JOINT BASE LANGLEY-EUSTIS OPSEC NEWSLETTER

Good Social Media Practices

Don't give criminals a chance to get your information. Be careful of the personal details, photos and videos you post to your profile on social networks. It's highly recommended that you set privacy settings so that only "friends" can see specifics. Even after establishing privacy settings, don't assume your information will remain private; there's no guarantee. Always use common sense: For example, don't inform potential criminals you're going out of town!

It's a good idea to always operate under the assumption that anything you post online might be stolen by an adversary. Social content shared by JBLE personnel and families is a major target for those looking to impersonate them to gain access to sensitive information, blackmail or intimidate. While there is a definite benefit to using social media to help with support networks, be wary of posting detailed information about support groups. Posting unclassified sensitive information could be just as dangerous as posting classified information.

Operations Security

The primary concern for JBLE personnel using social media is maintaining operations security. Information moves and evolves quickly via social media, which means OPSEC awareness is more important than ever before. Make sure you understand the risks and communicate them to other JBLE personnel. Information about social media awareness is provided in annual computer-based training.

Review all content (photos, videos, links to articles, etc.) for OPSEC violations prior to posting. Remember to take a holistic approach when evaluating whether or not your content violates OPSEC. Don't provide adversaries any advantage by posting classified, controlled unclassified information or sensitive information (for example, troop movements, force size, weapons details, etc.). When compiled, such details can reveal more than intended.

Countermeasures:

- Do not post personally identifiable information.
- Do not allow others to tag you in images they post. Doing so makes you easier to locate and accurately construct your network of friends, relatives and associates.
- Be cautious about the images you post. What is in them may be more revealing than who is in them. Images posted over time may form a complete mosaic of you and your family.
- Do not post your specific location.
- Be cautious when accessing online accounts from public Wi-Fi connections. Someone might have installed software capable of capturing your login credentials and other sensitive information.
- Securely configure your social networking accounts to minimize who can see your information.
- Do not accept friend/follower requests from anyone you do not know; independently verify identities.
- Avoid using third-party applications; if needed, do not allow them to access your social networking accounts, friends list or address books.
- Do not use "check-in". If check-in is enabled, disable it.
- Do not arrange meetings with people you meet online.

Further information related to protective measures while using social media can be found on the 633 ABW OPSEC SharePoint site:

https://langley.eim.acc.af.mil/org/633abw/IG/OPSEC/default.aspx

DET 201 AFOSI/US ARMY CID 3 MP GROUP CORNER

The Air Force Office of Special Investigations along with Army CID 3 MP Group continues to monitor the current threat stream with regard to the Islamic State and recent threats made to DoD members utilizing research from social media websites. In response to queries about information that can be provided to families, I'd like to pass along the information attached and also listed below. All of this information can be shared publicly, and I would encourage wide dissemination to your units. AFOSI Det 201/Army CID 3 MP Group stands ready to provide tailored briefings to individual units upon request, and we will certainly provide updates on the threat via established channels as they are received.

Please do not hesitate to contact AFOSI at 757-764-7971 (main number) or Army CID 3 MP Group at 757-878-4811 or contact us direct at any of the below numbers with any questions or concerns.

Thank you and be safe,

Very Respectfully,

Special Agent Bret Irwin
Commander, AFOSI Det 201
Desk: 757-225-4600
Cell: 757-268-1223

Special Agent Vanessa Neff
Army CID 3 MP Group
Desk: 757-878-4811
Cell: 989-277-8793

SA Irwin's Talking Points for JBLE Personnel and Families

1) Recognize that the social media environment has changed permanently

2) Groups such as the Islamic State will use the information you post to spread fear and alarm, and possibly to plan attacks -- DON'T MAKE IT EASY FOR THEM

3) The best manner in which to protect yourself from becoming a future target is to have a low social media profile

4) Best case scenario: When someone conducts an internet search for your name, the results do not show a military affiliation

5) This is not hiding your service affiliation, but protecting yourself and your families -- only share with verified people

6) Information is power -- don't empower people you don't know by broadcasting details about your life, your family, and your service affiliation

See link for additional information:

http://airforcelive.dodlive.mil/2014/10/securing-your-digital-footprint/

See link and below for information from the Federal Bureau of Investigations:

http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks

See link and below for information from the Computer Crime Investigation Unit US Army Criminal Investigation Command Cyber Crime Prevention Flyer.

http://www.jble.af.mil/shared/media/document/AFD-141217-019.pdf

AIR COMBAT COMMAND
COMMAND INTEREST ITEM

DIGITAL SECURITY

AIR COMBAT COMMAND IS THE PRIMARY FORCE PROVIDER OF COMBAT AIRPOWER TO AMERICA'S WARFIGHTING COMMANDS

COMMUNICATING WITH AIRMEN ABOUT DIGITAL SECURITY

REMEMBER

Social media is a powerful communication tool in both our personal and professional lives. Airmen have a special obligation to carefully consider the image and information they portray and to ensure both operational and personal security.

INFORMATION SHARING

Be cautious with sharing. Maintain privacy settings on your social media accounts, change your passwords regurarly and don't give out personally identifiable information.

GEOTAGGING

Airmen should be cautious when enabling the geotagging feature on mobile, location based apps. This feature can potentially create significant personal and operational security risks.

CORRESPONDENCE

Airmen are responsible for their correspondence. Photos, videos, and text posted online must comply with federal law, DoD Directives and Instructions, and Air Force Instructions.

KEY MESSAGES FOR COMMANDERS ABOUT DIGITAL SECURITY

- News reports have focused on ISIL using social media as a means to identify and threaten service members and their families. Recently, a few individuals were singled out after posting information about current operations on their personal pages. While terrorists exploiting social media is not new, it is important to pause and examine our practices to ensure we understand the risk.
- The very nature of our service means that military members face a special risk. But as with everything we do, it's critical to weigh circumstances carefully and responsibly. That means not only considering the OPSEC implications of your communication, but the personal ones as well.
- Be cautious about sharing too much information. Posting detailed information could jeopardize the security of Airmen and missions. Don't post your or others' exact whereabouts and activities and be careful about publicly posting too much data about family members as well.
- Social media use must comply with AFI 1-1, Air Force Culture, which outlines standards, obligations, and responsibilities. Airmen are responsible for what they say and post on social networking services and any other medium, so their posts must comply with Air Force standards.
- Engagement is ultimately an individual decision. Educate yourself about the facts, take recurring security training seriously, review recommendations about steps to safeguard your social media accounts. Airmen can engage, but should make informed decisions. Reach out to your supervisor and/or public affairs office if you have questions.

FREQUENTLY ASKED QUESTIONS REGARDING DIGITAL SECURITY

Q. Should I stop using social media? Can I order my subordinates to stop using it?
A. The very nature of our service means that military members face a special risk. But it's critical to responsibily and carefully weigh the circumstances. Recent cases of individuals being singled out on social media involved service members who were posting military information about current operations on their personal pages. Social media engagement is an individual decision; there is no blanket prohibition against it. Concerned leaders should talk to their legal office about options, but remember informed decisions require education about the facts and careful review of recommendations on how to protect social media accounts.

Q. Am I allowed to share information about the Air Force on my social media accounts?
A. Yes. Assess the risk and if you choose to engage, do so safely and within Air Force and DoD guidelines. In particular, military information about current operations has brought attention and on-line threats to a few of our Airmen. Think about what you are posting and, as always, ensure the information you're posting is cleared for release and appropriate. Be cautious with information you may have access to that is sensitive and should always follow established release protocols – such as if a unit member is injured, killed or missing. And for all posts, employ common sense by considering how information could be used. If you post that your family is on vacation, for example, that signals that your house is vacant.

Q. What can I do to protect myself on social media?
A. Refrain from tagging or posting your specific location. Know and manage your 'friend' or 'follower' list closely. Use strong passwords. Keep your personal information private and review any posts you are tagged in prior to them showing up on your profile. Do the same for your family.

RESOURCES FOR AIRMEN ABOUT DIGITAL & INFORMATION SECURITY

ACC Digital Security Page
http://newpreview.afnews.af.mil/acc/library/sm&digitalsecurity/index.asp
Air Force Social Media Guide
http://www.af.mil/Portals/1/documents/SocialMediaGuide2013.pdf
Department of Defense Social Media Hub
http://www.defense.gov/socialmedia/
Air Force Instruction 1-1, Air Force Standards
http://static.e-publishing.af.mil/production/1/af/publication/afi1-1/afi1-1.pdf
Air Force Instruction 10-701, Operations Security (OPSEC)
http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-701/afi10-701.pdf

ACC Threat Information Fusion Cell

Homeland Defense Information Summary

16 December 2014

United States Air Force ★ Headquarters Air Combat Command ★ Joint Base Langley-Eustis, Virginia

USNORTHCOM Baseline FPCON ALPHA With Select BRAVO Measures

NTAS National Terrorism Advisory System NO ACTIVE ALERTS www.DHS.gov/alerts

Defense Intelligence Agency THREAT LEVEL SIGNIFICANT (United States)

Note: ACC Wings have implemented additional measures from higher FPCON levels. For a complete rundown, please contact ACC/A7SOA.

Significant News Items: Homeland

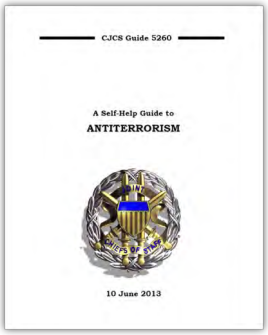
- Sony Warns Current, Former Employees About Potential Phishing Attacks
- Recent Arrests Show Broad Recruitment Efforts of Militant Group
- Nearly 600 Students, Staff Members Absent from Chicago-Area Schools Due to Flu-Like Symptoms
- Suspect in Six Pennsylvania Killing is Target of Manhunt

Significant News Items: International

- Taliban Storm Pakistani School, Killing 100-plus
- British Embassy in Cairo Reopens as Security Concerns Subside
- Militants Capture Two Key Syrian Military Bases
- Yemen Presidential Aide Says Houthis Plotting to Bring Down Government
- Police Make 7 Terror Arrests in Spain, Morocco

Additional Information...

- **OCJCS PC 5260 Pocket Card**
- **CJCS Guide 5260 - A Self-Help Guide to Antiterrorism** *(Click the images below to open the documents)*



(U) Threat Awareness/Individual Protective Measures

(U) Background. The threat environment within the U.S. continues to present new and diverse challenges for the force protection community. Multiple foreign terrorist organizations are actively encouraging supporters to take action against Americans and Westerners, and recent events in Canada and Australia suggest the call for action is reaching a somewhat receptive audience. Based on the complexities of the current threat, heightened vigilance/situational awareness is crucial. The information below offers some suggestions to assist personnel, including family members, in developing the individual protective measures necessary to prepare for threats.

- **(U) General Security Issues.** Being security conscious is the basis of individual protective measures no matter the threat. Be aware of your personal signature (clothing, hats, stickers, license plate frames, etc.) and consider limiting overt signs of DoD affiliation. This is not a recommendation to hide or live in fear, rather understand that current threat actors/terrorists may be looking for you; don't make it easier for them than it already is. Maintain a high level of situational awareness - pay attention to your surroundings and report suspicious behavior or out of place items (strange or illegally parked vehicles, unattended packages, suspicious people, etc.)
- **(U) Be Prepared for the Unexpected.** Current threat actors/ terrorists will likely attempt unsophisticated, violent attacks that will initiate quickly. Vehicle ramming, shooting, and stabbing/slashing are all easily executed tactics well within the capabilities of US-based extremists and lone-offenders. Remain aware of surroundings and know where facility exits and/or safe areas are at all times. Always have a plan.
- **(U) Operations Security.** Guard information about yourself and your unit's mission – this includes work correspondence and all forms of social media. Current threat actors are often extremely tech savvy. OPSEC violations or the careless sharing of too much information can *attract* a threat to a particular target or installation. Don't compromise your safety or the mission by giving away too much information.
- **(U) Family Security.** Threat actors/terrorists may strike out at residences or off base facilities frequented by DoD members and their families. These easily accessible locations are often referred to as "soft targets". Educate your families on the risk and consider having them complete the DoD Antiterrorism Level I training located here.
- **(U) Transit Security.** The attributes that make mass transportation convenient – defined schedules/routes & minimally invasive security procedures – make it an appealing and sometimes easy target for terrorists. Maintain a high level of situational awareness when traveling and take all precautions (clear security quickly, stand away from the crowd on subway/train platforms, avoid the middle seats on trains, subways, & buses, etc.) possible to enhance your security posture.

This product is compiled from various reporting sources and may be comprised of raw, uninvestigated information. **Threat data contained in this summary is not actionable or directive – it is provided for situational awareness.** Recipients are reminded content **may** be LAW ENFORCEMENT SENSITIVE. Unauthorized distribution (Outside of DoD or Federal Law Enforcement/Antiterrorism/Force Protection, State Law Enforcement, or Local Law Enforcement channels) of LES information could seriously jeopardize the conduct of on-going investigations and/or the safety of law enforcement personnel. NOTHING IN THIS DOCUMENT MAY BE DISTRIBUTED TO THE PUBLIC OR MEDIA. The ACC/TIFC HDIS may not be posted to any website without the expressed written permission of the originator. Furthermore, this document may contain information that may be exempt from public release under the Freedom of Information Act (5 USC 552). Intelligence Oversight policy applies to the information contained within the summary and the summary cannot be further disseminated without permission from the originator (ACC/TIFC). Questions, comments, or recommendations can be forwarded to the ACC TIFC at acc.tifc@langley.af.mil.

How Many Pieces of Military Flair are on Your Social Media?

Being a member of the United States Air Force should without question be a source of pride. The service you render to the United States is a vital one and retired Air Force members and family members take an equal pride in the service they have and do render to the Air Force. Unfortunately, there will always be people who, for various reasons, wish to bring harm to military members and those affiliated with the military. The wear of the uniform is a badge of honor and sets you apart, but in the wrong setting, can be unwise. Likewise, not just in person, display of the uniform and other Air Force symbolism also draws attention to your online presence – the more military pictures and information, the more attention. As in the movie *Office Space*, there is a difference between 1 or 37 pieces of flair! How much "military flair" is attracting attention to your social media?

Social media web pages can potentially be viewed by anyone with access to the Internet, and this information is easily exploited. One piece of information by itself may not be harmful, but multiple little pieces put together can, like a jigsaw puzzle, present a bigger picture.

Consider:

Jigsaw Piece #1 Post picture of self in uniform

Jigsaw Piece #2 Add location to profile: "Panama City, FL"

Jigsaw Piece #3 Post picture of your car which happens to be parked in front of your house – showing not only what you drive, but possibly a license plate number, possibly the mailbox with address on it, or a street sign, or your house number.

You just made yourself an easy target for anyone wanting to bring harm to a military member or their family.

Also consider the possibilities if your posting or profile has pictures of you; or if it has enough information for a stranger to find your residence. You then "check in" at your favorite restaurant. You just made both yourself and your unoccupied house potential targets. You just became a target to anyone who wants to take action against a military member – they know exactly what you look like and where you are. Your house just became a target for any common thief to break in and take your prized possessions. Is it worth the risk? Consider instead "checking in" as you leave the restaurant if you want to post a withering exposé about the service received, or bring out your epicurean side and rave about the delicious dinner.

Take pride in being a member of the United States Air Force and in the service you render to the United States, but use caution to go along with that pride. Social Networking is as much a part of modern life as breathing, but similar to hyperventilating, too much of it can be a bad thing. Take a few minutes to review your social networking sites: check the privacy settings, the amount of "military flair", and the sum of the information you have posted – the "jigsaw puzzle" available to anyone surfing the World Wide Web. Are you comfortable with what you see?