OPSEC and Media Guidance for Families

Operations Security for Family Members

As a family member of the military, you are vital to our success and we could not do our job without your support. You may not know it, but you also play a crucial role in ensuring your loved ones' safety. You keep your loved ones safe by protecting the information you know of the military's day-to-day operations. This is known in the military as Operations Security or OPSEC.

OPSEC is keeping potential adversaries from discovering information that is critical to your families' safety, your spouse's safety and the unit's mission accomplishment. Mission accomplishment depends on safeguarding critical information, which allows the unit to accomplish its mission with minimal risk. Our nation's enemies are always trying to find out information concerning your Marines/Sailors and their families.

Three primary things to remember about OPSEC:

- **WHERE** and **HOW** you discuss information is just as important as with **WHOM** you discuss it; places like the internet - social media, blogs, and chat rooms are not the places to reveal any unit deployment information since you are never certain as to who is on the receiving end of the information. Personal conversations conducted in public are also easily overheard.
- Individuals can easily collect data from unsecured cordless and cellular phones, even baby monitors and security cameras (e.g. Nest, Ring, etc). Always use varied passwords and enable two-factor authentication (2FA) when possible to ensure your safety.
- If anyone, especially a foreign national, persistently seeks information, notify your Marine and the unit immediately without beginning or continuing to respond to the individual. This includes when you're contacted from an unofficial source outside of the chain of command via text or social media messaging.

Limited Communication during training/deployment:

During deployment, your Marine or Sailor may not be able to communicate with you, for a limited period of time, either due to technical problems or the need for operations security. When necessary, the Commanding Officer will pass information to families, via the Deployment Readiness Coordinator (DRC). The Communication Strategy & Operations (COMMSTRAT) section will continuously update the unit's official sites with credible and accurate information.

Exercising Caution with Social Media

In today's electronic world, we are able to send and view information quickly, as social media access is available everywhere you go. The COMMSTRAT Office publishes information that has been approved by and is accordance with Department of Defense policies. Families and friends are encouraged to folllow and share the information provided on unit public web pages.

OPSEC issues stem from how people communicate on social media sites. **REMEMBER that anything published to social media is public and can be used by media outlets**.

Please follow these tips:

Personal Information

1. Keep sensitive, family-related information OFF your profile.
2. Keep your plans, schedules, and location data to yourself.
3. Protect the names and information of coworkers, friends, and family.
4. Tell friends to be careful when posting photos and information about you and your family.

Posted Data

1. Check photos for things in the background (or reflections) that could give away sensitive information.
2. Double check that you want this information available forever to anyone at any time.

Settings and Privacy

1. Carefully look for and set your privacy and security options.
2. Use the strongest password settings allowed, and don't reuse them for other sites.
3. Sort "friends" into groups and networks, and establish access permissions accordingly.
4. Verify through other channels that a "friend" request was actually from your friend.
5. Add "untrusted" people to the group with the lowest permissions and accesses.

Security

1. Keep your anti-virus software updated.
2. Beware of links, downloads, and attachments just as you would in e-mails.
3. Beware of "apps" or "plug-ins" - unknown parties can use these to access your data and friends.
4. Look for HTTPS on the URL line and the lock icon on the webpage indicating active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Remember that you are part of the military community and responsible for helping keep them safe. Be responsible with everything you share online. If you have any questions regarding what you can or cannot post, contact the DRC. While we provide the most up-to-date information, there are few restrictions on what others can post or claim. If you see any "new information," consider the source, the timing, and the content before reposting or reacting. When in doubt, reach out and report a concern.

Media Awareness

Anytime a unit is deployed, there is a potential for media members to reach out to family members for interviews or other stories. Here are a few things to keep in mind:

- Family members are allowed to speak with media, but it is important to keep OPSEC in mind during any interaction with the media.
- You can refuse to speak with media members.
- Once you agree to be interviewed, anything you say should be considered on the record.
- Be proud of your service member's service and feel free to speak generally about it.
- Be aware of what information you are sharing online or in public – OPSEC!
- Everything you post on social media is public and can be used by media outlets.
- You can always tell media members to contact the command COMMSTRAT office.
- Family and friend support is vital to mission success.

Contact information for II MEF COMMSTRAT Office
Phone: 910-451-7200, Email: IIMEFCOMMSTRAT@usmc.mil