BY ORDER OF THE COMMANDER
AIR EDUCATION AND TRAINING
COMMAND

AF INSTRUCTION 31-101

AIR EDUCATION AND TRAINING COMMAND
Supplement 1

4 OCTOBER 2004

Security

THE AIR FORCE INSTALLATION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AETC/ SFPF (SMSgt Alan Houchens)
Supersedes AFI 31-101/AETC Sup 1, 3 April 2001

HQ AETC/SF (Col John Kinsey)
Pages: 33
Distribution: F

AFI 31-101, 1 March 2003, is supplemented as follows:

This supplement is not applicable to the Air National Guard or Air Force Reserve units, 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. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) (available at https://webrims.amc.af.mil).

SUMMARY OF REVISIONS

This revision includes extensive changes and requires complete review. It changes threat condition to force protection condition (FPCON). It refers the reader to AFI 10-245, *Air Force Terrorism (AT) Standards,* and the AETC supplement for guidance concerning AT measures. It outlines the priority designation package (PDP) approval process in Chapter 2. It requires all AETC installations to publish an installation security instruction (ISI), and develop free zone approval processes in Chapter 3. It provides guidance on ISC responsibilities and ISI and installation security plan (ISP) content in Chapter 4. Chapter 6 outlines the approval process for deviations. Chapter 7 requires installations to develop Phase I and II training programs for all personnel working in or around protection level (PL) 4 and above areas. Chapter 8 requires unit orderly rooms to be the focal point for registry of firearms, if applicable, and prohibits the possession or storage of firearms in bachelor living quarters, transient quarters, or billeting. Procedures for completing the AF IMT 2586, **Unescorted Entry Authorization Certificate;** issuance of the AF Forms 1199A, **USAF Restricted Area Badge (Green);** 1199B, **USAF Restricted Area Badge (Pink);** 1199C, **USAF Restricted Area Badge (Yellow);** 1199D, **USAF Restricted Area Badge (Blue);** and use of an Automated Badging System (ABS) are contained in Chapter 9. Chapter 10 contains guidance concerning security response teams in support of PL aircraft and security forces arming and equipment requirements. Chapter 11 provides guidance on physical security requirements for security forces facilities and restricted areas. Intrusion Detection System (IDS) requirements in support of PL3 and above resources is contained in

Chapter 12. Aircraft security to include transient security of PL3 and above aircraft is contained in Chapter 14. Security of sensitive compartmented information facilities to include Headquarters Air Intelligence Agency (AIA) is contained in Chapter 17. Chapters 18 to 26 contain guidance concerning the protection of PL4 resources to include arms, ammunition, and equipment (AA&E); pharmacies, funds, and airfields and mission support aircraft. Attachment 18 (Added)(AETC) mandates implementation of the Flight Line Protection Program (FPP) for AETC installations supporting PL3 aircraft restricted areas.

1.8. Unit Commanders. AETC units located on other MAJCOM and/or other service installations will participate in the host installation Resource Protection Program.

1.9. Installation Chief of Security Forces (CSF). The installation CSF, or designee, coordinates on all statements of work or performance work statements involving base contractor operations or other construction actions in PL4 or above areas before the statement of work (SOW) or performance work statements (PWS) are submitted to the contracting office.

2.2.1. For new systems, HQ AETC program managers are responsible to ensure requested PLs are officially proposed and fiscally supported. AETC/CC is the risk authority for determining fiscal support levels for security of new or existing priority resources. Forward PL designation requests for PL4 resources only (not controlled area designation packages) to HQ AETC/SFO for final coordination. Requests for new, or changes to, PL designations for AETC PL1-3 resources will be completed by the HQ AETC owner and/or user agency, and forwarded to HQ AETC/SF. AETC/CV is the final requesting authority. For resources that belong to tenant organizations, forward requests through AETC/SFO who will then coordinate with the operating/owning MAJCOM.

2.2.1.2. Route PDP requests through HQ AETC/SFO.

2.3. Identifying Protection Level Resources. Facilities not identified in the basic instruction as a PL resource, to include intelligence facilities, must have a HQ USAF/XOF approved PDP in accordance with paragraph 2.2.1.1 to be considered as a PL resource. Keep the approved package on file in the installation security section (ISS). The presence of classified information alone does not warrant protection level designation.

2.7.1.5. A warehouse is considered a structure or facility designed for long-term storage.

2.7.1.7. The ISC will determine what constitutes large volumes.

2.7.1.8. The ISC determines areas that are mission essential.

2.7.1.9. This includes storage and dispensing areas handling controlled substances.

2.8.3.4. The ISC will place the responsibility of supporting forces and entry control procedures for restricted areas in the ISI.

3.3. Installation Security Instructions. All AETC installations will publish an ISI. The ISI must be reviewed annually by the ISC. Forward a copy to HQ AETC/SFO within 30 days of publication.

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

3.4. Restricted Areas. The CSF or designee will be involved during the planning phase of new areas, changes, or construction to existing areas. The CSF or designee will provide security requirements to the contracting office for incorporating into contracts. The contracting office will, in writing, identify the security requirements to project engineers and include requirements in all contracts.

3.4.2.2. During FPCON Charlie or higher, entry control points (ECP) for permanent PL3 and above aircraft areas will be reduced by at least half from lower FPCONs if manned by security forces during contingencies. Reducing ECPs enhances the ability of security forces personnel to detect personnel attempting spurious entry.

3.4.2.4.1. The ISC, in conjunction with airfield management, determines permanent and temporary areas that cannot have elevated barriers due to airfield restrictions. Those areas must have ground markings visible during periods of darkness and reduced visibility. Elevated barriers may include, but are not limited to: type A fencing, stanchions with red rope, restricted area signs, and jersey barriers.

3.5.2.2. AETC security forces units must maintain the capability to rapidly respond to, and contain, the scene of on- and off-base aircraft mishaps. Units with an active runway must maintain an aircraft mishap kit containing sufficient equipment to establish national defense areas (NDA) or restricted areas. Coordinate off-station emergency responses with the local staff judge advocate (SJA).

3.5.3.6. (Added)(AETC) For aircraft mishaps or major incidents requiring a security forces cordon, the on-scene entry controller will have an AF IMT 1109, **Visitor Register Log,** (or equivalent entry control documents); communication capability with the security forces control center (SFCC) (for example, cell phone or land mobile radio [LMR], and special security instructions [SSI]).

3.6.2. The individual appointed to perform crime prevention program monitor duties will attend course WCIP07A, *Resource Protection/Crime Prevention Theory, Practice, and Management,* or, if available, enroll in ECI Course 8100, *USAF Crime Prevention Program,* within 3 months of appointment.

3.6.3.2. The ISS will maintain separate files for controlled areas. The files will contain, as a minimum, those items listed in Attachment 16 (Added)(AETC). When similar controlled areas on the flight line have the same owner and/or user, for example, navigational aid facilities, one folder may be maintained.

3.6.3.5. The CSF will determine what data is relevant to analysis by using the Defense Incident-Based Reporting System (DIBRS) reporting criteria as a starting point.

3.6.4.2. ISC approval of controlled areas will be sufficient when new areas are added between ISI publications. Ensure the approval is in the minutes or other staff package.

3.7. Free Zones for Protection Level 1, 2, and 3 Resources. When a free zone corridor is impractical due to the location of the free zone, owner and/or user personnel will escort workers through the restricted area ECP to the free zone ECP in accordance with chapter 9 of this instruction, as supplemented. In these situations, the free zone entry controller (EC) must have a restricted area badge (RAB). Establish the free zone approval process in the ISI.

3.7.1. The ISC establishes and the installation commander approves free zones. The unit commander or agency chief responsible for the operational resources in the area will coordinate free zone requests with all agencies involved in the project and the CSF. Post the entry authority list (EAL) with the free zone owner and/or user entry controller and the SFCC.

3.7.2.2. Immediate visual assessment (IVA) sentries will possess radios capable of communicating with the SFCC and SSIs developed by the ISS. The SFCC will include the IVA sentries in communication status checks. Security forces patrols will verify required sentries are posted with required equipment and the EAL is posted before approving opening of the free zone.

3.7.2.3. The free zone must be segregated from the restricted area. An elevated free zone boundary must be established with posted restricted area signs visible from inside the free zone.

3.7.2.5. Sweeps will also be conducted for PL3 free zones. Record results of the sweep in the blotter. Ensure owner and/or user sentries are not released until the sweep is complete.

3.8. Free Zones for Protection Level 4 Resources (Controlled Areas). Develop local approval procedures for free zones in areas containing PL4 resources and publish in the ISI.

3.8.1.2. Security forces personnel will not be used as free zone boundary sentries.

4.2. Installation Security Council (ISC). The wing or vice wing commander will chair the ISC. ISC membership will include all group commanders or equivalents. At small sites and operating locations, the senior officer exercising command authority will serve as the chairperson. The ISC will meet semiannually for installations supporting PL1 and 2 resources. ***NOTE:*** Where AETC is the host command and the tenant command's resource is the only PL1 or 2 resources on the installation, the ISC may meet annually depending on host tenant agreements. Installations supporting PL3 resources will meet at least annually. The installation commander will review and approve all ISC minutes. The chairperson may act on behalf of the full committee between ISC meetings. Any actions approved by the chairperson will be reviewed at the next ISC meeting.

4.2.2. The ISC will ensure a local threat assessment is prepared, reviewed, and updated annually.

4.2.4.1. List these areas in the ISI or the ISP. The ISC will not assign a PL3 or above designation to resources or facilities other than those addressed in the basic instruction. For other facilities and resources not listed in the basic instruction, a formal PDP must be submitted in accordance with Chapter 2. When maintenance hangars frequently contain PL1-3 aircraft, designate them as restricted areas when aircraft are present, and delineate the restricted area boundary accordingly. Hangars, in and of themselves, will not be designated a permanent restricted area unless they meet the provisions of Chapter 2.

4.2.4.5. Document annual reviews in the ISC meeting minutes.

4.2.4.6. Document this review in either the ISC meeting minutes or other staff package. The ISC will review corrective actions to ensure progress in eliminating deficiencies.

4.2.5.1. The threat working group (TWG) will be comprised of representatives from security forces, intelligence, and the Air Force Office of Special Investigation. Other representatives will be determined locally. The TWG will review all local and higher headquarters assessments, and if applicable, assess the vulnerability of foreign students attending training on the installation.

4.2.5.2. If required by the ISC, the CSF or designee will chair the alarm working group (AWG). Submit status reports to the ISC for review. The AWG will convene as determined by the CSF. As a minimum, the AWG will meet during the planning, designing, budgeting, and installation of initial and replacement systems. Other meetings are not required unless directed by the ISC. Only systems from the Intrusion Detection System (IDS) approval memorandum, signed by HQ USAF/XOF, will be considered for new and replacement systems.

4.3.1. Establish response times for PL4 resources in the ISI.

4.3.2. The installation CSF, or designee, will publish a post priority chart for each FPCON. Distribution will be limited to the ISC, and as determined locally, within the security forces unit. As a minimum maintain the chart on the SFCC. The chart will list all security forces posts from the highest to the lowest priority, and vehicle and radio priorities. Create a visual aid for the SFCC (base grid map with overlays or markings) reflecting the patrol sectors.

4.3.2.1. (Added)(AETC) Posting in support of protection level resources will be the highest priority.

4.3.2.2. (Added)(AETC) Prior to the deletion of posts required by the post priority chart, delete security forces programs not directly supporting security of protection level resources. Posts for protection level resources will not go unmanned during personnel shortages.

4.3.4. The CSF will direct an annual review of checklists or when there is a change to the reference material.

4.3.5. SSIs will be specific for each post/patrol and will include higher FPCONs or contingency actions. Review SSIs or when there are significant changes in procedures. Operating instructions will not take the place of specific SSIs. At a minimum, SSIs will contain post limits, jurisdiction limits, use of force, post reporting instruction, special instructions, and security deviations with the compensatory measures within the post limits.

4.4. Contingency Security Operations. In accordance with paragraph 3.3, publish normal daily security requirements in the ISI. Document contingency planning in the ISP.

4.5.1.1. The installation commander may approve contingency actions or checklists that require automatic implementation of an FPCON.

4.9. Training Considerations. Contact HQ AETC/SFO prior to requesting assistance of the force protection battle lab.

4.10. Writing and Publishing the Installation Security Plan (ISP). Installations may publish a separate ISP, or combine the ISP and the antiterrorism plan into a consolidated plan. If combined, the requirements of AFI 31-101 and AFI 10-245, *Air Force Antiterrorism Standards,* as supplemented, apply equally. Installations will have 120 days to update their installation security plans upon release of AFI 10-245/AETC Sup 1. Send a copy to HQ AETC/SFP within 30 days of publication. Include HQ AETC/SFP on the distribution list for the ISP and/or the antiterrorism plan.

4.10.2. All AETC installations will have an ISP.

4.10.2.2. If classified, the threat assessment may be published separately directing the reader where to obtain the information. Include a general assessment in the plan. The ISS will maintain a detailed and current assessment. Assessments are an evolving process subject to change. When assessments change, brief the ISC.

4.11. Office of Primary Responsibility (OPR). The CSF is the OPR.

4.12. Installation Security Plan Contingencies. Address the contingencies in paragraphs 4.12.1 through 4.12.13 and 4.12.15 through 4.12.17 of the basic instruction. Additionally, installations will plan for a safe haven (nuclear/nonnuclear), communications failure, a gate runner during increased threats, and installations with an active runway will plan for an emergency landing of a nuclear-logistics aircraft.

5.3.1. AETC tenant units will comply with host-command security reporting and alerting requirements. Security forces will not delay initiation of a HELPING HAND report for incident investigation.

5.3.2. Identify the authority for HELPING HAND termination in the ISI. The SFCC will use a locally approved information management tool (IMT) to log and track HELPING HAND reports. Maintain logs in accordance with AFMAN 37-123.

5.4. COVERED WAGON Reports. COVERED WAGON reports do not have to be preceded by a HELPING HAND report. Submit COVERED WAGON reports when intentional damage occurs to PL1-3 resources regardless of severity (for example, hammering or splashing paint on an aircraft, etc.). Installations will use a locally approved IMT to log COVERED WAGON reports. Maintain logs in accordance with AFMAN 37-123.

5.4.2.1. The ISI will address reporting instructions if the command post is the affected resource and unable to complete the notification. If the affected resource belongs to a tenant unit or is transient, include that information in the report.

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

5.5. Force Protection Condition (FPCON) Reports. The installation commander may delegate FPCON implementing authority via the ISP.

6.1. Overview. The ISC will review deviations annually. Record this review in meeting minutes or other staff package.

6.5.1. Instructions for completing the AF IMT 116, **Request for Deviation from Security Criteria,** are located at Attachment 17 (Added)(AETC).

6.6.1.1. Deviation approval, disapproval, extension, and cancellation authority is delegated to each installation commander. Deviation approval authority for AETC units located on other installations will be in accordance with host MAJCOM directives.

6.6.1.2. Send tenant unit PL1-3 deviations to HQ AETC/SF for coordination prior to approval. HQ AETC/SF will forward deviation requests to the appropriate tenant MAJCOM for coordination.

6.6.2. Forward a copy of approved PL1-3 deviations to HQ AETC/SFO within 30 days of approval. The local security forces will notify HQ AETC/SFO when deviations are cancelled.

6.7.1. The standard must have a specific numerical requirement that is measurable (for example, feet, inches, etc.) to be considered for this exception.

6.8. Reporting Deviations for PL 1, 2, and 3 Resources. Deviations for PL4 resources will be accomplished and approved in accordance with Attachment 17 (Added)(AETC). Units will submit annual PL1-3 deviation reports electronically to HQ AETC/SFO no later than 15 January of each year. (The reporting requirement in this paragraph is exempt from licensing in accordance with AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections,* paragraph 2.11.12.)

6.9. Compensating for Deviations. Compensatory measures must be implemented immediately upon detection of vulnerability. Do not wait for the installation commander to approve the deviation request. Formal deviations are not required for temporary conditions. For example, if weather (floods, snow, etc.) creates unacceptable security conditions (SRT cannot maintain required response times). Temporary compensatory measures are required.

6.9.1. Posted security forces personnel must be made aware of PL1-3 deviations and compensatory measures affecting the area in which they are posted. List deviations and compensatory measures in SSIs.

7.2.1. As a minimum, AETC installations possessing or supporting protection level resources will develop Phase I and Phase II training programs. Identify participating units in the ISI. The CSF will develop Phase I and Phase II lesson plans and distribute it to unit training officials. The unit trainer must develop tailored lesson plans to specific work centers duties and as a minimum, must include: information on threats to protection level resources; as applicable, security procedures for restricted and controlled areas; and duress words and authentication procedures. Unit training officials will conduct Phase I and II with all personnel who work with or around protection level resources. A primary security education coordinator must be identified from each unit; this duty may be performed by the unit security manager.

7.2.2. This phase is initial training for newly assigned personnel and will be conducted within 30 days of assignment and/or prior to an individual performing their assigned duties inside PL1 to PL4 areas.

7.2.2.2. The installation CSF will develop a standard physical security awareness test of at least 25 questions to be administered during Phase I and Phase II training before granting unescorted entry into a PL1 to PL4 area. Tests will be reviewed annually. Minimum passing score is 80 percent. Remedial training will be conducted on individuals not attaining a score of 80 percent.

7.2.3. Phase II training is annual recurring training. The requirement for recurring detection exercises is through a viable FPP in accordance with Attachment 18 (Added)(AETC) and/or a resource protection program.

7.2.4.1. Refer to AFI 36-2225/AETC Sup 1, *Security Forces Training and Standardization Evaluation Programs,* for requirements. The ISC will determine local training requirements and publish them in the ISI.

7.2.4.4. Documentation requirements will be determined locally and published in the ISI. Maintain only the most current phase of training.

7.3. Security Forces Training. All distance learning training will be completed prior to progressing to Phase I training.

7.4.2. Refer to AETCI 10-205, *AETC Exercise Program.* During any exercise, the mixing of live ammunition with blank ammunition is strictly prohibited.

7.5. Inspections. Inspection procedures can be found in AFI 90-201, *Inspector General Activities,* as supplemented.

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

8.4. Installation Designation. The installation commander determines the designation based on paragraphs 8.4.1 and 8.4.2 of the basic instruction.

8.5. Installation Entry Points (Gates). During periods of increased operations tempo, consider closing convenience gates, or consider replacing security forces entry controllers with personnel trained in installation entry procedures.

8.5.2. When special purpose gates are not being used, security forces will maintain the keys. The ISC will determine the need to arm individuals posted at special purpose gates.

8.6. Gate Closure Procedures. Publish gate closure procedures in the ISP or ISI, SSIs, and unit operating instructions. Gates will be closed during actual COVERED WAGON incidents. Installations must have the capability to close entry and exit points with a well-marked physical barrier.

8.7. Random Installation Entry Point Checks. Entry point checks include identifying unauthorized removal of classified information according to DoD 5200.1-R, *Information Security Program,* Chapter 5. The schedule of checks will be protected from compromise. Security forces personnel conducting entry point checks must not have discretion to select vehicles.

8.7.1. The SJA will review the program for legal sufficiency at least annually.

8.7.2. Maintain the documentation of the installation entry checks for at least 1 year.

8.7.3. (Added)(AETC) Couriers. Personnel transporting classified material on or off the installation must have an authorization memorandum from the unit commander and/or a DD Form 2501, **Courier Authorization**, and an exemption notice from inspection memorandum. The vehicle will still be inspected, but the classified material container will not be inspected.

8.9.2. Maintain barred and driver's revocation lists at installation entry points and the visitor control center. This list may be computerized. When issuing visitor passes, or while conducting entry point checks, the EC will check the individual's name against the lists.

8.12.2.1. If required by the installation commander, unit orderly rooms will be the focal point for registry, and will ensure that one copy of the AF IMT 1314, **Firearms Registration,** is maintained in the orderly room and one copy is forwarded to the security forces armory. The security forces armory will maintain a master listing of registered firearms with names and locations, and provide these listings to the security forces control center on a locally determined basis. If the installation commander requires privately owned weapon registration, enter the information into SFMIS.

8.12.2.2. The possession or storage of firearms is specifically prohibited in bachelor living quarters, transient quarters, and billeting. Store ammunition in accordance with AFMAN 91-201, *Explosives Safety Standards.* The storage of cases, covers, boxes, and nonfirearm-type items such as bows, arrows, swords, knives, scopes, martial arts weapons, etc., in the security forces armory is prohibited. Commanders, first sergeants, and dormitory managers will establish areas or rooms within dormitory areas for nonfirearm weapon storage.

8.12.2.2.1. (Added)(AETC) Installation commanders will develop policies and procedures regarding storage of firearms in government housing. At a minimum, secure firearms in a locked container, or equipped with a tamper resistant mechanical lock, or other safety device. Mechanical locks or other safety devices will be properly engaged.

8.12.2.2.2. (Added)(AETC) Firearms stored in locking gun cabinets constructed with glass windows must have an additional level of security in place (for example, trigger locks, wire mesh, etc.). Keys and combinations will be closely controlled to prevent access by children and other unauthorized users.

8.12.2.2.3. (Added)(AETC) Installation commanders will develop an awareness program to familiarize off-base personnel with the dangers of child access to firearms.

9.2. Authorizing Unescorted Entry for Restricted Areas. The AF Forms 1199A, 1199B, 1199C, or 1199D, or a badge produced from an approved ABS or SFMIS, is required for unescorted entry to restricted areas. When SFMIS is capable of producing RABs, during the next normal badge reissuing process, units will use SFMIS to produce RABs.

9.2.2. Pen and ink changes are not authorized on the AF IMT 2586.

9.2.2.1. Granting unescorted entry and escort authority is a formal process. Installation commanders must strictly limit approval authority. The installation commander may only delegate approval authority to commissioned officers or DoD civilian-equivalent designees serving in positions with direct responsibility for the restricted area. The CSF may grant unescorted entry for security forces augmentee personnel. Unescorted entry and escort authority is granted when the appropriate approval authority signs Section IV of the AF IMT 2586 for their respective restricted area. When two or more organizations have priority resources within the same restricted area, approval is required from only one of the approval officials. Personnel designated to sign Section II of the AF IMT 2586 may also be designated to sign Section IV for unit-owned restricted areas. However, the same individual will not sign both sections on any one IMT.

9.2.2.1.1. (Added)(AETC) Tenant commanders with direct responsibility for priority resources located in restricted areas may be designated as approval authority to sign Section IV. The command post chief may be designated for the wing command post. Wing directors of staff may approve unescorted entry (escort authority) for the command post in the absence of the command post chief.

9.2.2.1.2. (Added)(AETC) Individuals designated by the installation commander cannot delegate their authority lower. In instances when a squadron commander is unavailable because of TDY, leave, or hospitalization, the acting commander may temporarily serve as the approving official.

9.2.2.6. (Added)(AETC) Unit trainers will forward documentation of completed Phase I training to the official authorized to sign Section II of the AF IMT 2586. Prior to the approving official signing Section IV of the AF IMT 2586 granting unescorted entry into PL1 to PL3 areas, Section III of the AF IMT 2586 will have the following statement: “The above named individual completed security education and training on (list the date completed). Approving officials will not sign section IV granting unescorted entry without this statement. An AF IMT 2586 accomplished prior to the date of this publication is not required to be reaccomplished for the sole purpose of adding this statement.

9.2.4. As a minimum, keep the original AF IMT 2586 on file at the requesting organization in accordance with paragraph 9.2.5. Locally determine the number of other copies, if any, required to meet operational requirements. In the event of a lost original AF IMT 2586, the replacement IMT will reflect all required data including completion of Section IV. New AF Forms 1199A, 1199B, 1199C, or 1199D need not be issued unless a change in data occurs.

9.2.5. The badge-issuing activity will document destruction of the badge in accordance with paragraph 9.5.3.3 and on the AF IMT 2586. Return the AF IMT 2586 to the requesting unit.

9.2.7. The approval authority will establish written procedures to immediately take custody of badges when an individual's authority for unescorted entry or escort authority has been permanently or temporarily revoked. Support agreements and contracts will include procedures to retrieve RABs for tenant units or civilian personnel.

9.4.1. The characteristics of an ABS badge will include a photograph and signature of the badge holder. The signature of the issuing official is not required if the ABS has a secure method to determine who issued the badge (for example, user ID and password system). The ABS must have the ability to sequentially number badges including those destroyed due to errors. Numbers will not be reused and the system must be secured from operators having the ability to alter the numbering system. Due to the migration to SFMIS technology, a deviation is not required for ABS purchased prior to March 2003 that does not meet the badge color scheme and size requirements of the basic instruction.

9.4.2. Do not account for completely blank forms (such as blank credit card stock or paper) used with an ABS. Physically secure ABS when not in use. The ABS should have a removable hard drive that can be secured when not in use.

9.4.3. Issue only one basic RAB to an individual. If an individual requires unescorted entry to perform duties for two different agencies, request additional open areas through the organization responsible for the area. The badge-issuing activity will verify the identity of the individual applying for unescorted entry through picture identification cards or other methods. When augmentation program personnel are issued a badge solely to perform security forces duties, the security forces unit will maintain the badge and issue it during the individual's assignment to the security forces unit. Establish procedures to ensure RABs are issued for the duration of duty, and recovered before releasing the individual at the end of the tour.

9.4.3.1.1. Enter unit of assignment (Unit) in Column D under "NAME AND RELATIONSHIP."

9.4.3.1.3. Each area will have a specific number designated. Document this designation in the ISI.

9.4.3.1.4. The on-duty security forces must be aware of the locally devised authentication feature.

9.4.3.1.5.3. Existing ABS that place the “E” next to the open area where escort is authorized meet the intent of the basic instruction and do not require modification. Design new systems to meet the requirements, as outlined in the basic instruction.

9.4.3.4. (Added)(AETC) Unit Air Force Reserve coordinators will maintain all badges issued to reserve personnel assigned to their unit. The coordinator will establish procedures to ensure RABs are issued for the duration of duty and recovered before releasing the individual at the end of the tour. Stored badges must be kept secured with limited access.

9.4.4. Adding escort authority requires a new entry along with the coordinating/approving official's signature in block IV.

9.4.5.2.2. For ABS, a new badge number must be generated during reissue. The same badge number will not be used.

9.4.7.2. For ABS, a new badge number must be generated during reissue. The same badge number will not be used.

9.4.7.4. The ISC will establish a maximum loss rate and publish it in the ISI. When computing loss rates, do not count badges turned in for destruction as being in issue.

9.4.8. (Added)(AETC) Master Entry Authority List (MEAL). Installations supporting PL3 or above resources will prepare a MEAL monthly and maintain it at the pass and registration section and the SFCC. As a minimum, the MEAL will reflect RAB numbers, the full name of the individual issued to, and the unit of assignment. Units may update and transmit the MEAL electronically between pass and registration and the SFCC. Coordinate with the local computer security office to ensure protection of the master restricted area badge list (MRABL) while in the local area network. When not located in continuously manned work centers, secure these listings in a locked container during nonduty hours. Maintain MEALs in accordance with AFMAN 37-123. Units using the SFMIS RAB will use the SFMIS generated MEAL.

9.4.8.1. (Added)(AETC) The MEAL may be used as a supporting technique for the single-badge system.

9.4.8.2. (Added)(AETC) If installations use the MEAL as an EAL with a single badge system, it must include the last six numbers of the SSN, the badge-issuing agency must perform daily updates, and it must be authenticated in accordance with paragraph 9.10, as supplemented.

9.5. Inventorying, Auditing, and Disposing of RABs. If used, generate the automated issuance/destruction log at the end of each duty day and file in the same manner as the AF IMT 335, **Issuance Record-Accountability Identification Card.** This log will contain the following information on all badges destroyed: serial number, date of destruction, and signature of an authorized destruction official. Use the AF IMT 335 or other automated log if the ABS is incapable of producing an automated issuance/destruction log.

9.5.2. For ABS, issuing officials will use the history log and issuance/destruction log, if applicable. ABS must have the capability to produce a history record, to include issued and deleted badges, over a requested period. Inventory officials may use this log in lieu of the AF IMT 335, comparing it against the issuance/destruction log.

9.5.2.1. (Added)(AETC) Unit security managers will conduct a physical inventory of all badges issued to unit personnel annually and forward the results to the badge issuing agency.

9.5.3. Publish badge turn-in procedures in the ISI. Personnel remaining on station, but permanently changing to a new unit, will surrender their badge to the issuing activity. If they require unescorted entry into restricted areas in their new unit, the new requesting official will accomplish a new AF IMT 2586. At no time will an individual retain a badge from their previous unit. Unit security managers will ensure unit out-processing checklist includes surrendering of badges.

9.5.3.1. Inform the badge issuing authority when an individual has had unescorted entry authority permanently withdrawn. The badge-issuing authority destroys the AF IMT 2586 along with the badge.

9.5.3.3. Include voided badges due to issuing errors. Destroy badges by the end of the duty day to preclude theft prior to destruction. Record printed and then destroyed badges.

9.6. Temporary Badging Systems for Restricted Area Badges. Temporary badge systems may be used at the discretion of the installation commander. Only issue temporary badges to individuals who have a recurring need to enter restricted areas to perform official duties, who are not assigned to the installation, and who cannot be issued a badge from home station (for example, other service members TDY for a joint exercise). If used, temporary badge systems allow unescorted entry to authorized personnel for a short period of time, not to exceed 90 days. Do not mass issue temporary badges for convenience. The commander of the sponsoring unit will ensure all personnel requiring unescorted entry have fulfilled all the investigative requirements in paragraph 9.2.1. The commander of the sponsoring unit will validate the recurring need for individuals to enter a restricted area via an EAL. Forward EALs to the CSF in accordance with paragraph 9.10. The sponsoring unit will brief personnel on entry requirements before issuing temporary badges. Personnel with temporary badges will not act as escorts.

9.6.1. Use the same series AF Forms 1199A, 1199B, 1199C, or 1199D in use for the installation, and 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. For accountability, individually number the badge. The badge issuing authority will maintain badges when they are not issued to the sponsoring unit. Sponsoring units will return issued badges for accountability within one duty day following the mission that required their use. Approved ABSs may also be used to create temporary badges with a photograph of the bearer. Cleary identify ABS badges as temporary badges and destroy upon completion of the mission that required their use.

9.6.2. Temporary badges may be issued to the sponsoring agency based on an approved EAL.

9.6.2.2. Security forces units will develop procedures to ensure sponsoring agencies maintain strict accountability of badges. Sponsoring agencies will investigate lost temporary badges and provide a report of their findings to the badge issuing authority. Security forces patrols will conduct random checks of individuals with temporary badges using a properly authenticated EAL against photo identification.

9.7.2. Periodically man and control entry to PL3 ECPs, and conduct ramp sweeps of aircraft restricted areas. The ISC will determine the frequency and duration which will be outlined in SSIs.

9.7.4. Allow for variations in the weight between an individual's ID card and RAB.

9.7.5. When worn, the RAB will be exposed on the outermost garment and worn above the waist. Installations may approve arm band devices or other means to secure the badge during flight line operations. The RAB must be visible at all times while inside restricted areas.

9.7.6. Drivers or escorts of vehicles entering manned ECPs to restricted areas will attest that the vehicle has been inspected prior to entry to the area. Vehicle operators will inspect vehicles prior to entering any restricted area.

9.7.7. For unmanned PL3 aircraft parking area ECPs, the sponsoring unit, prior to allowing entry into restricted areas, must search contractor and delivery vehicles. Civilian delivery vehicles will not be authorized escorted or unescorted entry into PL4 and above areas for the purpose of scheduled or unscheduled delivery of personal items (for example, food, beverages, etc.). Personnel will exit the area to receipt for deliveries and will search the item prior to reentering the area.

9.7.8. The CSF will publish the duress codes designating the codes as For Official Use Only, and develop local procedures for control and use of the primary and alternate codes. Do not use the actual codes for exercises.

9.7.8.1. All permanently assigned personnel authorized unescorted entry into PL3 and above areas will know the local duress code and how to use it. Establish procedures to change to an alternate duress code should the primary code be compromised. The ISC will determine the need for TDY personnel to know the duress code.

9.7.9. Using either the sign and countersign or code word is only required at manned ECPs. The sign and countersign requires verbal or physical interaction between the individual desiring entry and the EC. Establish procedures to change to an alternate sign and countersign should the primary numbers be compromised.

9.7.11. Publish emergency entry procedures in the ISI.

9.7.11.2. Pre-warning will include the number of vehicles and number of personnel responding.

9.7.11.4. Conduct a sweep of the affected area and route to/from the area to ensure all emergency personnel have departed and no unauthorized personnel or items were left behind.

9.7.12. The ISC will determine, based on available intelligence, if there is a threat of chemical weapons.

9.9. Unescorted Entry to Restricted Areas – Single Badge System. When entry into PL3 areas is controlled, one of the supporting techniques will be used.

9.10. Entry Authority Lists (EALs). Personnel TDY to an AETC installation may be granted unescorted entry into restricted areas if supported by an authenticated EAL and a home station RAB. The commander or person in charge of the TDY element must provide written notification to the installation commander or designated representative (normally the commander of the unit to be visited). The notification may be used as an EAL in support of single-badge systems if it contains all information required by paragraph 9.10.2. Destroy EALs when the visit is complete, or when no longer needed. Transient US military crew members will use their home station RAB and a supporting EAL, or crew orders, to establish authority to enter the restricted area, or escort as required. The ISI will establish procedures for providing EALs to the security forces. An EAL is only required for unescorted entry into PL3 and above areas. For unescorted entry into PL4 areas, refer to paragraph 9.16.

9.10.1. The security forces supervisor or higher authority authenticates the 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. The installation commander or designee may approve visits to restricted areas by US citizens, and local or regional news media without further coordination or approval.

9.10.2.1. Rank may be listed as ENL (enlisted), OFF (officer), CIV (government civilian employee), or CON (contractor) as reflected on the RAB.

9.10.3. If a memorandum of additions/deletions is attached to the original EAL, annotate the addition on the first page of the EAL with the phrase “see attached changes.” Line through deletions on the EAL and cite the source of the deletion. Pen and ink additions to an EAL are not authorized.

9.11.2. Locally developed escort briefings must be located at all ECPs supporting PL2 and above resources. ECs ensure the escort gives the briefing and it is understood.

9.11.3. For areas containing PL3 resources, any person holding unescorted entry authority may perform as an escort official for that area. No designation of this authority is required on the AF Form 2586 or AF Forms 1199A, 1199B, 1199C, or 1199D. However, areas that will be upgraded to a higher PL during contingencies will have designated escort officials. Escorts will not further delegate escort duties. Installations with manned PL3 and above restricted areas will establish search procedures for hand carried possessions of escorted personnel. Search procedures will be completed by the escort official. Escort officials determine the need for bringing hand carried items into PL1 and PL2 areas. If security forces have confiscated a RAB due to the badge being unserviceable, the individual may be escorted into the area pending reissue of a new RAB. Personnel who have forgotten their RAB will not be escorted. The individual must retrieve their badge prior to entering the area. The purpose is to ensure that personnel cannot circumvent the commander’s withdrawal of unescorted entry.

9.12. Visiting Restricted Areas. DoD personnel TDY may be granted unescorted entry in accordance with paragraph 9.10. The term visitor applies to all personnel who require escorted entry and are not assigned or attached via TDY orders to the installation. Military dependents are not considered assigned to the installation and are considered a visitor. Process visitors in accordance with paragraph 9.12.2. During FPCON Bravo or higher, the approval authority for visits to restricted areas is the installation commander. Visits to restricted areas must be reduced in FPCON Bravo, and completely eliminated in FPCON Charlie or higher.

9.12.1.1. Publish the local policy on official and unofficial photography procedures in the ISI.

9.12.2. The ISC will prescribe search policies for visitors in the ISI.

9.12.2.2. Upon arrival of the visitor at PL2 and above restricted area ECPs, the escort official and the visitor will be separated by a minimum of 10 feet until the EC verifies that no duress exists. The escort official, assisted by the EC, will ensure positive identification is established using two forms of ID (one containing a picture, if possible) and complete the AF Form 1109. The escort official will provide all escorted personnel an escort briefing in accordance with paragraph 9.11.2. In the case of visits involving large numbers of people or distinguished visitors, ID verification can take place at another location by the escort and a security forces member, provided escort procedures preclude anyone from joining the group after identification is complete. In this case, the security force member involved with the identification remains with the group and attests to the EC that positive identification has been accomplished.

9.13. AETCS Requirements for Restricted and Controlled Areas. Forward requests for Automated Entry Control Systems through HQ AETC/SF.

9.16.2. The RAB may be used for entry to controlled areas with the same issuing and use procedures as for restricted areas. Approving officials for controlled areas may be the commander or designee assigned to the unit responsible for the area, and designated by position in the ISI. The installation commander or designee will determine the need to use EALs in controlled areas.

10.1. Overview. Qualified security forces personnel will not be used for installation details when posts in support of PL1-3 resources, installation entry control points, and random antiterrorism patrols go unmanned. Base retreat and reveille details should be dispersed to all units on the installation if completed on a daily basis. Security forces patrols must not be assigned responsibility for housing and vehicle lockouts, stray animal control, or school crossing. Develop agreements with local animal control offices to assist with stray animals.

10.2.1. Establish an augmentation program if sufficient 3P0XX personnel are not available to meet FPCONs or contingencies. The number of augmentation program personnel required will be determined locally. Security forces augmentation program personnel will meet 3P031 entry-level requirements in accordance with AFMAN 36-2108, *Airman Classification;* AFI 31-207, *Arming and Use of Force by Air Force Personnel,* and have at least a favorable entrance national agency check. The resources and training flight will conduct augmentation program training. As a minimum, initial training will include use of force, weapons clearing and handling procedures, challenging, communication, and post related duties. Annual training must be conducted to keep augmentation program personnel current on practices and procedures and will include, as a minimum, working six duty days performing security forces duties. Units may use actual or exercise utilization to meet the annual six-day on post training requirement.

10.2.3.2. If security response teams (SRT) can meet response times in accordance with paragraph 10.4.9 for more than one restricted area, a formal security deviation is not required. SSIs and unit operating instructions will outline post limits and responsibilities. If the restricted areas are geographically separated by runways or large areas of terrain, and SRT cannot respond within established times, a dedicated SRT must be posted.

10.3. Support Forces. Include support forces in training and exercise scenarios whenever possible.

10.4.2.3. Record post checks in the security forces blotter.

10.4.5. EC positions for restricted areas containing PL2 and above resources are considered critical duty positions under the unit's standardization evaluation program. The ISC determines if ECs posted inside of enclosed buildings, entryways, and command and control facilities may arm with the M9 in lieu of the M16 or M4.

10.4.9. Units without permanent restricted areas may use police service patrols for security of temporary PL3 restricted areas. When police service patrols serve as both a security response team and a police patrol, they must be armed with the M16 in addition to the M9. In accordance with DoDD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives,* paragraph 4A1(A), the rifle may be locked in a weapons rack inside the vehicle. Permanently affix the rack in the trunk and use a standard padlock to lock. Individually assigned weapons will be drawn prior to guard mount and returned at the end of shift. Units will establish written guidance on when the weapon may be removed from the vehicle, securing the weapon (for example, disabling the automatic trunk release, and security of the vehicle during police services dispatches). Document procedures (for example, in security forces checklists, special security instructions, etc.) to combine patrols before deploying to incidents. Readjust installation patrol sectors to ensure PL response times can be met. Response to PL resources will take precedence over routine patrol duties. For temporary PL2 and above restricted areas, comply with the manpower and armament requirements in Chapter 14.

10.4.9.1. Internal SRTs for aircraft parking areas may also be utilized to respond to PL aircraft parked outside the area, provided response times can be maintained. Internal SRTs posted in internal facilities may be armed with the M9 pistol or M870 as determined by the ISC.

10.4.9.2. External SRTs will not perform duties that may prevent them from meeting the established response times. SSIs will outline post limits.

10.4.10. Mobilized sentries, elevated observers, etc., may more effectively satisfy surveillance requirements. Sentries must be armed in accordance with paragraph 10.5, and may be posted inside, or outside the restricted area boundary barrier.

10.4.13. Alarm monitors are posted in support of IDS used to protect PL4 resources. At the discretion of the CSF, these duties may be combined with SFCC duties into one post. Develop quick reaction checklists to provide step-by-step guidance. Additionally, create a prioritized list for simultaneous alarms.

10.4.14.3. The SFCC will ensure patrols know the location of PL3 and above aircraft parked outside permanent restricted areas.

10.4.16. The CSF must ensure procedures are in place to capture incidents reportable under DIBRS. Identify patrol sectors in the ISI, SSIs, and on an installation grid map located in the SFCC.

10.5. Arming and Equipping Security Forces. Use the Air Force Catalog (AFCAT) 21-209, Volume 1, *Ground Munitions,* for ammunition authorization. Issue all weapons and ammunition at the armory, and do not exchange on post at shift change or post relief. The following personnel may be armed with a sidearm in lieu of the M16 or M4 as determined by the ISC: flight commanders and flight chiefs (when not assigned to a response force [RF]), security forces controller, and RF and EC personnel posted on the interior of a building supporting PL resources.

10.5.1. 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, with no more concern for causing fratricide and significant collateral damage to resources than with the M16 or M4 series rifle. The ISC will determine which areas on the installation meet these requirements addressing safety issues. Consider likely fields of fire, expected approach routes of adversaries, and application of the M249 in semiautomatic and automatic fire modes. Do not store ammunition in a manner that requires the response forces to use tools to gain access. If the ISC determines the installation does not have open areas, deviations are not required. If the ISC determines there is an open area and the unit is unable to meet the armament requirement, a formal deviation in accordance with Chapter 6 is required.

10.5.2. Reflective accoutrements will not be worn by security forces personnel posted in support of PL1 to PL3 resources, or when performing detection or screening roles.

10.5.3. During FPCON Bravo or higher, these items will be available for immediate use. The CSF will specify when body armor must be worn and gas masks strapped on.

10.6. Arming and Equipping Support Forces. Support forces will be armed and equipped as determined by the ISC and addressed in the ISI.

10.7. Security Forces Vehicles. Develop a security forces vehicle priority listing and publish in accordance with paragraph 4.3.2.

10.8. Security Forces Communications Requirements. The security forces armament and equipment section will keep radio maintenance management records to ensure radios are promptly turned in for repair and subsequently returned to operation in a timely manner.

10.8.4. Develop a security forces radio priority list and publish it in accordance with paragraph 4.3.2.

10.8.4.3. Provide one radio per person for SRTs assigned a vehicle that is not equipped with a mobile or mobile-portable radio.

10.8.5.2. Include manual signal techniques in Phase I and II training.

11.2.1.1.10. (Added)(AETC) Command posts designated as a PL3 or above resource will have a duress warning system terminating in the SFCC.

11.2.1.1.11. (Added)(AETC) If supporting PL3 and above resources, the SFCC will have a duress warning system terminating at the command post, or at another fixed security forces position that is always manned by security forces personnel.

11.2.1.2.1. The alarm annunciator panel, aircraft plotting board, and post priority chart must not be within view of the customer service window. If the configuration places this information in view, the customer service window must be tinted or installed with one-way glass to prevent viewing.

11.2.4. ECFs for PL2 and above areas will have duress alarm capabilities annunciating at the SFCC.

11.2.7. The ISC will determine the need for an alternate arming point and the number of weapons needed during contingencies.

11.5. Barriers for Restricted Areas. Fences installed prior to 4 April 1989 do not require a deviation if they do not meet Type A standards.

11.5.4.2. All mounting hardware (bolts, nuts, screws, etc.), will be on the inside (site side) of the fence. Modify exposed mounting hardware on the outside of the fence so it cannot be removed with common hand tools. Consider welding, peening, or other methods.

11.5.4.3. Secure fence ties by twisting (close helix) at least three full twists and cutting the remaining wire off. Twists will be located on the inside (site side) of the fence. Do not use clip-type fasteners. If the fence has sensors, the fence ties will comply with the spacing requirements outlined in the sensor system siting criteria. If the fence does not have sensors, the intervals on fence posts will be no greater than 15 inches. Intervals will be no greater than 24 inches on top/bottom rails or tension wire.

11.5.5. Secure the outrigger arms or taut wire sensor arms to the fence posts so the arms cannot be easily removed.

11.5.7.1. Use Type II or III secondary padlocks with chains to secure gates with electronic locks that do not fail in the locked position during power outages.

11.5.7.2. Keys for gate locks must be accounted for by owner and/or user personnel for PL3 and below areas, and by the EC at shift change for PL2 and above areas.

11.5.8. When possible, elevate barriers for temporary restricted areas where not prohibited by airfield safety. When airfield restrictions specifically prohibit the use of elevated barriers, the ISC may approve painted red lines with painted ECP and restricted area signs. Mark aircraft mass parking area ECPs as determined locally. Consider vertically displayed signs. Refer to paragraph 14.1.1 (Added)(AETC).

11.5.9.1. When hangars, shelter walls, doors, and roof are used to define the restricted area, all doors, except the designated entry points, will be secured internally. For fenced facilities, if the fence is considered the restricted area boundary, it does not require IDS or close boundary sentries, provided the facility has IDS. Deviations are not required.

11.7. Clear Zones for Restricted Areas. Maintain a clear zone of 20 feet outside and 10 feet inside the boundary for restricted areas containing PL3 resources that are not upgraded during contingencies. Do not store movable items (for example, aerospace ground equipment) temporarily or permanently inside the clear zone. Barriers used to delineate the restricted area boundary do not constitute a clear zone violation. For PL3 and above areas located interior to a facility, there is no clear zone requirement for the exterior of the facility if the room's walls, floor, and ceiling are the boundary.

11.7.1.4. Utility lines that pass over fence lines of protection level restricted areas will be protected in a manner that precludes their use in circumventing fences or sensor systems. If local electrical or communications engineers certify in writing that a utility line cannot be used to circumvent the fence or sensor system, and approved by the ISC, protection measures are not required. File permanently the written certification, and make available for review at a location determined by the CSF.

11.7.2. Limit vegetation growth to eight inches in restricted areas and clear zones, and ensure this requirement in included in maintenance contracts. If the local CES determines plants and shrubs contribute to erosion control, a deviation is not required. In these instances, the CSF will determine the frequency of clear zone checks, and a memorandum from CES will be maintained on file in the ISS.

11.9. Lighting Requirements for Permanent Restricted Areas. Do not procure uninterrupted power supply (UPS) systems for PL2 or above areas, nor replace existing systems. Units relying solely on a UPS system will initiate action to install instant restrike-type lamps as a precaution against UPS failure.

11.9.1. For facilities, boundary lighting can be existing exterior lighting sufficient enough to observe an individual standing against the exterior wall.

11.9.3. Lighting must alleviate blind spots around PL resources mitigating areas of concealment. Use night vision equipment and special purpose lighting to compensate for the loss of area lighting to assist security forces in tracking intruders in restricted areas. If a PL3 or above facility is equipped with IDS, only the area around the resource being protected (the facility) must be illuminated. Parking lots or other facilities within the fenced area do not require lighting. For PL3 aircraft mass parking areas and maintenance docks, lighting similar to ballpark lighting (supplemented where necessary) is sufficient. 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.

11.9.3.1.2. It must allow for the capability to detect intruders in the area.

11.9.3.1.3. Security forces must know the location and operation of all area lighting systems and have immediate access to them. Lighting control boxes and switches will be secured as determined locally.

11.9.3.1.5. Power sources located outside the restricted area may be designated PL4 areas. PL1 to PL3 designation requires a PDP in accordance with Chapter 2.

11.9.4.2. Ballpark lighting, supplemented by hangar lights and portable light-all units, suffice for mass parking areas and maintenance docks. When manned, lighting for entry points for PL3 areas will provide adequate illumination to allow for positive identification of personnel desiring entry to the area. Installations must provide entry point lighting on any manned PL3 ECP.

11.9.5. Installations must plan for the use of special purpose lighting (light all units) on temporary and permanent restricted areas when boundary lighting systems are inoperative or insufficient. If boundary lighting for restricted areas becomes inoperative, equip security forces in support of the area with night vision equipment if the lighting levels warrant use.

11.10. Detection Enhancement Devices (DED). Do not operate in no-light situations simply to employ DED. Employ DEDs in restricted areas to enhance assessment capabilities and to mitigate the loss of normal lighting. If used, personnel must be trained on DED, and the training recorded as determined locally.

11.11. Warning Signs. Consult the local SJA to determine if non-English signs or illiteracy symbols are required.

11.11.1. The location, terrain, and number of entry and approach points determine spacing and placement. Installation perimeter signs should be placed not less than 100 yards apart. Ensure signs are placed conspicuously ensuring an approaching individual will see them.

11.11.1.3. Unless specifically prohibited by state laws, use of AFVA 31-206, **This Area is Patrolled by Military Working Dog Teams (Sign),** is authorized.

11.11.2. Restricted area signs painted on aircraft parking ramps and concrete barriers may be larger, but not smaller, than the size of AFVA 31-107, **Restricted Area Warning Sign 18 x 15.** Comply with all other sign specifications.

11.11.2.3. Unless specifically prohibited by state laws, use of AFVA 31-206 is authorized.

11.12.1. Locks and hasps must be compatible and provide the same level of security.

11.13. Alternate Power Supply Requirements. ISC will determine alternate power requirements in the ISI. The CSF will determine which security forces personnel or posts must be trained on emergency start-up procedures for alternate power supplies for the SFCC.

11.13.1. Automatic switchover is required in permanent PL2 and above restricted areas equipped with boundary or area lighting. Secure generator rooms.

11.13.2. Generators supporting PL3 and above facilities located outside the restricted area are not considered a priority resource unless a formal PDP in accordance with Chapter 2 is approved. Security of generators supporting facilities is an owner and/or user responsibility. The ISC will determine the need to post owner and/or user personnel on facility generators.

11.14. Securing Grills, Grates, and Other Openings. For areas containing PL3 and above resources, comply with the standards in paragraphs 11.14.1.1 through 11.14.2. Openings which pass through or under the boundary barrier, such as drainage culverts, having a cross-sectional area greater than 96 square inches, and a smallest dimension greater than 6.4 inches, shall be secured through use of welded steel grating or similar devices on one end of the opening. Security forces posted in restricted areas must be aware of grills, grates, and other openings within the area. Check openings once per shift.

11.14.1.1. Security forces will maintain keys and account for in accordance with local procedures.

11.14.1.2. Security forces will maintain keys and account for in accordance with local procedures.

11.15. Physical Security Checks. Develop procedures for documenting results and corrective actions for discrepancies. Incorporate procedures in local directives and operating instructions. If the discrepancy creates a security deficiency, implement compensatory measures immediately until corrected. At least once per quarter, the ISS will conduct a physical security check of all permanent PL3 and above areas.

11.16. Lighting Checks. If a lighting discrepancy creates a security deficiency, implement compensatory measures immediately until corrected. At least once per quarter, the ISS will conduct a lighting check of all permanent PL3 and above areas.

12.1. Overview. HQ AETC/SF is responsible for IDS product improvement and replacement. Coordinate all PL1-3 IDS planning and actions with HQ AETC/SF and HQ AETC/SC.

12.2.2.2. Document these procedures in local directives or operating instructions. Brief security forces members on the strength and weaknesses of the installed IDS during unit orientation training.

12.4.6. The PD rate for PL3 lines of detection will be a minimum of .85 at the 90 percent confidence level.

12.4.7.1. Substantially constructed walls and roofs are defined as those meeting or exceeding the delay, denial, and deterrent properties of cinder block construction.

12.4.8.1. Track PL3 and above area nuisance and false alarms each month. Electronic security systems (ESS) NCOs should make every effort to limit false and nuisance alarms. Excessive alarms can lead to operator complacency and loss of faith in the abilities of the system.

12.4.8.1.1.1. Upon receipt of a second false alarm, initiate a work order, and implement compensatory measures as outlined in paragraph 12.4.8.2.

12.4.8.1.1.2. If a fourth nuisance alarm occurs, follow guidance in paragraph 12.4.8.2.

12.4.8.1.2.1. Upon receipt of a second false alarm, initiate a work order, and implement compensatory measures as outlined in paragraph 12.4.8.2.

12.4.8.1.2.2. Upon receipt of a fourth nuisance alarm, follow guidance in paragraph 12.4.8.2.

12.4.8.2. When alarm rates are exceeded, implement compensatory measures to offset security vulnerabilities. In cases where wildlife, vegetation, blowing objects, or environmental factors are the cause, security forces personnel can correct the discrepancy without a maintenance work order. Document compensatory measures in the security forces blotter. Once discrepancies have been corrected, and the alarm is functioning properly after operational test, the false and nuisance alarm count will return to zero.

12.6.1. The IDS must be a closed system. Annunciators, enrollment and/or badging system terminals, system administrator terminal, or any other point must not be connected to a modem with external access. Security forces will monitor and verify contractor software or database maintenance actions.

12.6.5. Protect sensor system and power distribution systems from intentional or inadvertent disruption. Circuit breaker boxes or utility room doors will be locked and key control established by the CSF in writing.

12.6.5.2. The ISC will determine seal requirements. Use of Type II or III secondary padlocks is authorized.

12.8. Alternate Power Supplies. Protect power distribution systems supporting sensor systems from intentional or inadvertent disruption. Do not locate sensor circuit breakers on the exterior of facilities, in utility rooms with external access, or on the area perimeter.

12.8.2. Provide a power failure alarm for all sensors. After all failure alarms are received, a complete sweep of the fence line and inner area is required.

12.10. Immediate Visual Assessment (IVA). IVA may be provided using CCTV or posted sentries. IVA by stationary patrols or nearby posts may be used when CCTV coverage is temporarily affected by environmental conditions (for example, heavy rains, snow, or direct sunlight during sunrise or sunset). IDS for PL3 and above areas must include CCTV coverage for the entire boundary.

12.10.1. New restricted area construction will include interior and exterior patrol roads to facilitate alarm response.

12.12. Certification Test Requirements. Request certification testing via message to HQ AETC/SF. Include areas to be tested. Contact HQ AETC/SFX to determine the certification process based on the system requirement; provide 72-hour checkout, and 30-day test documentation. Maintain test and certification documents until the system is removed, replaced, or modifications are made that require recertification.

12.12.1.2. Testing criteria will be developed by HQ AETC/SF and delegated to the ISC.

12.13.1.7. Include flight chiefs and area supervisors in local training. Prepare sensor system OIs and checklists.

12.13.1.9. (Added)(AETC) Maintain a simple schematic or diagram of all IDS. This schematic or diagram should identify the location of sensors, junction boxes, junction points, transmission lines, and primary and remote annunciators. Ensure these diagrams are classified as required by the appropriate security classification guide. Retain the schematic or diagram where all area security supervisors have access. Security supervisors will use these schematics or diagrams to ensure proper inspection, surveillance, and security of IDS are accomplished. Maintain in accordance with AFMAN 37-123.

12.14. Periodic Test Requirements. Conduct a portion of testing while the annunciator is on battery power. Design testing to ensure the technical order tests are conducted in their entirety.

12.15. Vulnerability (Adversarial) Test Requirements. Record tests on the AF IMT 340, **Sensor Alarm Data,** or annunciator print out.

12.16.1.2. Applies only to the AF IMT 340 and Air Force Technical Order (AFTO) Form 781a, **Maintenance Discrepancy and Work Document.** Develop historical data for the life of the system.

12.17.4. Establish maintenance reporting procedures in the ISI, to include routine and emergency support. When repair of a sensor system is not possible, relocate resources to an alarmed area, if possible.

12.17.4.3. IDS maintenance personnel must respond to IDS failures in areas supporting PL3 resources no later than the next duty day. Immediate maintenance response is required when compensatory measures resulting from IDS failure require additional security manpower.

12.18. Sensor System Compensatory Measures. The CSF will determine compensatory measures. Measures implemented must be designed to provide the capabilities equivalent to those of the failed equipment.

13.2. Identifying Protection Level Resources. Provide a list of all PL3 and above C2 through C4 resources no later than 15 January of each calendar year to HQ AETC/SF. Advise HQ AETC/SFO when resources are added to or removed from an installation.

13.2.1. Designate AETC command posts as the same PL as the highest PL resource they support operationally. A higher PL designation requires a PDP in accordance with Chapter 2. Generators supporting the CP are not assigned a PL3 or higher designation without an approved PDP. In any case, security of generators during contingencies is the responsibility of owner and/or user personnel. Command posts supporting alert missions will have a PL commensurate with the highest priority of the operational alert mission where the command post exercises direct command and control over that mission. Upgrade command post PLs when alert resources are generated.

13.5. Manning Standards. The owner and/or user are responsible for normal security operations for PL3 and below areas and facilities. Entry control, to include during contingencies, is the responsibility of owner and/or user personnel. Post owner and/or user personnel or augmentees when local plans call for additional entry control personnel. Security forces personnel provide an external armed response, and owner and/or user personnel provide an internal response. If the installation commander validates the need for an armed security forces presence during contingencies, it will be in the form of an internal response force. Post security forces personnel only in positions requiring an armed response.

13.5.2. The ISC determines off-base site support requirements and publishes them in the ISI.

13.6.1. Provide Type A fencing for all facilities except when the facility walls, floor, and roof constitute the area boundary. The ISC will determine if a fence is impractical due to terrain, climate, or socio-political sensitivities.

13.6.2. Secure all doorways to prevent entry into or exit from other than established ECPs. Electromechanical locks may be used for entry of authorized personnel.

13.6.3. Owner and/or user personnel are responsible for ensuring vegetation growth is limited to eight inches within the clear zone.

13.6.4.2. Use type I or II secondary padlocks. Owner and/or 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.

14.1.1. (Added)(AETC) Transient Aircraft Security. If the installation has a permanent aircraft restricted area, park USAF aircraft designated a PL3 or above resource in the permanent restricted area. Foreign, civilian, and PL4 aircraft will not be parked in established PL3 and above restricted areas.

14.1.2. (Added)(AETC) Establish and enforce a temporary restricted area around aircraft parked outside a permanent restricted area. Elevated restricted area signs and red rope, or permanently posted or painted restricted area signs will mark the temporary restricted area no further than 30 feet from the aircraft. Permanently posted or painted restricted area signs must state: "Restricted Area When Aircraft Present."

14.1.3. (Added)(AETC) Aircraft should be parked in locations that take advantage of existing patrols. If a transient area is within the response time of existing internal and external SRTs in adjacent areas, the transient area may be included in the patrol's limits.

14.2. Classified Material on Aircraft. Do not use security forces to protect US aircraft based on the presence of classified material alone. Protection of, and access to classified, is an owner and/or user responsibility.

14.3. PL1 Aircraft. See DoD C-5210.41M/AF Sup, *Nuclear Weapon Security Manual* (U), for more guidance on transient nuclear command and control aircraft.

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. Establish a dedicated restricted area, either permanent or temporary, to contain generating aircraft. Conduct a purge of the area immediately prior to establishing a temporary area.

14.4.5.2. Develop strict local entry procedures for alert aircraft not protected by IDS that ensures an equivalent level of security. Comply with SAR directives as required.

14.4.8. Aircraft are considered SCI configured when SCI material is onboard and configured for actual (nontraining) missions.

14.5.3.1. During duty hours, the primary responsibility of security forces personnel is to respond to alarms generated by the owner and/or user personnel.

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.

14.5.5.1. Conduct random entry control point checks for PL3 restricted areas in accordance with paragraph 9.7.2 of this supplement.

14.5.5.3. The ISC will establish procedures for the transfer of security responsibilities between operations and maintenance personnel and security forces personnel. Ensure unattended aircraft hatches, doors, and other access points are secured.

14.6.1.2. Aircraft commanders must prearrange security at the deployed location prior to departure. Refer to AFJI 31-102, *Physical Security,* when USAF aircraft are located on other US military installations. At non-US protected locations, if US military security forces are not available, consult the US embassy assigned to that country to ensure security arrangements are made. When security cannot be arranged at the deployed location, consider canceling the mission, or routing the aircraft to a safer location to remain overnight. During display periods, such as air shows, an aircrew member will remain with the aircraft. At civilian airports and DoD installations, the aircraft commander must know the procedures for requesting civilian and/or military police assistance.

14.6.1.3.2. When PL3 aircraft are temporarily located at civilian airports due to mechanical failure or weather delays, the aircraft commander will arrange for airport security personnel to provide short-term security protection. An aircrew member or US military maintenance personnel will remain with the aircraft at all times, and will be knowledgeable of the method to contact civilian law enforcement for assistance. Home station security forces personnel are not required if the ground time is expected to be less than 24 hours. If the ground time is expected to be greater than 48 hours, the installation commander will determine the necessity of deploying home station security forces personnel. The CSF, after coordination with the SJA, will establish arming and use of force requirements.

14.6.1.3.2.1. (Added) (AETC) When PL2 and above aircraft are away from home station and security is inadequate, home station security forces personnel will be dispatched to protect the resource in accordance with this instruction. Owner and/or user personnel will protect PL4 aircraft, and will not require a security forces presence.

14.7.1.1. The ISI will establish procedures to ensure maintenance personnel notify the SFCC when an aircraft located outside the restricted area resumes PL3 or above mission capable status.

14.7.1.3. Lock unattended hangars; however, security forces patrols must maintain the capability to gain access to hangared PL3 and above aircraft to prevent intentional damage or destruction.

14.8.1. Alert crews and billets are not normally provided security support other than that provided the facility or restricted area in which they are located. Billets should be located in the alert area. Owners and users are responsible for security of billets, to include entry control, if required locally. Security forces will provide emergency response and assistance as determined by the ISC. The ISC prescribes the physical security requirements and procedures for alert crew billets located outside an alert area, to include increased security during FPCONs.

15.3. Presidential Aircraft Security. The Presidential Aircraft liaison officer will determine the posting and armament requirements for the aircraft, fuel, and ground equipment sentries, and response forces.

16.8.2. The ISC will determine any additional or special security measures, and address them in the ISI.

17.1. Overview. For classified storage other than sensitive compartmented information (SCI) facilities, use DoD 5200.1-R, *Information Security Program.*

17.4. Protection Levels. Presence alone of classified material does not determine a protection level designation. Other than the facilities listed in Figure 17.1, accomplish a PL designation request in accordance with Chapter 2.

17.6. Establishing Security Standards. Forward all requests for lesser or more stringent measures for SCIFs located on AETC installations to HQ AETC/SF for review prior to submission to HQ USAF/XOF and HQ USAF/XOI.

17.7. Circulation Control. The ISC will approve entry credentials for PL4 facilities. For PL3 and above facilities located on AETC installations, a RAB is required.

17.9.1.1. The ISC will determine if the SRT will remain inside or outside facilities. Use existing SRTs whenever possible. The two-person response element can be installation police patrols, and the ISC will determine response times.

17.9.1.1.1. (Added)(AETC) To include HQ Air Intelligence Agency (AIA), controlling access to SCI areas is an owner and/or user responsibility not to be performed by security forces personnel. Use security forces personnel to control entry into PL2 and above restricted area boundaries, and do not use to control access to offices, hallways, or buildings interior to the restricted area boundary. If required, implemented interior circulation control measures conducted within the restricted area boundary will be performed by owner and/or user personnel.

17.9.1.2. Security forces will not perform entry control for PL3 facilities on a routine basis. The owner and/or user personnel will provide entry and circulation control.

17.9.1.3. Security forces provide response elements only. Owner and/or user provide entry and circulation control.

17.9.3.2. For HQ AIA, the exterior fence does not require sensors since required facilities are protected by IDS in accordance with DCID 1/21. Deviations and enacting compensatory measures for a lack of sensors on the fence is not required. Surveillance assessment and tracking technology may be employed at the exterior of the facility or exterior fences and perimeters as an enhancement. These enhancements do not require MAJCOM certification; however, coordinate any procurement of surveillance assessment and tracking technology with both HQ AETC/SF and HQ ACC/SF prior to installation.

18.3. HQ Air Intelligence Agency (HQ AIA). For systems on AETC installations, route requests through HQ AETC/SFO.

18.5. HQ Electronic Systems Center (HQ ESC). Send requests for PL4 IDS to HQ AETC/SFO prior to requesting HQ ESC assistance.

18.6.1. List PL4 resources in the ISI and identify owner and/or user responsibilities for normal security. The installation commander is the deviation approval authority for PL4 resources. Follow the guidance in Chapter 6 and Attachment 18 (Added)(AETC).

19.2.2. Maintain initial survey in the controlled area folder for each facility. If the initial survey was conducted prior to the publication of the basic instruction, and does not comply with current standards, it will be reaccomplished.

19.2.4. If more than one controlled area is surveyed during a visit, one survey report may be produced. However, file a copy of the report containing information relative to each controlled area in each separate folder.

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 IMT 395, **Quarters/Vehicle Security Check,** to document requests for courtesy checks of vehicles and quarters. Use AETC IMT 1021, **Project Ride Along Application,** to document requests to observe patrol activities. Develop local procedures to manage these programs.

19.3. Anti-Robbery Exercises. The ISC will determine training and exercise requirements for facilities that store less than $100,000.

20.1. General Information. The ISC must consider the cost of physical protection standards, and weigh the cost against other factors, such as sensitivity, criticality, vulnerability, location, and mission of the installation, facility, or resource.

20.2.2. Place controlled area signs along the temporary controlled area boundary.

20.4.1. For fenced areas, marking of individual storage facilities or containers is not required, provided the fence is properly marked.

20.5. Intrusion Detection Equipment (IDE). The CSF ensures commercially procured IDE (new system or system upgrade and/or enhancements) contains a maintenance requirement for the IDE before approving any system or component purchase. Use DoDD 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support,* to determine the most suitable and cost efficient IDE application. Ensure specific information is included in the proposal, and 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 resource protection program manager, local communications squadron, and civil engineer.

20.5.4. Establish a facility alarm priority list for the SFCC to use during multiple alarm situations.

20.5.5. Configure alarm sensors to detect at 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.

20.5.10. Identify authorized personnel by memorandum or a computer-generated product endorsed by the unit commander or designee.

20.5.11. If the system includes an intelligent key pad (a pad that allows users access to the facility with a card or personal identification numbers [PIN]), locate it outside the alarmed facility, or inside, if so designed and equipped with an annunciation/authentication delay feature. Keypad systems will have the capability to record time and date accessed, along with identification of the user.

20.5.12. Computerized alarm systems with keypads using PINs to access facilities are not required to change codes every 6 months.

20.5.13. The ISC will determine the method to document openings and closings.

20.6.1. The ISC will establish and publish key control procedures in the ISI. As a minimum, require the designation in writing of key and lock custodians, and mandate key inventory procedures.

21.3.1. Use AETC IMT 1015, **Security Forces Building Checklist,** to document building security checks. Determine locally the facilities to be checked.

22.2.5.1. A warehouse is considered a structure or facility designed for long-term storage.

22.2.5.2. The ISC determines areas that require controlled area designation.

22.2.5.5. Within AETC, designate all SFCCs as controlled areas due to their mission-essential communication status.

22.2.8. Develop and publish local approval procedures for free zones in areas containing PL4 resources in the ISI. Refer to paragraph 3.8.

22.2.8.1. If contractors are required to complete work around sensitive equipment or materials, owner and/or user personnel will be present any time contractors are in the area or remove the materials.

22.2.8.2. Develop and publish local procedures in the ISI. Do not use security forces personnel as free zone boundary sentries.

22.2.9. The installation contracting office will draft and send the letter and the CSF will coordinate on the content.

22.2.10. Phase 1 and 2 training in accordance with paragraph 7.2.1 as supplemented, satisfies this requirement.

22.3. Entry to Controlled Areas. The ISI will state the frequency in which combination changes and key inventories for PL4 areas will be conducted. ***EXCEPTION:*** Specific key and lock management procedures for munitions storage areas are outlined in AFI 21-201, *Management and Maintenance of Non-Nuclear Munitions.* The installation commander or designee will determine how to grant personnel authority to enter controlled areas. Methods may include, but are not limited to, naming positions in the ISI, or memorandums listing names and/or positions posted in the area.

23.1.1. Use the AF IMT 1473, **Gun Equipment Room Inventory,** for armories. This IMT may be overprinted for local requirements. Security forces armories are not repositories for resources owned by other units. However, the installation commander may authorize (in writing) the storage of a unit's firearms and munitions in another unit's storage facility. In this case, develop local procedures regarding accountability, handling, inventory, issuing, and container and lock requisition (to include procedures for keys and combinations). For installation-level storage facilities, conduct an inventory semiannually.

23.1.5. Ensure facilities meet construction criteria and alarm coverage. Document approval in the activities' resource protection folder.

23.1.6. Personnel authorized to open armories must be armed before entering the facility or immediately after entering the facility. All keys to locks that open arms, ammunitions, and explosives (AA&E) storage facilities must be protected when not in use.

23.2. Protection Policy for Nonnuclear Munitions Storage Areas (NMSA). Munitions being delivered on base will not be left unattended while outside a munitions storage area. When outside a storage area, owner and/or user personnel, the courier, or the unit responsible for receiving the shipment will provide security. Owner and/or user personnel are also responsible for securing munitions left within restricted areas that require an armed guard. Do not use security forces personnel to provide security.

23.2.2. Arming of personnel performing duties other than entry control, within the NMSA, regardless of AA&E Category, is not required unless otherwise determined by the ISC. Address arming of personnel in the ISI.

23.2.4. Establish procedures for munitions personnel to notify the SFCC at the end of the duty day when the NMSA is longer be manned.

23.2.5. Owner and/or user personnel are responsible for securing munitions. Do not use security forces personnel to provide security.

23.3. AA&E Facility Criteria. The CSF or designees will review AA&E construction contracts and upgrades for facility security compliance.

23.3.2.4.3. When a facility storing Category I AA&E has an inoperative IDS (one or more levels), owner and/or user will provide constant surveillance of the facility. A communications capability will exist to contact security forces for armed response. The ISC will determine the need for constant surveillance requirements when storing Category II AA&E in facilities without an operative IDS for short-term periods (for example, malfunctions due to weather).

23.3.2.4.4. On-base facilities housing only Category III or IV AA&E are not required to have IDS. The ISC will determine who conducts nonduty hour checks, and will publish this requirement in the ISI. Off-base AA&E facilities must have two levels of IDS, regardless of the category of AA&E stored.

23.3.2.6.5. Unless continuously guarded, secure gates with security padlocks meeting commercial item description (CID) A-A-1927. Locks that are 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 ISI.

23.3.3.12. Unit operating instructions will address vehicular and pedestrian entry into and exit from unit areas.

23.3.6.1.1. The ISC will determine when to require the removal of bolts due to increased force protection conditions.

23.4.1. A significant incident of loss or attempted theft is also defined in DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives.* For the purpose of this publication, the armory is considered continuously manned for units with a flight armory program. Inventories are required at shift change, or when primary responsibility for the armory is transferred.

23.5. Transportation. For AA&E shipments arriving or departing the installation, if the shipment does not require a police vehicle or armed escort off the installation, there will be no requirement for a police vehicle or armed escort while traveling on the installation. If the ISC determines the need for an armed escort based on threat, it will be performed by owner and/or user personnel receiving or originating the shipment, and not security forces personnel.

23.5.2.7. Use of private vehicles will be determined by the ISC and published in the ISI.

23.5.6. Do not use security forces personnel to conduct these checks unless security forces are the receiving unit.

23.8. Security of Commercial Shipments Temporarily at DoD Installations and Activities. Protection is provided by the receiving agency. Do not post security forces personnel to protect shipments. The ISC determines armament requirements.

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. Cross-reference he report against the lessons learned report in accordance with AFI 31-201, *Security Forces Standards and Procedures.*

23.11.3. Prompt reporting is defined as within 12 hours of discovery. If a unit does not have access to the National Crime Information Center (NCIC), contact another AETC installation for assistance. Within 24 hours of discovery, AETC units will provide HQ AETC/SFO a copy of the message or message confirmation report to the NCIC, and the Bureau of Alcohol, Tobacco and Firearms, Intelligence Division, regarding confirmed thefts, losses, and recoveries of DoD arms.

24.1. General Guidelines. For installations supporting PL4 mission support aircraft parking areas, ensure law enforcement patrol sectors and SSIs include these aircraft parking areas. The ISC will determine the need for continuous patrol coverage, armament requirements, and/or frequency of area checks. The ISC will determine if increased protection for taxiways and runways is needed during contingencies. The ISC also determines the need to sweep runways for security hazards and unauthorized personnel prior to the launch of alert aircraft.

24.1.1. (Added)(AETC) Nonoperational aircraft used for maintenance training only do not retain a PL designation. Protect operational aircraft undergoing maintenance in accordance with paragraph 14.7. Protect operational weapons systems remaining on the aircraft in accordance with the basic instruction.

24.3.1.2. Designate aircraft maintenance complexes as controlled areas if not already located within a restricted area. Clearly mark the boundary of the controlled area with raised barriers and controlled area signs that do not interfere with airfield safety restrictions. A controlled area EAL is not required for flight line areas.

24.3.1.3. Designate flight line roadways immediately adjacent to permanent PL3 or above aircraft parking areas controlled areas, and control vehicle traffic in accordance with paragraph 24.3.4. The ISC will determine the controlled area boundary for roadways leading to active taxiways, runways, aircraft parking, or aircraft maintenance areas. Unless specifically prohibited by airfield safety, the boundary will be clearly delineated and will not be within 25 meters of the affected area. Inside the controlled area boundary, the provisions of paragraph 24.3.4 apply. Some installations have major thoroughfares crossing taxiways and overruns. In these instances, the ISC will approve vehicle control measures, and determine the necessity to delineate the boundary.

24.3.3. Do not park PL4 aircraft in established PL3 or above areas.

24.3.4. The airfield manager is responsible for issuing and controlling passes in accordance with AFI 13-213, paragraph 4.3.3.7. Do not issue passes to operate privately-owned vehicles in restricted areas. Strictly control vehicle traffic, and do not issue passes for convenience. Issue passes only for military necessity. Passes must be clearly visible to security forces and owner and/or user personnel when the vehicle is in motion.

25.3. Funds Escort Procedures. 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.

25.3.1. If required, finance personnel provide armed and unarmed funds protection during mobility processing, with security forces providing a response capability.

25.3.2.1. (Added)(AETC) Contracting Procedures. Installation commanders are the approval authority if funds facilities request to use a civilian armed courier. Couriers must be certified and trained, to include weapon proficiency, in accordance with local or state standards. Couriers used to transport nongovernmental funds will meet the same requirements as those used for the escort of government funds. The CSF will review all armed civilian (nonlaw enforcement) protective escort service contracts.

25.3.2.2. (Added)(AETC) Service contracts will address the installation antirobbery procedures, communication with security forces, duress and authentication procedures, and the roles of courier personnel during robbery situations. Integrate couriers into the installation exercise program.

25.4.2. The ISC determines resource protection standards and procedures for automated teller machines (ATM), to include controlled area designation.

26.1.2. If controlled substances are stored in a different location than the main dispensing area and are transported to the dispensing area daily, IDS for the dispensing area is not required, as long as the controlled substances are constantly protected by owner and/or user personnel. In these cases, a duress capability is required for both the dispensing area and the storage area, and the storage area will have two levels of IDS.

26.7 (Added)(AETC) IMTs Prescribed. AETC IMTs 395, 1015, and 1021.

26.8. (Added)(AETC) Forms and IMTs Adopted. DD Form 2501; AF IMTs 116, 335, 340, 1109, 1314, 1473, and 2586; AF Forms 1199A, 1199B, 1199C, 1199D; and AFTO 781A.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Production, Procurement, Deployment, and Support*

DoD 5100.76-M, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives*

DoD C-5210.41M/AF Sup, *Nuclear Weapon Security Manual* (U)

AFI 21-201, *Management and Maintenance of Non-Nuclear Munitions*

AFI 31-201, *Security Forces Standards and Procedures*

AFI 31-207, *Arming and Use of Force by Air Force Personnel*

AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*

AFMAN 36-2108, *Airman Classification*

AFMAN 37-123, *Management of Records*

AFMAN 91-201, *Explosives Safety Standards*

AFI 36-2225/AETC Sup 1, *Security Forces Training and Standardization Evaluation Programs*

AETCI 10-205, *AETC Exercise Program*

WCIP07A, *Resource Protection/Crime Prevention Theory, Practice, and Management*

ECI Course 8100, *USAF Crime Prevention Program*

Abbreviations and Acronyms

ABS—Automated Badging System

AIA—Air Intelligence Agency

AWG—alarm working group

DIBRS—Defense Incident-Based Reporting System

FPP—flight line protection program

MEAL—master entry authority list

PDP—priority designation package

SFCC—security forces control center

SJA—staff judge advocate

SSI—special security instructions

TWG—threat working group

JOHANN R. KINSEY, Colonel, USAF
Director of Security Forces

Attachment 16 (Added)(AETC)

RESOURCE PROTECTION FOLDER REQUIREMENTS

A16.1. 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:

A16.1.1. (Added)(AETC) All initial, follow-up, and special program reviews.

A16.1.2. (Added)(AETC) Diagram of the facility showing locations of protected resources and sensors.

A16.1.3. (Added)(AETC) Copy of the most recent staff assistance visit.

A16.1.4. (Added)(AETC) Annual self-assessments, if applicable.

A16.1.5. (Added)(AETC) Appointment memorandums for funds custodians, munitions/weapons custodians, and controlled area monitors.

A16.1.6. (Added)(AETC) Authorization memorandum to store funds and firearms.

A16.1.7. (Added)(AETC) Memorandums designating the storage of munitions and storage limits.

A16.1.8. (Added)(AETC) Controlled area designation memorandum.

A16.1.9. (Added)(AETC) Current deviations.

A16.1.10. (Added)(AETC) Record of resource protection and controlled area training conducted in the last two years.

A16.1.11. (Added)(AETC) Most current resource protection operating instruction or other installation instruction.

A16.1.12. (Added)(AETC) Copy of facility initial survey.

A16.1.13. (Added)(AETC) Copy of antirobbery exercise documentation.

Attachment 17 (Added)(AETC)

INSTRUCTIONS FOR PREPARING AF IMT 116, REQUEST FOR DEVIATION FROM SECURITY CRITERIA

A17.1. (Added)(AETC) Deviation Program. The deviation program is managed by the CSF or designee. An AF IMT 116 is required for deviations from established PL1 to PL4 security criteria. The AF IMT 116 is used to record all data bearing on temporary, permanent, and technical deviation requests. Process extension requests the same as initial requests, but with sufficient coordination time to ensure the extension is complete and approved before the original deviation expires. Complete the IMT as follows:

A17.1.1. (Added)(AETC) Block 1. Show the installation, last two digits of the current calendar year, and the cumulative number of requests submitted. For example, the first deviation from Luke AFB for calendar year 2004 is Luke AFB 04-1. This number will remain with the deviation and will not be changed during annual review or reapproval.

A17.1.2. (Added)(AETC) Block 2. Self-explanatory. Refer to paragraph 6.3 for expiration guidelines.

A17.1.3. (Added)(AETC) Block 3. Check the proper block.

A17.1.4. (Added)(AETC) Block 4. Check the proper blocks. Deviations are considered canceled and expired on the stated expiration date unless the proper authority has approved a request for extension.

A17.1.5. (Added)(AETC) Block 5. Give the specific directives and paragraph establishing the requirement that the deviation is requested for.

A17.1.6. (Added)(AETC) Block 6. Self-explanatory.

A17.1.7. (Added)(AETC) Block 7. State the specific requirements contained in the directive and paragraph cited in block 5.

A17.1.8. (Added)(AETC) Block 8. Provide a description of the deficiency and the reason for noncompliance.

A17.1.9. (Added)(AETC) Block 9. Be specific and provide all the information needed (to include maps, photographs, and line drawings) by the approving authority to make an informed decision. If the request is for a technical deviation, explain the situation that justifies the variance (for example, why the deviation provides essentially the same degree of security).

A17.1.10. (Added)(AETC) Block 10. Use this block for temporary and permanent deviations. State specifically those measures taken to compensate for the deviation. Do not cite increased security awareness or security force vigilance as compensatory measures. The compensatory measure must provide the same level of security as the required standard. List all other deviations in effect for the area, and consider them when developing compensatory measures to make sure the measures are realistic and do not over task security forces personnel.

A17.1.11. (Added)(AETC) Block 11. Be specific. Explain what action has been taken or programmed to correct the deviation and its current status.

A17.1.12. (Added)(AETC) Block 12. If funding or monetary cost is a factor, show the estimated cost of correction.

A17.1.13. (Added)(AETC) Block 13. Specify the funding, repair or construction project number, and priority applied by the base. If applicable, note priorities for construction projects setup by intermediate commands and MAJCOMs in block 20.

A17.1.14. (Added)(AETC) Block 14. Enter the anticipated correction date, if applicable.

A17.1.15. (Added)(AETC) Block 15. Show coordination of other base agencies affected by, or involved in correcting the deviation.

A17.1.16. (Added)(AETC) Block 16. Self-explanatory.

A17.1.17. (Added)(AETC) Blocks 17 and 18. For AETC PL3 and above areas, the CSF is the requestor. For PL4 areas, the unit commander responsible for the resource is the requestor.

A17.1.17.1. (Added)(AETC) For PL3 and above resources belonging to other MAJCOMs located on AETC installations, the commander responsible for the resource is the requestor. The CSF will coordinate in block 15. Address deviation approval processes in support agreements.

A17.1.18. (Added)(AETC) Block 19. Self-explanatory.

A17.1.19. (Added)(AETC) Blocks 20 to 24. For AETC PL3 and above areas, the HQ AETC director of security forces completes this section prior to the approval authority's signature.

A17.1.19.1. (Added)(AETC) For PL3 and above resources belonging to other MAJCOMs located on AETC installations, the owning MAJCOM SF director or designee completes this section and determines block 21 coordination.

A17.1.19.2. (Added)(AETC) For PL4 areas, the group commander responsible for the resource completes this section. When needed, the reviewing official adds pertinent information in block 20 to assist the approval authority in validating the request. Block 21 coordination is determined locally. The reviewing official notes whether compensatory measures are considered adequate. If the reviewing authority disapproves the request, return the request to the requester with rationale for the disapproval.

A17.1.20. (Added)(AETC) Block 25 to 32. The deviation approval authority for PL4 and above areas is the installation commander. This authority cannot be delegated. Coordination in block 29 will consist of ISC members prior to the installation commander approving the deviation. For PL3 and above resources belonging to other MAJCOMs located on AETC installations, the approval authority will be in accordance with owning MAJCOM guidance.

A17.2. (Added)(AETC) Deviations. Forward copies of approved deviations to HQ AETC/SFO within 30 days of approval.

Attachment 18 (Added)(AETC)

FLIGHTLINE PROTECTION PROGRAM (FPP)

A18.1. (Added)(AETC) General. The FPP is the AETC physical security awareness program. Protection of PL aircraft is the responsibility of all personnel working within restricted areas. The FPP strengthens and bolsters physical security and force protection awareness among personnel performing duties within aircraft PL3 restricted areas.

A18.2. (Added)(AETC) Scope:

A18.2.1. (Added)(AETC) This program equally applies to units of other MAJCOM organizations that are tenant units on AETC installations.

A18.2.2. (Added)(AETC) AETC units tenant to another installation must participate in the host physical security awareness training program, if available.

A18.3. (Added)(AETC) Installation Commander. Commanders at installations with permanently assigned PL3 aircraft are responsible for developing a FPP focusing on the effectiveness of physical security awareness training while improving the security awareness level of personnel. The installation commander designates an installation FPP manager.

A18.4. (Added)(AETC) FPP Manager. The FPP manager promotes joint responsibility with owner and/or user personnel to assure the highest level of security awareness. It is recommended this individual be the same one responsible for conducting wing-level exercises. The FPP manager's responsibilities include:

A18.4.1. (Added)(AETC) Assessing physical security awareness training by visiting restricted areas at a frequency determined by the installation commander.

A18.4.2. (Added)(AETC) Developing and implementing a local exercise plan in coordination with FPP monitors. Conduct monthly no-notice exercises to evaluate security awareness effectiveness. Security forces must approve exercise plans and scenarios prior to implementation. The installation commander will determine the number of exercises to be performed each month. As a minimum, conduct 10 exercises each quarter, to include ramp and hangar areas; conduct half the exercises during nighttime hours. At the discretion of the installation commander, exercises may be suspended during FPCON Charlie or higher.

A18.4.3. (Added)(AETC) Maintain an exercise database containing exercise summaries, results, trends, and outstanding performers. Brief and record these items during ISC meetings.

A18.5. (Added)(AETC) FPP Monitor Responsibilities. Unit commanders whose personnel routinely work in or around aircraft PL3 restricted areas will appoint an FPP monitor, usually the unit security manager, antiterrorism NCO, or force protection NCO. The installation commander will identify these units in the ISI. The FPP monitor's responsibilities include:

A18.5.1. (Added)(AETC) Through verbal or written surveys and performance-based indicators ensure owner and/or user personnel know their security responsibilities.

A18.5.2. (Added)(AETC) Conduct unit-level, no-notice, SF-approved exercises to emphasize and enhance owner and/or user security, and evaluate the security reporting and alerting system.

A18.6. (Added)(AETC) CSF Responsibilities. The CSF or designee should host periodic meetings with the FPP manager and monitors, and provide technical assistance and advice as needed.

A18.7. (Added)(AETC) FPP Exercises. If the perpetrator is challenged, and the event is properly reported within 15 minutes, the exercise is considered a detection. If the perpetrator has been unchallenged by three or more owner and/or user personnel, or has not been detected or challenged within 15 minutes, the exercise is terminated and reported as a nondetection. To be successful, the quarterly exercises must result in detection of unauthorized personnel 80 percent of the time.

A18.7.1. (Added)(AETC) Design exercises to evaluate the ability of non-SF personnel to detect and report security violations. Security forces personnel participate by providing a response to the simulated threat. Use caution to prevent on-duty security forces personnel from interpreting exercises as an actual hostile act. Perpetrators may not use simulated weapons or explosive devices, and must not attempt to flee from anyone requesting identification. Perform exercises in accordance safety directives, and develop clear, standard procedures to prevent injury or unsafe acts.

A18.7.2. (Added)(AETC) Perpetrators must have unescorted entry authority for the selected exercise location and should attempt to enter the area overtly (such as crossing a restricted area boundary at a place other than the ECP) or covertly (for example, no RAB displayed). Control and secure altered or fake RABs in accordance with local procedures.