



Personnel

**ANCILLARY TRAINING – SECURITY AWARENESS,
TRAINING, AND EDUCATION (SATE)**

OPR: 446 MSS/SCB (MSgt Thomas Henry) Certified by: 446 AW/CC (Col Alan M. Mitchell)
No. of Printed Pages: 3
Distribution: F

This pamphlet implements Air Force Policy Directive (AFPD) 36-22, *Military Training*. It provides an understanding of the inherent weaknesses in information systems and the potential harm to national security due to the improper use of information systems. It further recognizes practices that create vulnerabilities in information systems, and uses established security procedures to address them. Finally, it provides an understanding of how COMPUSEC, COMSEC, and EMSEC relate to the overall protection of information generated, process, stored or transferred by information systems. This pamphlet fulfills the annual requirement to conduct the SATE training. It applies to all individuals assigned to the 446th Airlift Wing (446 AW).

1. Purpose. The goal of the SATE Program is to train all personnel (military and civilian) to protect information and communication. NOTE: This is no substitute for the network users—in order to obtain a network account, you must still accomplish the SATE CBT on-line.

2. Governing Directives:

- 2.1. Air Force Instruction (AFI) 33-119, *E-mail, Management, and Use*
- 2.2. AFI 33-129, *Transmission of Information via the Internet*
- 2.3. Air Force Instructions (AFI) 33-204, *SATE Program*
- 2.4. AFI 33-219, *Telecommunications Monitoring*

3. Reason for Learning:

- 3.1. The SATE Program is comprised of three elements:
 - 3.1.1. Computer Security (COMPUSEC),
 - 3.1.2. Communications Security (COMSEC),
 - 3.1.3. Emissions Security (EMSEC).

4. Telecommunication Monitoring:

4.1. When talking about telecommunication monitors, we are talking about: telephones, computers, that is the email part, modems, fax machines, LMR and cellular phones.

4.2. NOTE: All government owned devices are subject to monitoring!

4.3. Labeling Telecommunication Devices:

4.3.1. All government telephone must have a DD Form 2056, **Telephone Monitoring Notification Decal**, affixed to them.

4.3.2. All faxes that are transmitted need to have a cover sheet and consent to monitoring statement.

4.3.3. All computers need to have a consent to monitoring log-on banner. This is normally found at the log-on script of a computer connected on a network computer.

4.4. Protect and Secure. The following are some things to consider in order to protect and secure your computer. They are:

4.4.1. Lock windows and doors.

4.4.2. Turn monitor away from windows.

4.4.3. When leaving a workstation, activate password protected screensaver or log-off.

4.4.4. Challenge unknown personnel.

4.5. Password Composition:

4.5.1. Each password must have at least eight characters,

4.5.2. No dictionary words (This includes foreign languages).

4.5.3. The password must include at least one number, at least one letter, a mixture of upper and lower case letters and at least two special characters (i.e., *& \$# @).

4.6. Internet and E-mail. The following items are not authorized: games, chat, offensive materials and/or sites, activity for personal financial gain, and chain letters.

4.7. Accountability. Violations of the proper use of government systems are punishable under Article 92 of the Uniform Code of Military Justice.

4.8. Virus Protection:

4.8.1. Ensure all systems contain virus protection software (including latest updates),

4.8.2. Scan all diskettes,

4.8.3. Use only approved software. NOTE: Downloadable “freeware” may contain viruses.

4.9. Unit Level Support. Once you are in your unit, all viruses, suspected intrusions, or other system problems should be directed to your Unit COMPUSEC Manager (UCM) or Work Group Manager (WGM).

ALAN M. MITCHELL, Colonel, USAFR
Commander