept default account privacy settings. Carefully look for and set all your privacy and security options – in all your online accounts (not just Facebook).

146 AW

ONLINE LITERACY: DEEP FAKES & FAKE NEWS

WHAT IS FAKE NEWS?

Fake news is fabricated information, which mimics news media content in form, but not in organizational processes or intent.

It overlaps with other information disorders, such as misinformation (false or misleading information) and disinformation (false information that is purposely spread to deceive people).

In order to be media literate, you need to be aware of other questionable sources of information.

DEEPFAKES

Deepfakes use software to create events that never happened or distort a person's statements. Satire uses humor, irony, exaggeration, ridicule, satire, and false information to comment on current events.

METHODS OF MISINFORMATION

State-sponsored news is often the source of propaganda in repressive states operating under government sanctions. Junk science promotes discredited conspiracy theories, naturalistic fallacies, and scientifically false or dubious claims. Click bait provides generally credible content, but uses exaggerated, misleading, or questionable headlines, social media descriptions, and/or images.

UNDERSTANDING THE INTENT

There is no shortage of information, and accuracy can be hard to gauge. Misinformation is unintentionally inaccurate. Disinformation is intentionally inaccurate. Critical thinking skills are the best defense against mis/disinformation. It is important for Airmen to be critical consumers of information, to not fall for disinformation campaigns, to recognize when misinformation may be present, and to not contribute to the spread of either.

BE CURIOUS

Independently verify the source and the information. Is more than one source reporting the same thing, or is this the only place you have seen the information?

BE REFLECTIVE

Pause, reflect, and investigate — especially if you immediately have an emotional reaction, which is the primary goal of fake news producers.

INVESTIGATE YOUR NEWS SOURCES

Select news sources known for high-quality, investigative reporting. Search for these sources directly. Social media algorithms present information that reinforces your current views, not a balanced view.

LOOK FOR IN-DEPTH COVERAGE

Look for lengthy articles — long-form reporting — that capture some of the complexity of topics and events. One or two paragraphs is not sufficient.

USE CARE BEFORE SHARING NEWS CONTENT ON SOCIAL MEDIA.

Pause and reflect on news sources that arouse strong emotions, positive or negative.

REPORTING IMPOSTER ACCOUNTS

The best way to combat the issue is to help ensure you know where to find authentic and credible information from .mil and social media sources.

The Department of the Air Force Office of Special Investigation highlights the threats posed by cyber-cybercriminals who impersonate Department of the Air Force personnel online.

AFOSI offers mitigation techniques and address law enforcement's limited ability to investigate these incidents and remove fraudulent accounts. You can also refer to OSI Cybersecurity: Identifying and Reporting Impostor Accounts.

DEEPFAKES AND DECEPTION
A STATEMENT FROM ASSISTANT DIRECTOR FBI, CYBER DIVISION

"We are seeing advances in artificial intelligence and machine learning that are improving the speed, believability, scale, and automation of the creation and dissemination of deepfakes and other synthetic content to produce high-quality videos, pictures, audio, and text of events which never happened. Although deepfake videos are currently difficult to create and require resources and sophistication, they are becoming increasingly more accessible. Cybercriminals can create highly personalized content for targeted social engineering, spear phishing, business e-mail compromises, other fraud schemes, and to victimize vulnerable individuals, and nation-states could use these techniques for malign foreign influence and to spread disinformation and misinformation," - Bryan A. Vorndran. *(Statement Before the House Judiciary Committee, Washington, D.C. - March 29, 2022)*

You may have been exposed to hundreds of pieces of news content online today before reading this. Do you ever wonder how many of them were factual pieces of information? In today's social media news cycle, information comes much faster than before. Most of the time first reports are riddled with misinformation as even recognized news outlets scramble to be the first to break big stories.

It's up to you to decide which stories and news informational pieces are worth your text, tweet, or share. If you are truly interested in sorting fact from fiction, then you are going to need to do some research. Begin to answer these questions: Is the content well-made? Does this information seem editorilized? (News vs opinion). Does it entertain me or raise awareness? Is it biased? Is that bias open or sneaky? Is it supported by facts? Finally, ask yourself, is this story share-worthy?

• • • • •

HOW TO SPOT FAKE NEWS

CONSIDER THE SOURCE
Click away from the story to investigate the site, its mission and its contact info.

CHECK THE AUTHOR
Do a quick search on the author. Are they credible? Are they real?

CHECK THE DATE
Reposting old news stories doesn't mean they're relevant to current events.

CHECK YOUR BIASES
Consider if your own beliefs could affect your judgement.

READ BEYOND
Headlines can be outrageous in an effort to get clicks. What's the whole story?

SUPPORTING SOURCES?
Click on those links. Determine if the info given actually supports the story.

IS IT A JOKE?
If it is too outlandish, it might be satire. Research the site and author to be sure.

ASK THE EXPERTS
Consider asking a Librarian or consult a fact-checking site.
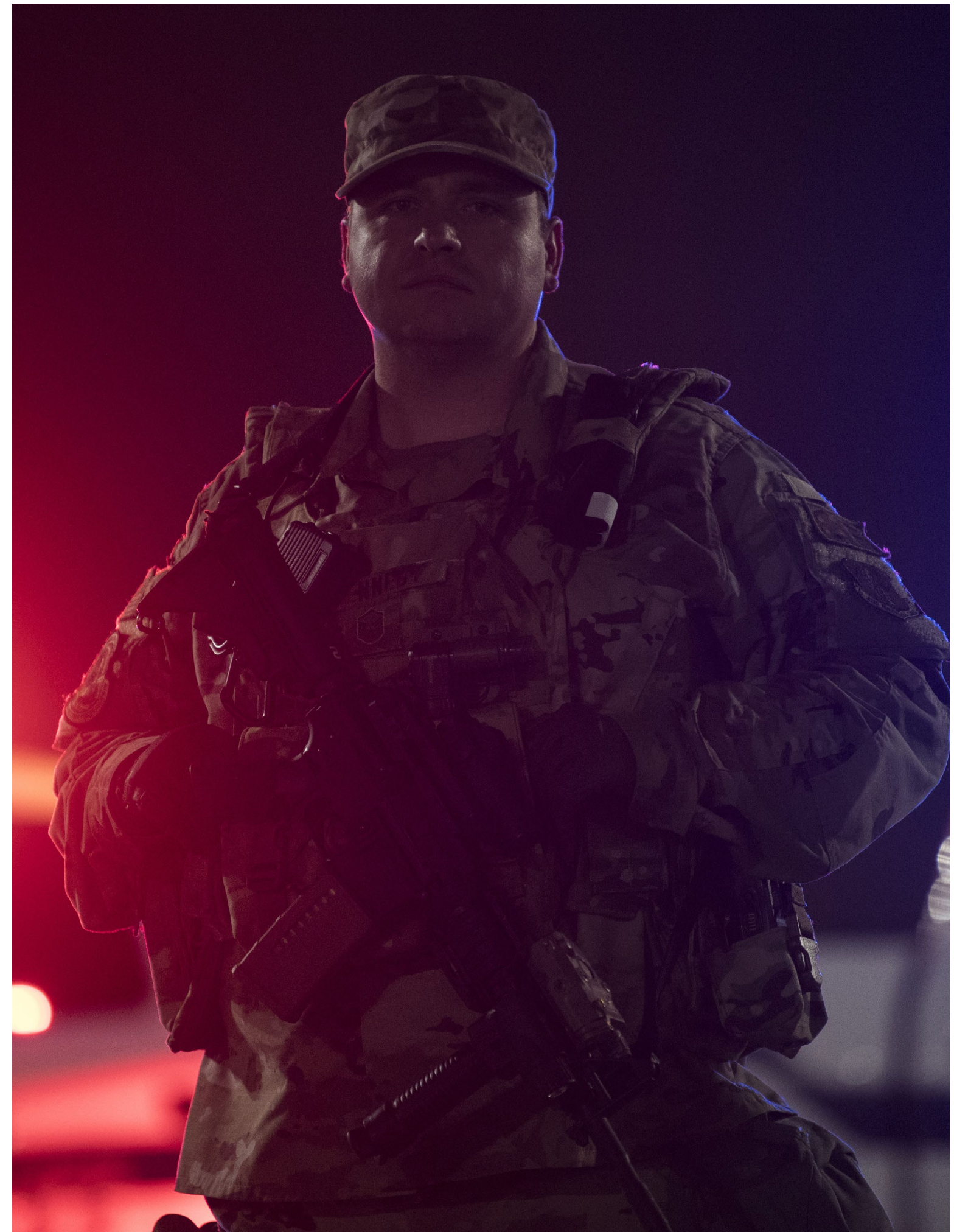
PROTECTING YOUR FAMILY

Your families are integral to the success of the Air National Guard. Without their support, Airmen wouldn't be able to accomplish the great work they do daily. Additionally, the Air National Guard stories you and your family share on social media help maintain Airmen's morale and educate the public about the Air National Guard.

Airmen and their families must identify and safeguard critical information about military operations. Be cautious about sharing personal information or communicating with people over social media. Posting too much information could jeopardize the security of your fellow Airmen and missions. A simple rule is this: If you wouldn't want to see the information on the news, do not post it on the internet.

Think about this: social content shared by Airmen and families is a target for those looking to gain access to sensitive information to impersonate, blackmail, or intimidate. So don't post the exact whereabouts and activities of deployed Airmen.

Additionally, don't publicly post precisely how long you or your family will be gone on a trip or deployment. Finally, don't make your vacation dates public on social networks. Criminals may track your activities and know exactly when to break into your home while on vacation.

Be careful about publicly posting your children's photos, names, schools, ages, and schedules.

Your families are encouraged to use social media to engage in support networks, such as spouse's clubs, event committees, child care groups, or local civic activities. These groups are not considered official Air Force social media, and you don't need permission to form a group of your own. However, you may want to limit the membership and visibility of the group to help protect the information exchanged. (NOTE: Do not create official squadron pages or groups online; they are not allowed. All official military pages, web pages, and social media sites must be registered with SAF/PA per AFI 35-101).

Even if the membership and visibility are limited, never discuss sensitive information online. Instead, tell your family to follow the main 146th Airlift Wing social media accounts for the latest news. Let them know they can support your specific missions by sharing their social media content and experiences with your followers and friends.

• • •

FINAL CONSIDERATIONS

What happens online stays online and can have real-world impacts in the moment and years after. When you're online, you're in public — so act like it. Don't do or say anything online you wouldn't do or display in public. Keep relationships and personal life private.

Treat everyone online how you'd like to be treated. The "Golden Rule" applies even online. There's no such thing as complete anonymity online. "No one will figure out who I am." Wrong. The people you know will recognize you. Likewise, Google, Amazon, and other online services designed to capture your online habits to optimize your experience may identify you.

Before you hit send, stop and think. The things you say matter. Images can be taken out of context. Cool off before responding to messages in anger. You'll never agree with everyone online. Respect others' opinions. Anyone anywhere could see what you post. The internet doesn't forget. It's effortless for bad actors to save a screenshot, download an image, or do something else to ensure a moment online lasts an eternity.

Anything shared online, although intended to be private and confidential, can become public. If it's best left unsaid, don't say it. If you don't want it shared, don't post it.

Protect your and your friend's privacy by not sharing without their permission. Unless you're prepared to attach that post, text, or photo to your next college application, security clearance package, or resume, stop and think before you post.

Anything posted on the internet is permanent. Through the use of publicly Available online tools, data can be recovered and used against you. Personal, nonofficial accounts may not be used to conduct official DoD Communications for personal convenience or preferences.
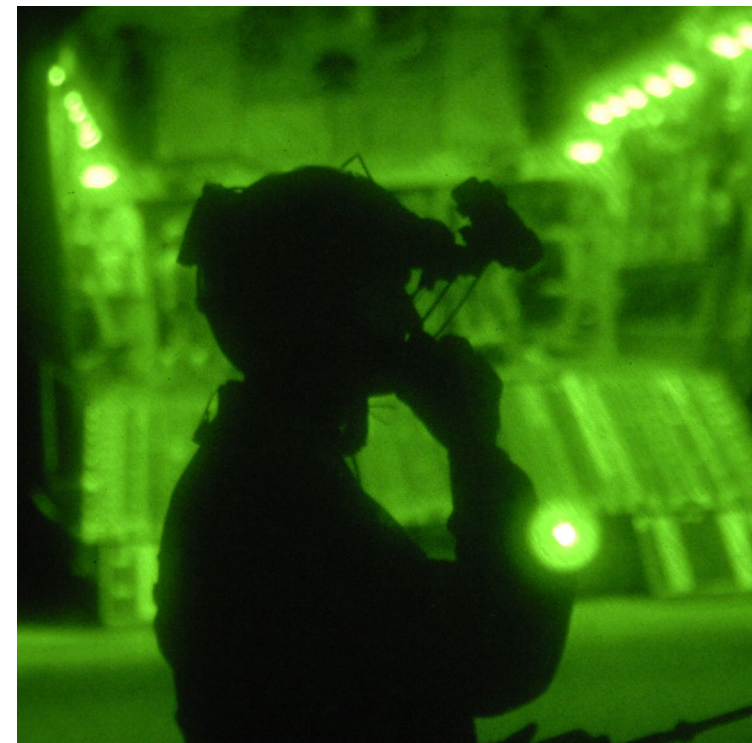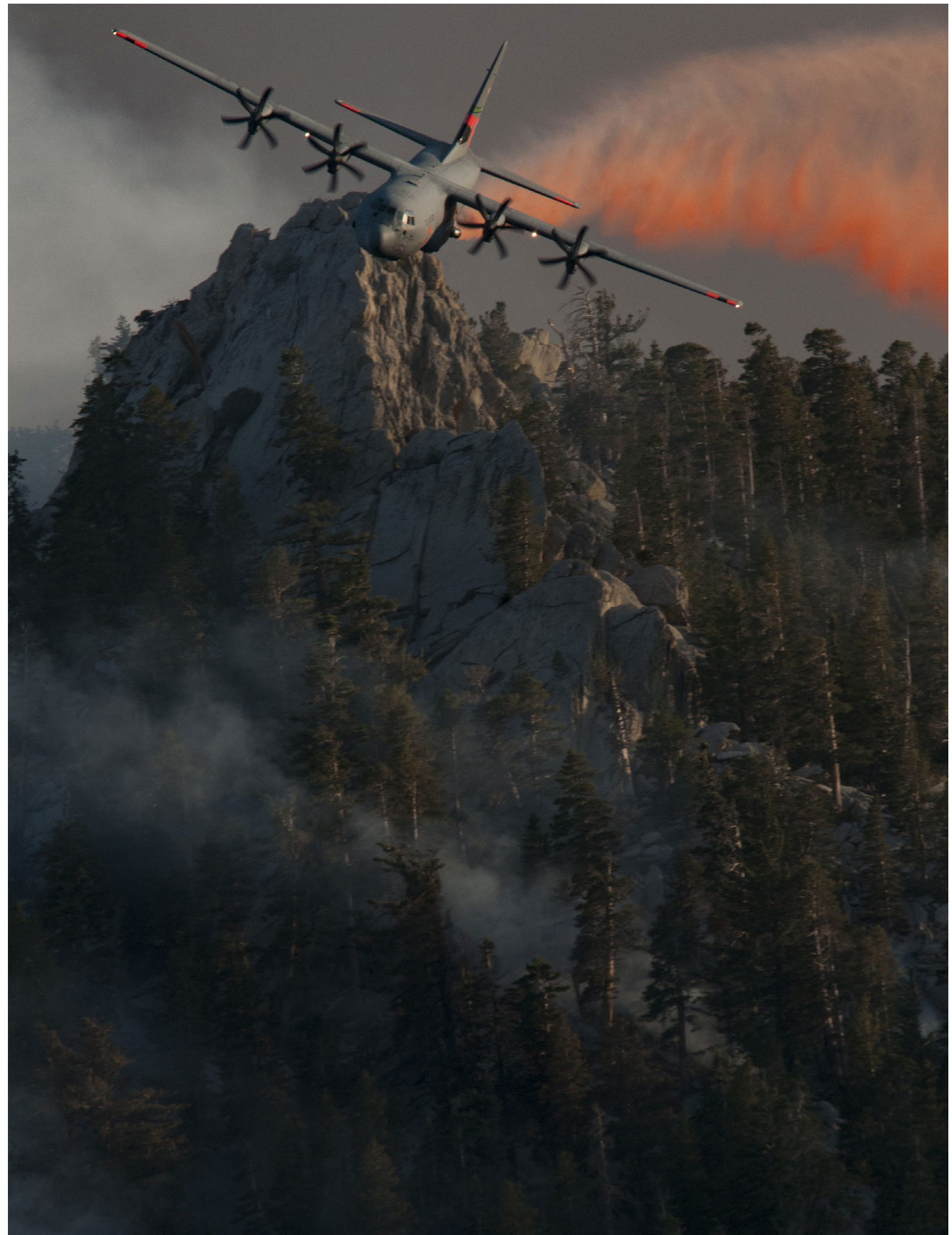
HOLLYWOOD GUARD
PH⊕TO
TACTICAL DIGITAL MEDIA

https://www.146aw.ang.af.mil/Resources/Public-Affairs/
Twitter @146airliftwing
Instagram @HollywoodGuard
Facebook 146th Airlift Wing

• • •