



**Security**

**\*PERSONNEL AND INFORMATION SECURITY  
PROGRAM MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

NOTICE: This publication is available digitally on the AFOATS Restricted Website at: <https://afoats.hq.af.mil>.

---

OPR: HQ AFOATS/SDPP (2Lt Benjamin Gardner)

Certified by: HQ AFOATS/SD (Col Greg C. Winn)

Pages: 8

Distribution: F

---

This instruction defines and explains the responsibilities and procedures for the protection and handling of classified information received by the Air Force Officer Accession and Training Schools (AFOATS). It implements the applicable provisions of DoD 5200.1-R, *Information Security Program*, AFI 31-401, *Information Security Program Management*, and AFI 31-501, *Personnel Security Program Management*. Additional references also include DoD 5200.2-R, *Personnel Security Program*, AFI 31-401 AETC Sup 1, *Information Security Program Management*, AFI 31-401 MAFB Sup 1, *Information Security Program Management*, AFI 31-501 AETC Sup 1, *Personnel Security Program Management*, and AFI 31-501 MAFB Sup 1, *Personnel Security Program Management*. This instruction applies to all personnel (military and civilian) permanently assigned to AFOATS.

## **1. Responsibilities**

### **1.1. The AFOATS Commander will:**

1.1.1. Appoint a primary and alternate security manager and ensure these appointees receive the necessary unit security manager training.

1.1.2. Appoint an individual, E-5 or above (or civilian equivalent employee), to conduct an annual self-inspection for the purpose of evaluating information and personnel security program effectiveness.

1.1.3. Review annual self-inspection reports and biannual program reviews and provide written endorsement of concurrence.

1.1.4. Appoint an individual E-7 or above (or civilian equivalent), to conduct a preliminary inquiry and/or formal investigation in the event of a security incident. The appointment shall occur by the end of the duty day on which the incident transpired.

1.1.5. Review unfavorable information on individuals in AFOATS when reported or developed which would directly impact an individual's security clearance. Follow procedures in AFI 31-501 para 8.2. to establish a Security Information File (SIF).

1.1.6. Review the Unit Manning Document (UMD) on an annual basis to determine if the positions within the organization are assigned the proper security code.

## **1.2. The AFOATS Security Manager will:**

1.2.1. Contact the Installation Security Program Manager (ISPM) within 30 days after appointment to receive the formal unit security manager training. This training must occur within 90 days of assignment to the position.

1.2.2. Maintain a security manager's handbook in accordance with AFI 31-401 and review it periodically to ensure effectiveness and accuracy.

1.2.3. Develop and maintain internal instructions that cover the overall AFOATS security program. A review of the instructions will occur on an annual basis. The instruction will be forwarded to the ISPM prior to implementation.

1.2.4. Attend all scheduled security manager meetings.

1.2.5. Handle all personnel security actions for AFOATS members assigned to Maxwell AFB, to include clearance verifications, completing periodic reinvestigations, and security clearance terminations.

1.2.6. Provide information security support to all AFOATS members assigned to Maxwell AFB to include applicable education and training.

1.2.7. Ensure unit SIFs are reviewed and a status report is sent to 42 SFS/SFAIP every 30 days.

1.2.8. Maintain a monthly Clearance and Access Verification System (CAVS) roster and ensure that unit personnel's security clearances are accurate and up-to-date.

1.2.9. Create a unit security education and training program to provide initial security training and yearly security training on a quarterly basis to all unit personnel.

1.2.10. Assist security self-inspection appointees by providing them a copy of the current self-inspection guidelines and briefing them on all applicable requirements. The Unit Security Manager will aid the inspector as necessary for a comprehensive inspection of the program, will ensure the AFOATS Commander reviews the report and provides written endorsement after the inspection, and will forward a copy of the report to the ISPM.

1.2.11. Post AFVAs 31-6, Unclassified Reproduction Only and 31-8, Unclassified Destruction Only on or near all copiers and shredders respectively to ensure all AFOATS personnel recognize they are not authorized to reproduce or destroy classified material.

1.2.12. Coordinate with AFOATS Computer Support to ensure appropriate informational stickers are posted on all computers and phones indicating to all AFOATS personnel that they are not allowed to produce, access, record, process, or transmit classified data within those means.

**1.3. The AFOATS Commander's Support Staff will:**

1.3.1. Ensure all new personnel meet with the AFOATS Security Manager for their initial unit security orientation.

**1.4. Supervisors will:**

1.4.1. Assist the Unit Security Manager by ensuring their personnel (cleared and uncleared) receive the necessary security training outlined in this instruction.

1.4.2. Continuously evaluate cleared personnel to ensure they continue to be trustworthy in accordance with the standards established in DOD 5200.2-R, Chapter 2.

**1.5. All Unit Personnel will:**

1.5.1. Become familiar with and implement the directives outlined in this instruction.

**2. Procedures**

**2.1. Safeguarding of Classified Material:**

2.1.1. AFOATS does not store any classified material or have any safes authorized to store classified material.

2.1.2. AFOATS has several cleared personnel authorized to process classified material during duty hours.

2.1.2.1. Cleared personnel will maintain personnel control of classified material at all times.

2.1.2.2. Use the appropriate cover sheet when carrying classified information within the HQ AFOATS building (Bldg 500) or the OTS building (Bldg 1487). The correct forms to use are the SF 703, Top Secret Cover Sheet, SF 704, Secret Cover Sheet, or SF 705 Confidential Cover Sheet.

2.1.2.3. When carrying classified material outside of buildings, the classified material must be covered by two opaque containers. The outer container must not contain any

markings identifying the level of classification of the material within. The inner container must identify the highest level of classification of the material within (See DoD 5200.1-R para C7.2.1).

2.1.3. Personnel working with classified material must do so in a secure room with no windows or with windows covered. The door to the room must be locked to prevent unauthorized access and AETC VA 31-10, Classified Work in Progress will be posted on the outside of the door to the room.

2.1.4. When cleared personnel complete work on classified material, the material will be hand-carried to the 42 ABW Command Post for proper storage.

2.1.5. All other AFOATS personnel are designated as uncleared personnel. These are personnel that do not require access to classified material.

2.1.6. If uncleared personnel discover classified material unattended in the workplace or if the mail or distribution systems deliver classified to AFOATS, members will take control of it and safeguard it immediately. They will not leave it unsecured.

2.1.6.1. The member discovering it will immediately notify the Security Manager. Members will not open sealed classified material.

2.1.6.2. The Security Manager, at the direction of the AFOATS Commander or senior ranking officer, will notify the ISPM to ensure proper control of all misdirected classified information.

2.1.7. The Security Manager will continuously make attempts to ensure an appropriate, authorized agent receives the material. If all attempts fail, an appointee with the proper clearance eligibility and access code will destroy the classified material in accordance with United States Air Force (USAF) guidance. Other members may have to witness or sign a destruction log as necessary.

2.1.8. If scheduled, classified material arrives at AFOATS, authorized personnel must properly safeguard the material.

2.1.9. Designated personnel will maintain personal control of the material until they hand-carry it to the 42 ABW Command Post for authorized storage.

2.1.10. At no time will personnel leave classified material unattended or take the material off the installation.

2.1.11. The authorized agent and Security Manager will ensure proper disposal, destruction, and declassification of material as soon as possible after its use.

2.1.12. In the event of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, personnel who process classified material must take personal control of the material and protect it at all times until it can be properly destroyed or stored.

2.1.13. Personnel with questions pertaining to the protection of classified material will direct them to the AFOATS Security Manager.

## **2.2. Reproduction of Classified Material:**

2.2.1. AFOATS reproduction equipment is not certified to copy classified material. Personnel will not, under any circumstances, use AFOATS copy machines for reproducing classified material.

2.2.2. If absolutely necessary and with the specific permission of the AFOATS Commander and the originating authority, personnel will only use those copiers (outside the organization) certified for classified reproduction. The AFOATS Commander will grant permission on a case-by-case basis.

## **2.3. Receipt, Transmission, and Dissemination of Classified Materials:**

2.3.1. With the exception of those situations covered under paragraph 2 and others within the authorized parameters of the AFOATS Commander's authority and the Air Force guidance, AFOATS personnel will not communicate or receive classified material or information through any means (computer, fax, modem, oral, written, etc.).

2.3.2. Under no circumstances will AFOATS personnel attempt to receive, transmit, or disseminate classified information by "talking around the subject" or using codes.

## **2.4. Destruction of Classified Material:**

2.4.1. AFOATS shredders are not certified to destroy classified material. Personnel will not, under any circumstances, use unit shredders to destroy classified material.

2.4.2. If necessary and with the specific permission of the AFOATS Commander, personnel will only use those shredders (outside the organization) certified for classified destruction. Personnel will coordinate with the AFOATS Security Manager to ensure proper destruction procedures in accordance with AFI 31-401.

## **2.5. Awareness and Training:**

2.5.1. Because of the quantity of unclassified material used at AFOATS, personnel must be extremely careful not to "slip out" classified information in a classroom or work setting. Access to classified material is not based on rank or position. Rather, it is based on a "need to know", which is not established at the unit level.

2.5.2. If unauthorized people or people unknown to AFOATS ask repeated questions about doctrine or other information, and the situation is suspicious, unit personnel must report the activity to their supervisor and to the Security Manager so that these activities are relayed to the proper base agencies.

2.5.3. AFOATS personnel will receive initial and recurring information security training according to the AFOATS Security Manager's Training Plan.

## **2.6. Administrative Sanctions:**

2.6.1. Anyone who knows of a security violation has an obligation to report it to their supervisor, their commander, or the AFOATS Security Manager. If the violation is unreported, the witness is equally responsible for the breach of the information security.

2.6.2. All USAF military and civilian members are subject to administrative or disciplinary action under the Uniform Code of Military Justice or United States Code for willful or negligent disclosure of classified information.

PAUL M. HANKINS  
Brigadier General, USAF  
Commander, AFOATS

Attachment:  
Glossary of References and Supporting Information

**Attachment 1**

***GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION***

***References***

DoD 5200.1-R, *Information Security Program, Jan 97*

DoD 5200.2-R, *Personnel Security Program, Jan 87*

AFI 31-401, *Information Security Program Management, 1 Nov 01*

AFI 31-401 AETC Sup 1, *Information Security Program Management, 28 Jan 03*

AFI 31-401 MAFB Sup 1, *Information Security Program Management, 15 May 00*

AFI 31-501, *Personnel Security Program Management, 1 Aug 00*

AFI 31-501 AETC Sup 1, *Personnel Security Program Management, 28 Jan 02*

AFI 31-501 MAFB Sup 1, *Personnel Security Program Management, 10 Jun 98*

**Forms**

AETC VA 31-10, **Classified Work in Progress**

AFVA 31-6, **Unclassified Reproduction Only**

AFVA 31-8, **Unclassified Destruction Only**

SF 702, **Top Secret Cover Sheet**

SF 704, **Secret Cover Sheet**

SF 705, **Confidential Cover Sheet**

***Abbreviations and Acronyms***

**ABW** – Air Base Wing

**AETC** – Air Education and Training Command

**AFB** – Air Force Base

**AFOATS** – Air Force Officer Accession and Training Schools

## **Attachment 1**

### **GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION (Continued)**

**AFVA** – Air Force Visual Aid

**CAVS** – Clearance and Access Verification System

**DoD** – Department of Defense

**ISPM** – Installation Security Program Manager

**SIF** – Security Information File

**SF** – Standard Form

**USAF** – United States Air Force