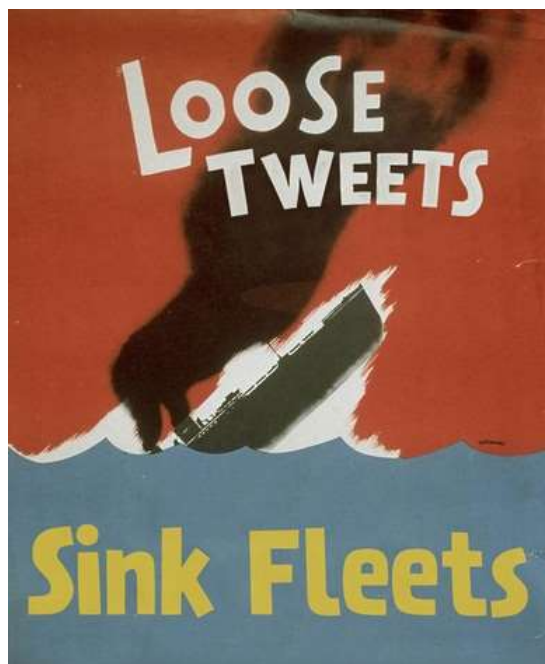# What Information is Sensitive?

Examples of Critical Information: The following examples may help you in defining parameters for your communications. It is important to remember that there are many more examples than those listed below:

- Detailed information about missions of assigned units.
- Details concerning locations and times of unit deployments.
- Personnel transactions that occur in large numbers (e.g., pay information, power of attorney, wills or deployment information).
- References to trends in unit morale or personnel problems.
- Details concerning security procedures
- Puzzle Pieces: These bits of information may seem insignificant. However, to a trained adversary, they are small pieces of a puzzle that highlight what US forces are doing and planning. Remember, the elements of security and surprise is vital to the accomplishment of US goals and collective DOD personnel protection.

Where and how you discuss this information is just as important as with whom you discuss it. Adversary agents tasked with collecting information frequently visit some of the same stores, clubs, recreational areas, places of worship and social networking sites as you do.

Determined individuals can easily collect data from cordless and cellular phones and even baby monitors using inexpensive receivers available from local electronics stores.

Make sure if you use Social Networking sites such as Facebook or Twitter, to only add friends you really know. If you have never met them face to face, they probably do not need access to see photos or news about you and your family.

If anyone, especially a foreign national, persistently seeks information, notify your military sponsor immediately.

OPSEC for Families

Operations Security Guidance for Family Members

As a family member of the military community, you are a vital player in 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 just by what you know of the military's day-to-day operations. You can protect your loved ones by protecting the information that you know. This is known in the military as, "Operations Security", or OPSEC.

What is OPSEC? OPSEC is keeping potential adversaries from discovering Information that is Critical to your families safety and also your spouse's Mission Accomplishment. Mission Accomplishment depends on secrecy and surprise, so the military can accomplish the mission more quickly and with less risk. Enemies of freedom want this information, and they are not just after the military member to get it. In December 2009, Al Qaeda gave instructions to all their operatives to target military personnel and their families. They were told to search for personal information, find out where their families live, and find the easiest way to target their workplaces.

The posting of pictures and information to unofficial websites about your loved ones military unit and/or to personal and family websites has the potential to jeopardize the safety of the entire unit. eMarine serves as a central location that allows families the opportunity to still share pictures and information, while also allowing your family readiness officer to ensure proper OPSEC will help keep your family and the Marines safe.

What Can You Do?

There are many countries and organizations that would like to harm Americans and degrade US influence in the world. It is possible and not unprecedented for spouses and family members of US military personnel to be targeted for intelligence collection. This is true in the United States, and especially true overseas! What can you do?

1. Be Alert - Foreign Governments and organizations can collect significant amounts of useful information by using spies. A foreign agent may use a variety of approaches to befriend someone and get sensitive information. This sensitive information can be critical to the success of a terrorist or spy, and consequently deadly to Americans.
2. Be Careful - There may be times when your spouse cannot talk about the specifics of his or her job. It is very important to conceal and protect certain information such as flight schedules, ship movements, temporary duty locations and installation activities, just to name a few. Something as simple as a phone discussion concerning where your spouse is going on temporary duty or deploying to can be very useful to adversaries.
3. Protecting Critical Information - Even though this information may not be secret, it is what the Department of Defense calls "critical information." Critical information deals with specific facts about military intentions, capabilities, operations or activities. If an adversary knew this detailed information, US mission accomplishment and personnel safety could be jeopardized. It must be protected to ensure an adversary doesn't gain a significant advantage. By being a member of the military family, you will often know some bits of critical information. Do not discuss them outside of your immediate family and especially not over the telephone or online.

CDSE — Center For Development of Security Excellence

Security Awareness Hub

OPSEC Awareness for Military Members, DoD Employees and Contractors

This is an interactive web-based course that provides OPSEC awareness for military members, government employees, contractors and dependents. The course provides information on the basic need to protect unclassified information about operations and personal information to ensure safe and successful operations and personal safety.

NOTE 1: The course includes a printable certificate which can serve as evidence that a student completed the course. When a student takes the course using this link, CDSE will not maintain any record of that student by name or any personally identifiable information. If the student needs documentation that he or she has completed the course, he or she will have to print the certificate at the end of the course.

Launch Course

Recommendations

Here are some other recommendations based on this course.

OPSEC Fundamentals

JIOWC Joint OPSEC Support Element OPSEC Awareness Videos

DoD Education Activity

Security Posters

Security Awareness Hub

This website is the premier destination for accessing security awareness courses for DoD and other U.S. Government and defense industry personnel who do not require transcripts to fulfill training requirements for their specialty.

A certificate is provided after the course is completed; however, there is no record maintained by CDSE. Additional eLearning and instructor-led courses, that CDSE maintains a record of, are available on the CDSE Learning Management System called STEPP. To view these additional courses, please see the complete course catalog at http://www.cdse.edu/catalog/index.html.

Counterintelligence

- Counterintelligence Awareness and Reporting for DoD
- Counterintelligence Awareness and Security Brief
- Integrating CI and Threat Awareness into Your Security Program
- Thwarting the Enemy: Providing Counterintelligence and Threat Awareness to the Defense Industrial Base

Cybersecurity

- Cybersecurity Awareness
- Introduction to the Risk Management Framework (RMF)

Information Security

- Derivative Classification
- Derivative Classification Refresher
- Identifying and Safeguarding Personally Identifiable Information (PII) Version 2.0
- Marking Classified Information
- Original Classification
- Safeguarding Personally Identifiable Information - PII
- Unauthorized Disclosure of Classified Information for DoD and Industry
- Unauthorized Disclosure Refresher

Insider Threat

- Establishing an Insider Threat Program
- Insider Threat Awareness

Operations Security

- OPSEC Awareness for Military Members, DoD Employees and Contractors

You should see our new videos »