

**BY THE ORDER OF THE COMMANDER,
SPACE AND MISSILE SYSTEMS CENTER**



AIR FORCE INSTRUCTION 33-202

SPACE AND MISSILE SYSTEMS CENTER

Supplement 1

23 JULY 2003

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: 61CS/SCSB (Sylvia Montemayor)
Supersedes AFI33-202_SMCSUP1,
dated 30 Sept 00

Certified by: 61CS/SCB (Major Terri Centner)
Pages: 2
Distribution: F

This instruction supplements Air Force Instruction (AFI) 33-202, *Computer Security*, 30 August 01. This supplement describes SMC's procedures for use in conjunction with the basic AFI and AFSPC policies and procedures. This supplement is applicable to all SMC organizations and other organizations located on Los Angeles AFB CA or supported by SMC in the Los Angeles Area. SMC publications and forms are kept in a backup repository on <http://intranet.losangeles.af.mil/61ABG/61CS/SMCPDL/>.

SUMMARY OF REVISIONS

This revision added paragraphs 3.14.1, and 3.14.2 and removed paragraphs 2.7, 2.7.2, 2.11.2, 3.2.1, 3.2.1.1, and 3.1.3.4

2.7.5. The organizational Information Systems Security Officer (ISSO) serves as the Certifying Official for that organization's systems.

2.10.1. As Los Angeles AFB (LAAFB) has no wings in its organizational structure, the Base Information Assurance Office (BIAO) is the equivalent organization. All references to the Wing IA Office should be understood to refer to the BIAO unless otherwise indicated. All references to the Wing Information Systems Officer (ISO) should be understood to refer to the Chief, BIAO, unless otherwise indicated.

2.11.1. LAAFB has not implemented unit COMPUSEC managers. These functions are performed by the ISSOs.

2.11.3.7. LAAFB ISSOs are responsible for ensuring implementation of Air Force Time Compliance Network Orders (TCNOs), Air Force Computer Emergency Response Team (AFCERT) advisories, AFSPC Network Operations Security Center (NOSC) Notice To Airman (NOTAMs), and all other computer security directives, using the BIAO's Computer Security Message Tracking System (CSMTS). The alternate method of reporting procedures is via e-mail initiated by the BIAO. Responses will be submitted to the BIAO according to the following timetable:

TCNOs: Comply and report compliance status to BIAO using the Computer Security Message Tracking System (CSMTS) or other approved means by the established suspense date.

NOTAMs: Comply and report compliance status to BIAO using the CSMTS or other approved means by the established suspense date.

3.14. **Training.** All network users will take the Information Assurance and Information Operation Conditions (INFOCON) Computer Base Training (CBT) annually. All Functional System Administrators will take the "System Administrator" CBT annually. All base users who handle classified information will take the "Classified" CBT annually.

3.14.1. (Added) Users will print out their test results and provide the printout to their ISSO. ISSOs will maintain test results for all users on file for a minimum of one year.

3.14.2. (Added) All network users who provide their password or respond in any way to an e-mail message or other "social engineering" request for their password will immediately have their network account disabled and must re-take the IA CBT to ensure they understand Information Assurance policies and procedures.

STEPHEN W. STARKS, Lt Col, USAF
Commander