



3 APRIL 2001

Security

THE AIR FORCE INSTALLATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AETC Publishing WWW site at: <http://www.aetc.randolph.af.mil/im>. If you lack access, contact your Base Publishing Manager.

OPR: HQ AETC/SFP (MSgt Eddie England)
Supersedes AFI 31-101/AETC Sup 1, 13 December 2000

HQ AETC/SFP (Lt Col Billy R. Detrick)
Pages: 11
Distribution: F

AFI 31-101, 1 June 2000, is supplemented as follows:

This supplement is not applicable to the Air National Guard, unless mobilized under AETC. Where AFI 31-101 states "MAJCOM determines" and this supplement does not address the area, authority is delegated to the Installation Security Council (ISC). ISCs document procedures in local supplements. Maintain and dispose of records created as a result of processes prescribed in this publication in accordance with AFMAN 37-139, *Records Disposition Schedule*.

★SUMMARY OF REVISIONS

This change incorporates interim change (IC) 2001-1 which deletes the requirement for munitions storage facilities to use the AF Form 1473 (paragraph 23.1.1); changes the requirement for all personnel authorized to open AA&E facilities to be armed (paragraph 23.1.6); changes the requirement for Category III and IV facilities to have intrusion detection equipment (IDE) (paragraph 23.3.2.4); and adds guidance on IDE for Category III and IV storage structures and containers (paragraph 23.3.3.8). See the last attachment of this publication for the complete IC. A ★ indicates revision from the previous edition.

1.8. AETC units located on other MAJCOM and/or other service bases also participate in the host base Resource Protection Program.

1.9. The installation chief of security forces (CSF) coordinates on all statements of work (SOW) or performance work statements (PWS) involving base contractor operations before the SOWs or PWSs are submitted to the contracting office.

2.8.3.4. The installation security council (ISC) will place supporting forces' responsibilities and entry control procedures for restricted areas containing protection level 3 (PL3) resources in the base installation security instruction (ISI).

3.3.2.3. State in the ISI how base directives will be publicized to all military personnel.

3.3.4.7. List the post priority charts as attachments to the ISI. Units may limit the distribution of these charts as they deem necessary.

3.4.2.1. Establish sufficient clear zones around the parking area boundary. Ensure the boundary is free of vegetation and impediments that will conceal the approach of an intruder.

3.6.2. The individual appointed to perform Crime Prevention Program Monitor duties will either attend course WCIP07A, Resource Protection/Crime prevention Theory, Practice, and Management, or enroll in ECI course 8100, USAF Crime Prevention Program, within three months of appointment.

3.6.3.2. The Installation Security Section (ISS) will maintain separate files for all controlled areas. The files will contain, as a minimum, those items listed in Attachment 1.

3.6.4.2. A memorandum signed by the installation commander will be sufficient when new areas are added between ISI publications.

3.7.2.5. Record results of the sweep in the security force desk blotter.

4.2.1.2. Security forces will coordinate with AFOSI to conduct a local threat assessment annually. The assessment will be made available to the threat working group (TWG).

4.2.4.1. Designate these areas in the ISI or ISP as appropriate.

4.2.5.1. The TWG will form part of the installation security council. The TWG will be comprised of representatives from security forces, intelligence, and AFOSI. Consider other representatives as may be appropriate. The TWG will review the last assessment conducted by the Joint Staff Integrated Vulnerability Assessment (JSIVA) team, the Air Force Vulnerability Assessment (VA) team, or the HQ AETC Vulnerability Assessment team and current means of intelligence and threat assessment. The TWG will also assess political vulnerability of foreign students attending training at the base.

4.2.5.2. The alarm working group (AWG) must convene annually or as determined by the ISC during the planning, designing, budgeting, and installation of initial and replacement systems. Only systems from the intrusion detection system (IDS) approval letter, signed by HQ USAF/XOF, will be considered for new and replacement systems.

4.3.1. For PL4 resources, if only one alarm is originating within a patrol sector, the response time will not exceed 5 minutes, unless a more stringent requirement is stated in local directives.

4.3.5. Special Security Instructions (SSI) should be specific for each post/patrol and should be updated as needed. General unit or branch operating instructions will not take the place of specific SSIs.

4.9. Within AETC, all SF units will contact HQ AETC/SFP prior to requesting the assistance of the Air Force, Force Protection Battlelab.

4.10. Under the provisions of AFI 31-210, *The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards*, paragraph 3.2.3, if the installation does not publish a supplement to AFI 31-210, the installation security plan must include the following: security and law enforcement assets, fortification plans, sensor plans, obstacle emplacement, contract/hired forces unit guards and on-call support from reaction forces, AT/FP training and education, vulnerabilities, associated countermeasures (classified annex), and a written barrier plan/annex. Installations will have 120 days to update their installation security plans upon release of AFI 31-210/AETC Sup 1. A copy must be sent to HQ AETC/SF.

4.11. The installation CSF is the OPR.

4.12.15. (Added)(AETC) A crisis management plan must be included as an annex if the installation does not have a supplement to AFI 31-210. (**NOTE:** A crisis management plan covers the same areas as contingency plans. Use the format in the AT/FP installation planning template compact disk.)

5.3.2. Identify termination authority for HELPING HAND reports in the ISI.

5.4.5. Identify termination authority for COVERED WAGON reports in the ISI.

6.5.1. Identify deviations by the year initially approved and number sequentially.

6.6. Deviation approval, disapproval, extension, and cancellation authority is delegated to each installation commander. All deviations will be forwarded to the HQ AETC/SF reviewing official for review prior to obtaining the installation commander's approval.

6.6.1.1. AETC units located on another MAJCOM's installation will forward deviations to the HQ AETC/SF reviewing official for review prior to obtaining the installation commander's approval.

6.6.1.2. Send tenant unit deviations to HQ AETC/SF for coordination. HQ AETC/SF will forward deviation requests to the appropriate tenant MAJCOM for coordination and return them to the installation commander.

6.8.1. Installation CSFs forward copies of all deviations (approval, disapproval, extension, and cancellation) to HQ AETC/SF. CSFs must forward a list of all deviations **NLT 15 January** of each year.

6.9.2. Follow the guidance in paragraph 6.9 when applying compensatory measures to deviations. The HQ AETC/SF reviewing official will address additional guidance, when needed, in block 20 of the AF Form 116, **Request for Deviation from Security Criteria**. This guidance will be addressed on a case by case basis.

7.2.2. Phase I, Orientation Training, will be conducted within 30 days of assignment, but prior to an individual performing their assigned duties.

7.2.4.1. Refer to AFI 36-2225/AETC Sup1, *Security Forces Training and Standardization Evaluation Programs*, for requirements.

7.2.4.2. All units within AETC possessing or supporting protection level resources will develop Phase I and Phase II training programs.

7.2.4.3. Phase II, Continuation Training, will be administered annually.

7.2.4.4. Training will be documented in unit training NCO databases and personnel OJT records.

7.3. All type six training will be completed prior to progressing to Phase I training.

7.3.1. AFI 36-2225/AETC Sup 1 outlines minimum proficiency training for AETC security forces members.

7.6. Staff assistance visits are conducted at the request of the installation or support group commander.

8.5.2. When special purpose gates are not being used, the keys will be maintained at the SF control center or with the patrol that has responsibility for that sector.

8.6. Publish gate closure procedures in the ISP.

8.7. Entry point checks include identifying unauthorized removal of classified information according to DoD 5200.1-R, *Information Security Program*, chapter 5.

8.7.2. Maintain the documentation of the installation entry checks for at least two years.

9.2.2. The approving official ensures the individual completes Phase I, physical security awareness training, before authorizing unescorted entry or escort official duties.

9.2.4. Each installation shall determine the number of copies, if any, of AF Form 2586, **Unescorted Entry Authorization Certificate**, and letters, if used, to meet operational requirements.

9.5.3. Publish restricted area badge turn-in procedures in the ISI.

9.6. Temporary badge systems are optional for each AETC SF unit. If established, use temporary badge systems to allow unescorted entry to authorized personnel for a short period of time, not to exceed 90 days. Badge issuing officials brief personnel on entry requirements before issuing temporary badges. Only personnel with permanent badges will act as escorts or escort officials.

9.6.1. Type or stamp a prominent letter "T" on the badge in place of the picture. Have the appropriate area on the badge open, list the installation name, badge number, and have an authorized badge issuing official sign the badge.

9.7.8.1. All personnel authorized unescorted entry into restricted areas are required to know the local duress code.

9.7.11. Publish emergency entry procedures in the ISI.

9.10.1. The on-duty flight chief or a security force supervisor authenticates entry authority lists (EAL). Authentication includes typed or printed name, grade, office symbol, and signature of authenticating official; date and time of authentication; and expiration date of EAL.

10.5. Units without permanent restricted areas may use installation security forces patrols armed with M16s for security of temporary restricted areas. Document procedures (for example, in security forces checklists, special security instructions, etc.) for combining patrols before deploying to incidents. Internal security response teams (SRT) posted in internal facilities may be armed with the M9 pistol or M870 shotgun if it is more appropriate for the threat and environment. The ISC specifies the type of weapon in the ISI.

10.5.1. Within AETC, open areas are defined as an area where the weapon can be effectively employed without the potential to cause injury or damage in surrounding built-up residential or industrial areas. The ISC will determine which areas on the installation meet these requirements.

10.5.3. Body armor, helmets, and protective masks should be readily available on post during THREATCON BRAVO or higher. The equipment will be worn on the person during THREATCON CHARLIE or DELTA unless determined otherwise by the installation commander.

10.6. On-duty support forces will be armed and equipped as determined by the ISC.

11.2.7. The ISC will designate in the ISP an alternate arming point with at least 10 percent of the weapons needed to support installation security forces during contingencies.

11.7. Maintain a clear zone of 20 feet outside and 10 feet inside the boundary for PL3 resources that are not upgraded during contingencies. Do not park vehicles or aircraft generation equipment (AGE) in clear zones.

11.7.2. For restricted areas, in or around operational flying missions, limit vegetation growth to eight inches.

11.9.4.2. Security forces need to know the location and operation of all area lighting systems and have immediate access to them. Ballpark lighting, supplemented by hanger lights and portable light-all units, suffice for mass parking areas and maintenance docks. Lighting is also needed around maintenance complexes housing aircraft, transient-parking areas, and overflow parking areas outside restricted areas. Design lighting to enhance flight line surveillance closed circuit television (CCTV) systems.

11.11.1.3. AFVA 31-206, *Military Working Dog Notice*, will be used at all AETC bases. There is no further need for units to obtain MAJCOM approval prior to posting the signs.

11.11.2.3. AFVA 31-206 will be used at all AETC bases. There is no further need for units to obtain MAJCOM approval prior to posting the signs.

11.13. ISC identifies alternate power supply requirements in the ISP.

11.14. For AETC bases with areas containing protection level resources, paragraph 11.14.1.1 through 11.14.2 are mandatory.

11.15. Develop procedures for documenting results and corrective actions for discrepancies. Incorporate procedures in local directives and operating instructions.

12.2.2.2. Document these procedures in local directives and operating instructions.

12.4.6. Within AETC the Pd rates for PL3 are the same as those listed in paragraph 12.4.5.

12.17.4.3. IDS maintenance personnel must respond to IDS failures in areas supporting PL3 resources no later than the next duty day.

13.2. AETC units will provide HQ AETC/SFP a list of all C2 through C4 resources designated PL1, 2, and 3, initially NLT 30 days after release of this supplement, and annually NLT 15 January of each calendar year.

13.6.3. For PL3 off-base facilities, limit vegetation growth to eight inches.

13.6.4.2. Use type I or II secondary padlocks. Owner and user personnel will specify key control procedures in local operating instructions.

13.6.6. PL3 facilities require the same protection requirements identified in paragraphs 13.6.6 through 13.6.6.2.

14.4.5. In AETC, aircraft on alert status will be provided security as identified in paragraphs 14.4.5.1 through 14.4.5.4.2.

14.5.3.3.1. Due to size and number of aircraft assigned, Little Rock AFB and Luke AFB are authorized an additional internal SRT.

14.5.5. Support forces will perform additional duties as determined by ISC.

14.6.2.1. (Added)(AETC) Park transient priority aircraft in existing restricted areas. When not possible, establish a temporary restricted area, and delineate the area with a raised boundary and appropriate warning signs. Consolidate temporary areas where possible. Protect these areas with flight line patrols armed with the appropriate weapons.

14.6.2.2. (Added)(AETC) At installations without permanent restricted areas, park transient priority aircraft in the mission support aircraft parking area or as close as possible, taking advantage of existing patrols. Establish a temporary restricted area and delineate the area with a raised boundary and appropriate warning signs. When selecting locations, keep response times in mind.

14.8.1. AETC/SF units will implement the procedures outlined in paragraph 14.8.3.1 through 14.8.3.5. Document procedures in the local ISI/ISP.

16.8.2. Operating installations will address unique security procedures in the ISI.

19.2.4.7. (Added)(AETC) A copy of approved deviations.

19.2.5. (Added)(AETC) Community policing involves personnel on an installation working together to engage the community in a cooperative effort to fight crime. Use AETC Form 395, **Quarters/Vehicle Security Check**, to document requests for courtesy checks of vehicles and quarters. Use AETC Form 1021, **Project Ride Along Application**, to document requests to observe patrol activities.

20.5. The installation chief, security forces, ensures commercially procured intrusion detection equipment (IDE) (new system or system upgrade/enhancements) contains a maintenance requirement for the IDE before approving any system or component purchase. Additionally, the AWG ensures specific information is included in the proposal on how the installation will fund the purchase, installation, training, and maintenance of the alarm system before the system is procured. All agencies acquiring, replacing, or upgrading IDE must coordinate with the installation security resource protection program manager (RPPM), local communications squadron, and civil engineer.

20.5.1.8. (Added)(AETC) Configure alarm sensors to detect entrance through logical avenues of approach. For example, in a room containing major funds, infrared coverage on doors, windows, and safes is ample coverage. Alarm the protected resource if possible and cost effective.

20.5.4. Alarm monitors at the primary and alternate (when activated) security forces control center (SFCC), for PL4 resources, will be armed.

20.5.12. Memorandum or a computer-generated product may identify authorized personnel receipting for codes.

21.3.1. Use AETC Form 1015, **Security Forces Building Checklist**, to document building security checks.

22.2.5.5. Within AETC, all law enforcement desks (LED) will be designated as controlled areas due to their mission essential communication status.

★23.1.1. Use the AF Form 1473, **Gun Equipment Room Inventory**, for armories. This form may be overprinted for local requirements.

23.1.3. Personnel possessing firearms must comply with all federal, state, and local laws, ordinances, and military rules on registering and bearing firearms. The ISC will establish procedures for authorized storage locations and transportation of firearms. Procedures for carrying concealed firearms must be coordinated through the local staff judge advocate office.

23.1.5. Ensure facilities meet construction criteria and alarm coverage. Document this information in the activity's resource protection (RP) folder.

★23.1.6. Personnel authorized to open armories must be armed before entering the facility or immediately after entering the facility.

★23.3.2.4. Facilities housing only Category III or IV arms, ammunition, and explosives (AA&E) are not required to have IDE. The ISC will determine who conducts nonduty hour checks and will publish this requirement in the installation security plan (ISP).

23.3.2.6.5. Unless continuously guarded, gates shall be secured with low security padlocks meeting commercial item description (CID) A-A-1927. Locks assigned national stock number (NSN) 5340-00-158-3805, NSN 5340-00-158-3807, NSN 5340-01-408-8434, or NSN 5340-01-269-9345 meet this CID.

★23.3.3.8. There is no IDE requirement for Category III and IV storage structures and containers. The ISC will determine who conducts nonduty hour checks and will publish this requirement in the ISP.

23.4.1. A significant incident of loss or attempted theft is also defined in DoD 5100.76-M, *Physical Security of Sensitive Arms, Ammunition, and Explosives*.

23.11.2. The reporting period is by calendar year and reports must be received at HQ AETC/SF no later than 7 January each year.

23.11.3. (Added)(AETC) Within 24 hours of being notified, AETC units will provide HQ AETC/SFP a copy of the message or message confirmation report to the National Crime Information Center (NCIC), and the Bureau of Alcohol, Tobacco and Firearms (ATF), Intelligence Division regarding confirmed thefts, losses, and recoveries of DoD arms.

24.1.1. (Added)(AETC) Bases supporting basic and/or advanced trainer or permanent mission support aircraft must have continuous security forces patrol coverage on the flight line and maintain an assured security force response. Flight lines and associated hangars on these installations will be identified as sectors that require a continuous installation security force patrol.

24.1.2. (Added)(AETC) The ISC will establish procedures for protecting aircraft at auxiliary fields. The installation should survey its most frequently used auxiliary fields and establish protection based on the threat, distance from base, staffing of the auxiliary field after duty hours, hangar facilities, and availability of local police. If local police are involved in protection, wings should develop appropriate memorandums of agreement addressing their coverage and response. When military protection is required, consider use of reserve augmentation duty (READY) personnel.

25.3.3. (Added)(AETC) Frequent transfer of small amounts of funds between the activity and a secure storage facility by an owner or user reduces the threat of theft, reduces the need for armed escorts, and ensures funds will not exceed maximum storage limitations.

25.4.3. (Added)(AETC) Automated Teller Machines (ATM). The ISC determines resource protection standards and procedures for ATMs operated on base. These ATMs must meet state regulations governing ATMs, as applicable.

25.4.4. (Added)(AETC) Protecting Air Force Recruiting Service (AFRS) and Air Force Officer Accession and Training Schools (AFOATS). Recruiting Service and HQ AFOATS commanders determine protection required for all subordinate units.

26.6.18. (Added)(AETC) AETC Forms 395, 1015 and 1021.

RICHARD K. ELDARD, Colonel, USAF
Director of Security Forces

2 Attachments (Added)(AETC)

15. Resource Protection Folder Requirements

16. IC 2001-1

Attachment 15**RESOURCE PROTECTION FOLDER REQUIREMENTS**

A15.1. Folder Requirements. The resource protection monitor prepares and maintains a resource protection folder for each facility that falls under the base resource protection program. The folder serves as a management tool and single point of reference for all resource protection documents, issues, questions, or problems affecting a facility. As a minimum, each folder must contain the following:

A15.1.1. All initial, followup, and special program reviews.

A15.1.2. Diagram of the facility showing locations of protected resources and sensors.

A15.1.3. Copy of the most recent staff assistance visit.

A15.1.4. Annual self-assessments, if applicable.

A15.1.5. Appointment memorandums for funds custodians, munitions/weapons custodians, and controlled area monitors.

A15.1.6. Copy of the controlled area entry authority list (EAL).

A15.1.7. Authorization memorandum to store funds and firearms.

A15.1.8. Memorandums designating the storage of munitions and storage limits.

A15.1.9. Controlled area designation memorandum.

A15.1.10. Current waivers and/or exceptions.

A15.1.11. Record of all resource protection and controlled area training.

A15.1.12. Most current resource protection operating instruction or other installation instruction.

A15.1.13. Copy of facility initial survey.

A15.1.14. Copy of anti-robbery exercise documentation.

Attachment 16**IC 2001-1****IC 01-1 TO AFI 31-101/AETC SUP 1, *THE AIR FORCE INSTALLATION SECURITY PROGRAM*, 13 DECEMBER 2000****3 APRIL 2001****★SUMMARY OF REVISIONS**

This change incorporates interim change (IC) 2001-1 which deletes the requirement for munitions storage facilities to use the AF Form 1473 (paragraph 23.1.1); changes the requirement for all personnel authorized to open AA&E facilities to be armed (paragraph 23.1.6); changes the requirement for Category III and IV facilities to have intrusion detection equipment (IDE) (paragraph 23.3.2.4); and adds guidance on IDE for Category III and IV storage structures and containers (paragraph 23.3.3.8). See the last attachment of this publication for the complete IC. A ★ indicates revision from the previous edition.

★23.1.1. Use the AF Form 1473, **Gun Equipment Room Inventory**, for armories. This form may be overprinted for local requirements.

★23.1.6. Personnel authorized to open armories must be armed before entering the facility or immediately after entering the facility.

★23.3.2.4. Facilities housing only Category III or IV arms, ammunition, and explosives (AA&E) are not required to have IDE. The ISC will determine who conducts nonduty hour checks and will publish this requirement in the installation security plan (ISP).

★23.3.3.8. There is no IDE requirement for Category III and IV storage structures and containers. The ISC will determine who conducts nonduty hour checks and will publish this requirement in the ISP.