



*Personnel*

**ANCILLARY TRAINING –  
OPERATIONS SECURITY**

---

OPR: 446 OSF/IN (Major Guy Perry)

Certified by: 446 AW/CC (Col Alan M. Mitchell)

No. of Printed Pages: 2

Distribution: F

---

This pamphlet implements Air Force Policy Directive (AFPD) 36-22, *Military Training*. It provides information on the importance of maintaining Operations Security (OPSEC) which is the responsibility of all personnel. This pamphlet fulfills the annual requirement for all personnel to be briefed on OPSEC procedures. It applies to all individuals assigned to the 446<sup>th</sup> Airlift Wing (446 AW).

**1. Purpose.** The goal of OPSEC is to control information and observable actions about mission capabilities, limitations, and intentions in order to prevent and/or control exploitation by an adversary.

**2. Prescribing Directive:**

2.1. Air Force Instruction (AFI) 10-1101, *Operations Security*.

**3. Reason for Learning.** Military Necessity. OPSEC does not only apply to classified information. Safeguarding sensitive unclassified information prevents an adversary from piecing together small pieces of the puzzle to obtain valuable information on current and future unit operations. Good OPSEC procedures prevent the adversary from gaining an advantage during a conflict.

**4. OPSEC:**

4.1. Classified information constitutes only a small fraction of the information and activities that the majority of us process every day. Most of the information we deal with is unclassified. Many wrongly think that if information and/or activities are not important enough to be classified, then they do not need to be protected. However, government sources estimate that 75-90 percent of our adversaries' information collection requirements can be satisfied through unclassified open sources.

4.2. Look at yourself from the adversary's point of view, not only when deployed, but at all times, from home station through deployment, employment and redeployment back to home station. Security regulations are primarily concerned with safeguarding classified documents and information. Be sure to safeguard sensitive unclassified information too.

4.3. Unclassified information of a sensitive nature, improperly handled, can easily provide adversaries with valuable insights into future operations.

4.3.1. "Dumpster diving" is the number one means of gaining espionage information and is perfectly legal according to the ruling of the Supreme Court. Orders and other documents may be easily picked out of the trash at the landfill to find their way to a new home with a Foreign Intelligence Service (FIS).

4.3.2. Press releases are another source of information for a possible adversary. Be cognizant of what you say in any press interviews. The FIS can read an article in the local newspaper and identify your unit, mission, deployment dates and a wealth of other information. This unclassified information verifies and adds to any other information the FIS may have.

4.3.3. Telephone conversations can include information that is unclassified, but when monitored by an adversary can be detrimental to your unit's mission. Remember the telephone may be monitored by a FIS. It's illegal, but that won't stop them from doing it. They can take any information you give, add it to what they already have and know more about an upcoming deployment than you do.

4.3.4. E-mail, conversations in public places, and many other sources of unclassified information can provide an adversary in learning of upcoming events and give them an advantage in any possible conflict. It is everyone's responsibility to practice good OPSEC by limiting the disclosure of sensitive information.

**5. Summary.** This has been a short discussion of the importance of Operations Security. You should realize the importance of safeguarding sensitive information. Your unit OPSEC monitor can assist you in determining what is critical information and what is not. If you have any questions, don't hesitate to ask for their assistance.

ALAN M. MITCHELL, Colonel, USAFR  
Commander