

18 May 1998

Communications

**ANDREWS AIR FORCE BASE INFORMATION
PROTECTION OPERATIONS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available in electronic format on the local server. If you lack access, contact your Base Publishing Office.

OPR: 89 CS/SCBS (Mr. Mays)

Certified by: 89 CG/CC (Col Jakowatz)

Pages: 6

Distribution: F;X HQ AMC/SC...3

This instruction implements Air Force Policy Directive (AFPD) 33-2, *C4 Systems Security*, and Public Law 100-235, *The Computer Security Act of 1987*. It provides detailed guidance and responsibility for establishing and managing the Information Protection Operations; defines the program goals; and applies to all military and civilian personnel including the Air National Guard and US Air Force Reserve. It also supports the programs outlined in other publications such as Air Force Instruction (AFI) 33-202, *The Computer Security (COMPUSEC) Program* and AFI 33-208, *Information Protections (IP) Operations*.

1. Introduction. Command, control, communications, and computer (C4) systems and the information processed or stored by them are important to the operation of the 89th Airlift Wing, as well as Andrews Air Force Base (AFB) tenant organizations.

1.1. 89th Airlift Wing and Andrews AFB tenant personnel who operate and maintain C4 systems will protect them at a level commensurate with the risk and the magnitude of harm that could result from disclosure, loss, misuse, alteration, or destruction of information or systems.

1.2. Andrews AFB personnel authorized use of C4 systems will prevent unauthorized access to, and will prevent the introduction of malicious logic into C4 systems.

1.3. Andrews AFB personnel are responsible for compliance with copyright laws covering computer software. Individual users are responsible for all software on their computer system according to AFI 33-112, Automatic Data Processing Equipment (ADPE) Management.

1.3.1. The installation commander delegates to the communications-computer systems officer (89th Communications Group Commander) the authority to conduct random computer checks/inspections upon computer systems located on Andrews AFB.

1.3.2. The IP office will be the office of primary responsibility for the random computer checks/inspections program. Under Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797) and in accordance with AFI 33-202, the IP office will conduct checks/inspections (**Attachment 1**) to

ensure compliance with copyright laws and Air Force computer security policies. The unit computer systems security officer (CSSO) or NCO may accompany the IP office during the check.

1.4. Andrews AFB C4 systems will be accredited before operational use.

1.5. Andrews AFB C4 systems users will identify requirements and ensure cost-effective C4 systems security capabilities are incorporated into acquisition programs.

2. Andrews AFB Responsibilities:

2.1. 89th Security Forces Squadron provides policy, guidance, and direction on information, personnel, industrial, and physical security programs as they apply to the protection of classified information in C4 systems, facilities, and personnel IAW DoD and Air Force directives.

2.2. Detachment 302, 3d FIR (AFOSI) provides hostile and criminal threat assessment, technical surveillance countermeasures, and information on the exploitation of C4 systems resources.

2.3. The integrated C4 systems security office for the 89th Airlift Wing and Andrews AFB tenants is the 89th Communications Squadron, base IP office, extension 2-9334.

3. C4 Systems Security Programs:

3.1. The IP office manages four programs for the installation, which are: Communications Security (COMSEC), Computer Security, Emissions Security (EMSEC, formerly TEMPEST), and Security Awareness, Training, and Education (SATE). Specific responsibilities are in the 89th Airlift Wing C4 systems security instructions.

3.2. COMSEC is responsible for the management of the Andrews AFB communications security account that controls and safeguards all registered and sensitive classified cryptographic documents held for issue and use by C4 system users.

3.2.1. COMSEC Manager ensures implementation of the COMSEC Incident Reporting Program prescribed by AFI 33-212, Reporting COMSEC Incidents.

3.3. COMPUSEC manages the computer security program for the installation and is responsible for the measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

3.3.1. COMPUSEC Manager ensures implementation of the COMPUSEC Incident Reporting Program. Report all Automated Information Systems (AIS) vulnerabilities, security incidents, and virus attacks according to instructions outlined in AFMAN 33-225, Vulnerability and Incident Reporting.

3.4. Emissions Security is responsible for program management involving the investigation, study, and the control of compromising emanations from telecommunications and AIS equipment for Andrews AFB.

3.5. SATE is responsible for the establishment and development of an aggressive C4 systems security education program for all Andrews AFB personnel.

3.5.1. The primary SATE Program Manager for Andrews Air Force Base is assigned to the 89th Communications Squadron, base IP office.

3.6. IP office conducts staff visits and functional reviews of C4 systems users to evaluate the adequacy of classification, declassification, and safeguarding policies; observes implementation of security programs to ensure they have emergency plans, adequate training, and maintain accountability; and obtains information required for the development of new or revised policy procedures.

4. Incident Reports. C4 systems security incidents must be reported immediately to the IP office and the appropriate chain of command. If an accident involves classified information, the unit security manager must report it to 89 SFS/SFAI.

ARTHUR J. LICHTER, Brigadier General, USAF
Commander

Attachment 1

CHECK AND INSPECTION OF COMPUTER SYSTEMS ON ANDREWS AFB

A1.1. Assess compliance with C4 systems security policy by conducting random computer checks/inspections of Andrews AFB automated information systems.

A1.1.1. While on the installation, all personnel and the property under their control, are subject to search under Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797).

A1.2. Purpose of random computer checks/inspections.

A1.2.1. Ensure that the operating organization has a Designated Approving Authority (DAA) accreditation for the AIS in operation.

A1.2.2. Ensure that the AIS is protected as sensitive but unclassified (SBU) IAW AFI 33-202, [Attachment 2](#).

A1.2.3. Ensure that the AIS has identification, authentication, and audit capability IAW AFMAN 33-229.

A1.2.4. Ensure that safeguards are effective, efficient, and integrated to ensure AIS meets security requirements.

A1.2.5. Verify that the AIS is protected and stored according to AFI 31-401.

A1.2.6. Ensure that only Air Force owned, approved contractor-owned, or DAA approved personally-owned hardware or software is used.

A1.2.7. Ensure compliance with software copyright laws.

A1.2.8. Verify that the AIS is used only for official government business.

A1.3. Procedures for random computer checks/inspections.

A1.3.1. The Communications-Computer Systems Officer (SC) will select the organization, date, and number of computers to be checked by drawing lots.

A1.3.2. The SC will fill in the appropriate blocks on the **Check and Inspection of Computer Systems on Andrews AFB MD** memorandum ([Attachment 2](#)) and provide this to the base IP office.

A1.3.3. The IP office will present the memorandum to the identified organization upon their arrival to conduct the computer checks/inspections.

A1.3.4. The identified organization will provide any needed assistance and cooperation in the conduct and completion of the checks/inspections.

A1.3.5. The results of the checks/inspections will be provided to the SC and forwarded to the installation commander.

Attachment 2

SAMPLE CHECK AND INSPECTION MEMORANDUM

MEMORANDUM FOR 89 CS/SCBS

FROM: 89 CG/CC

1558 Alabama Ave., Suite 9

Andrews AFB MD 20762-6116

SUBJECT: Check and Inspection of Computer Systems on Andrews AFB MD

1. By the authority granted to me by the installation commander, Under Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797), and IAW procedures listed within AFI 33-202, The Computer Security Program, I order that random computer checks/inspections be conducted upon computer systems located on Andrews AFB.

2. The below procedures are to be used for the examination of computers without the foundation for a check. These random inspections are not based on probable cause but on my authority granted to me by the installation commander to protect the security of this command and to protect government property. When conducting these inspections, the information protection (IP) office is not acting as law enforcement, but is charged with safeguarding automated information systems and protecting government property.

3. Computer inspections will be conducted on:

a. DATE: _____

b. TIME: _____

c. LOCATION: _____

d. NUMBER OF COMPUTERS CHECKED: _____

4. IP office personnel will conduct these checks/inspections IAW AFI 33-202, and are reminded that every person operating automated information systems will be provided the utmost courtesy and consideration. The highest degree of professionalism, tact, and diplomacy will be displayed at all times.

5. Any questions on the above information, please contact the IP office at extension 2-9334, during normal duty hours.

Communications-Computer Systems Officer