

15 DECEMBER 2001

Security

**TRAVIS AFB INSTALLATION SECURITY
PROGRAM**



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://afpubs.hq.af.mil>.

OPR: 60 SFS/SFOS (MSgt Hector Rodriguez)

Certified by: 60 SFS/CC
(Maj Harry R. Kimberly III)

Supersedes TAFBI 31-101, 1 May 1998

Pages: 47
Distribution: F

This instruction implements Air Force Policy Directive 31-1, *Physical Security* and AFI 31-101, *The Air Force Installation Security Program* as they apply to Travis Air Force Base (TAFB). The provisions of this instruction apply to and are enforceable against all military and civilian personnel, including the general public, who enter TAFB. It establishes and describes the restricted and controlled areas located within the boundaries of TAFB and the procedures for establishing new restricted and controlled areas, free zones, and changes to existing restricted and controlled areas. It prescribes procedures for granting authorized entry into restricted and controlled areas. The restricted and controlled areas described in this publication are established according to lawful authority and are published under DoD Directed 5200.8, Security of DoD Installation and Resources, and Section 21, Internal Security Act of 1950 (Act of September 1959; Chapter 1024, 64 Statute. 1005, 51 United States Code (USC) 797). Full compliance with entry requirements to restricted and controlled areas constitutes specific permission of the installation commander and applicable associate unit commanders. This instruction requires the collection of data protected by the Privacy Act of 1974. The authority to collect the data is Title 10 USC 8012, title 44 3101.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. Paragraph 3.1.7. is updated to reflect procedures for photography, video, and audio recordings. Paragraph 3.6. provides additional information on crew bus/transportation in restricted and controlled areas. Paragraph 3.11. further discusses procedures on establishment of free zones, restricted area badge wear and detaining violators. Paragraph 3.13. incorporates new procedures for visiting restricted areas. Paragraph 3.16. adds the revamped TAFB Security Education and Training (SET) program. Paragraph 5. gives additional guidance on PL 4 resources and controlled areas on TAFB. Paragraph 5.3. is revised to clarify owner/user responsibilities of controlled areas and intrusion detection equipment. Paragraph 5.5. clarifies procedures for alarm activation/anti-robbery procedures. Paragraph 5.6. is completely updated to reflect funds facility procedures. Paragraph 5.7. incorporates revised procedures for on-base movement of Arms, Ammunition and Explosives (AA&E). Paragraph 5.8. adds requirements of classified information and secure room requirements.

Paragraph 5.10. provides additional guidance to users on requirements for resource protection folder. Paragraph 7. lists procedural changes in normal security operations, installation entry points, normal installation entry procedures and normal installation visitor procedures. Paragraph 7.6. is updated to reflect base entry/exit point checks (BEPC). Paragraph 8.2. assigns normal tasks to additional units. Paragraph 9. is added to clarify requirements for the Installation Security Council (ISC). Paragraph 10. gives further guidance on weapons registration, storage, and transportation.

- 1. SECURITY PROTECTION LEVEL SYSTEM: 3
- 2. CONTROL AND ISSUE OF RESTRICTED AREA BADGES (RAB): 5
- 3. RESTRICTED AREA ENTRY AND CIRCULATION CONTROL PROCEDURES: 9
- 4. SECURITY REPORTING AND ALERTING SYSTEM 17
- 5. PROTECTION LEVEL 4 RESOURCES: 19
- 6. NORMAL SECURITY OPERATIONS: 26
- 7. INSTALLATION ENTRY AND CIRCULATION PROCEDURES: 28
- 8. NORMAL TASKS FOR ASSIGNED UNITS: 33
- 9. INSTALLATION SECURITY COUNCIL (ISC): 35
- 10. WEAPONS REGISTRATION, STORAGE, AND TRANSPORTATION: 36
- 11. Forms Prescribed: 38

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 39

Attachment 2—EXAMPLE OF CALL SIGN-POST TITLE-WEAPON ARMED WITH, AND RADIO PRIORITY FORMAT 40

Attachment 3—HOW TO COMPLETE AF FORM 2586 42

Attachment 4—COMPLETING DD FORM 577, SIGNATURE CARD 43

Attachment 5—(SAMPLE FORMAT FOR REPORTING LOST OR STOLEN RESTRICTED AREA BADGES) 44

Attachment 6—STATEMENT 46

Attachment 7—(SAMPLE FORMAT FOR LETTER IN LIEU OF AN AF FORM 2586) 47

1. SECURITY PROTECTION LEVEL SYSTEM:

1.1. Protection Level 1 (PL 1). Applies to weapons systems on alert status for direct enemy engagement, all nuclear weapons in the United States Air Force arsenal and components of tactical command/control/warning facilities.

1.1.1. Permanent PL 1 resources assigned to TAFB are the Naval "Take Charge and Move Out" (TACAMO) E-6A and E-6B aircraft.

1.2. Protection Level 2 (PL 2). Applies to the major components of weapons systems that are not on alert status but are on bases and sites from which they could be launched for direct strikes against or engagement with the enemy. Certain aircraft support facilities are also PL 2.

1.2.1. There are no permanent PL 2 resources assigned to TAFB.

1.2.2. The Alternate Tanker Airlift Control Center (ATACC) located on TAFB is a PL 2 resource when activated.

1.3. Protection Level 3 (PL 3). Applies to combat aircraft and missiles that cannot be considered in place forces by virtue of their present location. It also applies to logistic, air commando, reconnaissance, and the like aircraft designated for direct support of engaged combat forces or required to sustain operations in general limited war.

1.3.1. Permanent PL 3 resources assigned to TAFB are mission capable C-5, KC-10 aircraft, Naval TACAMO E-6A and E-6B aircraft when not on alert status, and the Travis Command Post (TCP) with adjacent Crisis Action Team (CAT) room.

1.3.1.1. PL 3 aircraft in maintenance will retain their PL status.

1.3.2. The alternate TCP in Building 977 is a temporary PL 3 resource when activated.

1.4. Protection Level 4 (PL 4). Areas not meeting the above PL criteria but require additional security measures.

1.4.1. All controlled areas on TAFB are designated as PL 4.

1.5. Restricted Areas. A legally established military zone under United States Air Force jurisdiction into which persons may not enter without specific authorization. This authorization comes from the installation commander. Restricted areas contain operational resources such as the Command Post (CP), PL 1, 2, or 3 aircraft, or missile systems. The use of deadly force in these areas is authorized for Security Forces personnel.

1.5.1. Restricted area boundaries are identified by raised barriers or a 4-6 inch red stripe painted on the concrete and restricted area signs posted every 100 feet. If a building or room is a restricted area, all doors will be marked with restricted area signs.

1.5.2. You may only enter restricted areas via established entry control points which are marked by a 4-6 inch white stripe painted onto the concrete and signs denoting that area as a valid entry control point. If a building or room is a restricted area, you will only enter through established entry control doorways.

1.5.3. Permanent restricted areas on TAFB are:

1.5.3.1. TACAMO aircraft parking area. TACAMO is located on the southeast side of the installation along taxiway golf. This includes Sugar Area (SA) parking spots 1, 2, 3, 4, and 5,

Buildings 1166, 1167, 1168, 1171, 1174, 1175 and surrounding area encompassed by chain-link fencing. Restricted area warning signs are posted every 100 feet along the boundary. The TACAMO area is located adjacent to the end of runway 3R near the south central boundary of the base. The TACAMO aircraft parking area routinely contains PL 1 and PL 3 resources. Security Forces provide primary security, entry, and internal control at all times.

1.5.3.2. Mass Parking Area (MPA). The MPA is the combined 200-600 ramps and is surrounded by ropes and rubber disks, a 4-6 inch red line painted on the ground or cement jersey barriers. Restricted Area warning signs are posted every 100 feet along the boundary. The MPA generally contains PL 3 resources, however, may contain higher PL resources. Support forces provide primary security, entry, and internal control during normal security operations.

1.5.3.3. TCP. The PL 3 TCP and the adjacent CAT room are located in the southeast portion of Building 31. The existing walls of the structure serve as a restricted area boundary. Restricted area signs are posted on all doors entering the area. Support forces provide primary security, entry, and internal control during normal security operations.

1.5.4. Temporary restricted areas on TAFB are:

1.5.4.1. ATACC. The PL 2 ATACC is designated a temporary restricted area when activated. ATACC is located in Building 241, first floor, Bay D. The existing walls of the structure serve as a restricted area boundary. Restricted Area signs are posted on all doors entering the area.

1.5.4.2. Hangars P-14, 808, 809, 810, 811, and 818. When PL assets are present, hangars P-14, 808-811, and 818 will be designated as restricted areas. The restricted areas will be supported by a 4-6 inch red stripe painted on the concrete, restricted area warning signs painted on the concrete every 100 feet, and posted on the building on all entry points. Support forces provide primary security, entry, and internal control during normal security operations.

1.5.4.3. Aircraft parking spots 903, 904, 905, and 906. The restricted area portion of the 900 ramp, spots 903-906, are surrounded by a 4-6 inch red line painted on the ground. Restricted area warning signs are painted every 100 feet along the boundary. This area is designated a restricted area when PL resources are located on one of the above parking spots. Support forces provide primary security, entry, and internal control during normal security operations.

1.5.4.4. Hotel Ramp Parking Area(HRPA). When PL assets are present, the entire area will be designated as a restricted area by raised barriers, restricted area warning signs, and entry controlled by supporting forces, when present, or by random Security Force coverage when supporting forces are not present. Hotel area is the hazardous handling area (Munitions/Hazardous Materials) and is also the alternate location for Safe Haven (SH) and the alternate location for Emergency Nuclear Airlift Forces (ENAF).

1.5.4.5. SA. When PL assets are present, the parking spot occupied will be designated as a restricted area. The restricted area is supported by raised barriers and restricted area signs. SA 10, 11, and 12 are primary parking spots for ENAF and SH arrivals. Support forces provide primary security, entry, and internal control during normal security operations.

1.5.4.6. Alternate Travis Command Post (ATCP). The ATCP is located in Building 977 and is designated a restricted area when activated.

1.6. Security Response Priority. Following is a priority listing for emergency response to PL resources assigned to TAFB.

- 1.6.1. TACAMO alert area and transient PL 1 resources.
- 1.6.2. ATACC when activated and transient PL 2 resources.
- 1.6.3. C-5/KC-10 aircraft.
- 1.6.4. TCP or CAT room.
- 1.6.5. Transient PL 3 US Military Aircraft and PL 3 resources.
- 1.6.6. Civilian contracted and Civil Reserve Air Fleet (CRAF) aircraft.
- 1.6.7. PL 4 resources.

2. CONTROL AND ISSUE OF RESTRICTED AREA BADGES (RAB):

NOTE: The Chief, Security Forces, 60 SPTG/CSF, has been designated as the base RAB issuing official. This authority has been delegated to the NCOIC, Pass and Registration (60 SFS/SFOXI).

2.1. Procedures for Control and Issue of RAB.

2.1.1. Entry Authority. The number of personnel permitted to enter a restricted area will be limited to those with a need to enter to perform official duties. A person may be authorized entry either by being granted unescorted entry according to AFI 31-101, and AFI 31-501, *Personnel Security Management Program*, or by being properly escorted.

2.1.2. Unescorted entry applies to a person who has a continuing and frequent need for entry (at least once per week). Investigative requirements must be satisfied prior to badge issue. AFI 31-501 outlines investigative and personnel security requirements. Unescorted entry to restricted areas begins with the administrative processing of an AF Form 2586, **Unescorted Entry Authorization Certificate (Attachment 3)**. The authority for a person to enter a restricted area comes from the installation commander. This authority may be delegated to and exercised by base officials or restricted area coordinating officials (see Paragraph 2.2.) designated by the installation commander.

2.1.3. Escorted entry applies to a person who does not qualify for unescorted entry but is needed within a restricted area on a one-time or infrequent basis. The investigative requirements of AFI 31-501 are not applicable to escorted personnel, unless classified information will be divulged during the visit.

2.1.4. Restricted Area Badge Request and Processing. To obtain an AF Form 1199, **USAF RESTRICTED AREA BADGE ACCOUNTABLE** the requesting organization will ensure all applicable requirements and appropriated applicable agency or departmental directives are met.

2.2. Issuance of RAB:

2.2.1. Obtain coordination, escort, and entry approval (Sections II and IV of AF Form 2586) from the designated official identified in Paragraph 2.4.2.

2.2.1.1. Sign Section II of the AF Form 2586. The signing of Section II certifies that records have been reviewed and a favorable security investigation is on file. Unit security managers will ensure Sections I through III are complete, as applicable. To speed processing time, the AF Form 2586 should be hand carried to each applicable coordinating official by the unit security manager. When completing Column 2 (Escort Official) of Section IV, indicate whether the individual has escort authority by indicating **YES** or **NO** in this block. Approving officials

type or print their names and titles in the signature blocks and sign the forms. NOTE: Area 11 is the only area on TAFB requiring an E for escort official. **NOTE:** Security clearance of individual must be verified either from Sentinel Key or the current ASCAS roster before completing the AF Form 2586. When AF Form 2586 is completed for escort officials, the following must be typed in Section II: Security escort training completed on date. Include typed name with signature in Section III (this will help identify signatures).

2.2.1.2. Ensure the individual hand carries the original AF Form 2586 to Pass and Registration (60 SFS/SFOXI) for completion of Section V and issuance of the RAB.

2.2.1.3. Upon completion and issuance of the RAB Pass and Registration will give the original AF Form 2586 to the individual to return it to the requesting activity for filing. Pass and Registration will file a copy of the AF Form 2586 until the badge has been turned in. (See [Attachment 3](#))

2.3. Authorization to Sign AF Form 2586:

2.3.1. Unit commander/staff agency chief will annually or when a change occurs, provide Pass and Registration with a DD Form 577 or letter for each individual designated to authenticate Section II (usually security manager) and Section IV of the AF Form 2586 for signature verification. DD Form 577 must be specific, for example: Sign Section IV, AF Form 2586 for restricted area 1 and area 4. (See [Attachment 4](#))

2.3.2. Individuals listed below will be designated approving officials for restricted areas on TAFB and will sign Section IV of the AF Form 2586. This area is to be signed by the approving official only. Approving officials and designees may not grant themselves unescorted entry.

<u>Area</u>	<u>Approving Official</u>
01 Command Post	60 AMW Commander Chief, Consolidated Command Post Superintendent, Consolidated Command Post Chief Controller 60 SFS (Security Forces Squadron) Commander
04 Mass Parking Area	60 AMW Commander 60 LG (Logistics Group) Commander 60 AGS (Aircraft Generation Squadron) Commander 660 AGS (Aircraft Generation Squadron) Commander 60 EMS (Equipment Maintenance Squadron) Commander 60 CRS (Component Repair Squadron) Commander 60 LSS (Logistics Support Squadron) Commander 60 OG (Operation Group) Commander 60 OSS (Operation Support Squadron) Commander 60 APS (Aerial Port Squadron) Commander

<u>Area</u>	<u>Approving Official</u>
	21 AS (Airlift Squadron) Commander
	22 AS (Airlift Squadron) Commander
	9 ARS (Air Refueling Squadron) Commander
	6 ARS (Air Refueling Squadron) Commander
	349 AMW/CC/LG/OG (see Section 2.3.2.3.)
	60 SFS (Security Forces Squadron) Commander
	615 AMOG Commander
	615 AMOS Commander
	15 AF Commander
11 TACAMO	60 AMW Commander
	VQ-3/OIC
	60 SFS (Security Forces Squadron) Commander
12 ALT TACC	60 AMW Commander
	60 CS (Communications Squadron) Commander
20 MARC	60 AMW Commander
	615 AMOG (Air Mobility Operations Group) Commander
	615 AMOS (Air Mobility Operations Squadron) Commander
	615 AMS (Air Mobility Squadron) Commander
	715 AMS (Air Mobility Squadron) Commander
	815 AMS (Air Mobility Squadron) Commander

2.3.2.1. 60th Security Forces Squadron Commander (60 SFS/CC) is the approving official for all Security Forces personnel for each area of responsibility.

2.3.2.2. If the squadron commander is on TDY, leave or on an extended absence, the acting commander is authorized to sign as the coordinating/approving official if on G-Series orders only.

2.3.2.3. Unescorted entry approval for 349th AMW personnel to Area 4 is limited to the commanders of the 349th OG, 349 LG, 349 OSF, 301 AS, 312 AS, 708 AS, 710 AS, 349th ACF, 70 ARS, 349 AES, 45 APS, 55 APS 82 APS, 349th AGS, 945 AGS, 349 CRS, 79 ARS, 349th EMS, 749 AGS, and 349th SFS. The 349th SFS/CC will hold the same responsibilities as the 60 SFS/CC as stated in Paragraph 2.3.2.1.

2.3.3. Commanders down to the squadron level are authorized to designate escort officials within their functions. This authority may not be delegated further. Escorts are required for PL 1 and PL 2 resources only.

2.3.3.1. Personnel assigned to squadrons without a designated approving official must coordinate their request through 60 AMW/CC, 60 LG/CC, 60 OG/CC, or the primary functional commander (e.g., TACAMO, CP, alternate TACC, etc.) as listed in Paragraph 2.3.2.

2.3.4. Badge Issue. Individuals requesting badges will be required to present their military or civilian identification card to the badge issuing official. The badge-issuing agency must develop a system to validate all AF Form 2586s to ensure fraudulent or erroneous requests for restricted area entry credentials are not accepted.

2.3.4.1. Badge issuing activity will use a supporting technique (i.e., DD Form 577, **Signature Card** or letter containing original signatures of designated individuals) to prevent fraudulent or erroneous requests for restricted area entry credentials. All AF Form 2586s without proper signatures will not be accepted. DD Form 577s must be typed with name, grade, title and areas authorized to approve.

2.3.4.1.1. DD Form 577 or a letter, must specify the requesting official's and the approving official's signatures. DD Form 577 must specify the areas authorized for the approving officials to sign. No areas will be left open on the DD Form 577. Write-in changes are not accepted. Approving officials and designees may not grant themselves unescorted entry. All DD Form 577s need to be updated when a change of command takes place.

2.4. Reissue of RAB:

2.4.1. Reissue all badges for the installation or a specific area will be made when a compromise of the badge system is indicated, the installation commander loses confidence in the system, or the badge loss rate is 10 percent or greater.

2.4.1.1. Lost Badge. If an individual loses his/her RAB, he/she must report the loss immediately to his/her unit/staff agency security manager and squadron commander. The unit security manager/designee will follow these steps:

2.4.1.2. Thoroughly investigate the loss within three duty days. **NOTE:** If the lost badge involves a TACAMO escort official, the security manager will immediately report the loss to the Security Forces Control Center (SFCC).

2.4.1.3. Send the report of investigation (see **Attachment 5**) endorsed by the squadron commander to 60 SFS/SFOXI. Include the individual's statement (see **Attachment 6**) and the original AF Form 2586. (If the original AF Form 2586 is lost or missing, a letter in lieu of will suffice. (See **Attachment 7**))

2.4.1.4. Investigations and reports must be completed before reissuing a badge.

2.4.2. Damaged/confiscated badge. When a badge needs replacement due to damage, mutilation, deterioration, or change of identification, the individual will bring the original badge and the original AF Form 2586 to Pass and Registration for reissue. If a badge is confiscated by Security Forces personnel, the bearer must take the AF Form 52, **Evidence Tag/Receipt for Property** receipt along with the original AF Form 2586 to Pass and Registration for reissue. If the commander who signed the original AF Form 2586 is no longer assigned, the newly appointed squadron commander must annotate and sign in the remark section reissue due to damage/mutilation/confiscation.

2.4.3. Add an Area. When reissuing a badge to add an area, annotate the remark section of the original AF Form 2586 at the bearer's unit with *Add area X* and include the name and signature of the individual's commander. Add the new area in Section IV and ensure normal area coordination is accomplished. If the AF Form 2586 remarks section does not have sufficient space to annotate the change, complete a new AF Form 2586. The bearer hand carries the original badge and the

newly annotated original AF Form 2586 to Pass and Registration. Pass and Registration will verify the form and issue the new RAB. The badge-issuing activity will file a copy of the new AF Form 2586 with the previous AF Form 2586 maintained within the Pass and Registration office.

2.4.4. Delete an Area. When an area must be deleted, the individual's unit commander annotates the original AF Form 2586 with a "*Delete area X*" in the remarks section on the back of the form. If the AF Form 2586 remarks section does not have sufficient space to annotate the change, complete a new AF Form 2586. The bearer hand carries the old badge and the newly annotated AF Form 2586 goes to Pass and Registration. Pass and Registration will issue a new RAB. Pass and Registration will add the new badge number, strike out the deleted area and mark the form deleted per attached letter on all copies of the AF Form 2586. Pass and Registration will file a copy of the newly annotated AF Form 2586 with a copy of the old AF Form 2586.

2.4.5. It is the individual's responsibility to inform his/her unit security manager of any significant changes in facial features so the RAB can be corrected to reflect the change.

2.5. Inventory/Control of RAB:

2.5.1. Each unit will receive a roster of personnel possessing RAB from Pass and Registration annually. Unit/staff agency security managers will use this roster to make corrections to their AF Form 2586 file and RAB inventory.

2.5.2. Security managers will ensure that the RAB and AF Form 2586 are hand-carried and surrendered to Pass and Registration *NLT one workday* before the person departs the base. Personnel can not out-process through 60 MSS until cleared through Pass and Registration.

NOTE: If the AF Form 2586 has been misplaced/lost, the security manager will prepare a letter in lieu of the AF Form 2586. (See [Attachment 7](#))

2.5.3. Storage of RAB for AFRES units: AMC AFRES unit commanders will establish a system whereby RAB will be securely stored at the unit when individuals are not on active duty. When personnel sign-in for a unit training assembly (UTA), the RAB will be issued. Once the UTA is completed, the RAB will be returned to the unit for safekeeping and inventory. Personnel on flying status in an Air Reserve Technician (ART) position or designated by the unit commanders may retain their assigned RAB.

2.5.4. Pass and Registration will provide SFCC with an updated hardcopy of the master restricted area badge listing monthly. Daily additions will be mailed electronically.

3. RESTRICTED AREA ENTRY AND CIRCULATION CONTROL PROCEDURES:

3.1. TACAMO Area. Entry into TACAMO requires area 11 open on the Travis AFB-issued RAB. Temporary Duty (TDY) personnel will be allowed entry with a valid RAB along with EAL/crew orders authenticated by a 60 SFS official, E-6 or above.

3.1.1. All personnel authorized unescorted entry into the TACAMO alert aircraft parking area will drive around the base perimeter road and enter through the permanently established ECP.

3.1.1.1. Pre-announced emergency vehicles/alert crews responding to an actual exercise emergency klaxon may enter the TACAMO alert aircraft parking area through the restricted area boundary at taxiway "G" or taxiway "T".

3.1.1.2. Pre-announced special purpose vehicles, which are too large to enter through the vehi-

cle entrapment area, may enter at taxiway "T" after the vehicle and passenger(s) have been searched.

3.1.2. All hand-carried items will be searched. The following items are prohibited inside the TACAMO restricted area:

3.1.2.1. Cameras or video equipment unless authorized in writing by the OIC VQ-3 and authenticated by a 60 SFS official, E-6 or above.

3.1.2.2. Any hazardous chemicals or liquids not being used for official purposes are not authorized. Any type of MACE, other than SF issued OC spray, is also prohibited.

3.1.2.3. Weapons or explosives. SFS and TACAMO personnel authorized to carry weapons to perform their official duties are exempt.

3.1.3. Government-owned vehicles (GOV)/contractor vehicles will be allowed in the TACAMO area for official business only. All vehicle occupants will dismount the vehicle prior to entering the entrapment area and process as pedestrians; the vehicle driver will process last. Once processed, both the vehicle driver and a Security Forces member will inspect the vehicle in the entrapment area. The driver is responsible for opening the glove box, hood and all compartments. When all actions are complete, the entry controller (EC) will allow entry into the area. This procedure does not apply to personnel responding to emergencies/klaxons.

3.1.4. Privately owned vehicles (POV) are prohibited inside the restricted area or parked within 30 feet of its boundary.

3.1.5. Trash vehicles equipped with a compactor will be required to activate the compactor prior to entry and VQ-3 will provide an escort for the trash vehicle while it is within the TACAMO area.

3.1.6. Security Forces will not conduct a sweep of the flightline prior to TACAMO aircraft departures unless in Force Protection Condition (FPCON) Bravo or higher or situation dictates.

3.2. ATACC Area when activated. Entry into Bay D requires area 12 open on a TAFB issued RAB or be listed on an authenticated entry authority list (EAL).

3.3. PL 3 Mass Parking Area (MPA)/900 Ramp/Hotel Ramp/Sugar Ramp (Spots 6-12)/Hangars. Area 4 must be open on the TAFB-issued RAB for unescorted entry.

3.3.1. US Customs and Department of Agriculture officials are granted unescorted entry into PL 3 flightline restricted areas upon presentation of their official credentials in lieu of AF Form 1199 series.

3.3.2. The appropriate level of security for transient aircraft will be determined according to the standards set forth in AFI 31-101. Security presence, detection capability, entry control, threats, and alarm response will be considered.

3.3.2.1. A single badge system consisting of home station restricted area badge, authenticated EAL, or crew orders will be used for unescorted entry.

3.3.2.2. Transient aircraft with weapons or classified information contained on board will be guarded by owner/user personnel or the material removed and stored in appropriate locations.

3.3.2.3. The External Security Response Team (ESRT) will meet all transient aircraft upon arrival and obtain a copy of crew orders.

3.3.2.3.1. Crew orders must be authenticated by a Security Forces member in the grade of E-6 or higher.

3.3.2.3.2. Authenticated crew orders will be distributed to the ESRT, internal Security Response Team (ISRT), and the SFCC.

3.3.2.3.3. Security Forces will make security arrangements with the aircraft commander using a security acknowledgement letter provided by SFOS.

3.3.3. Security Forces will conduct four fifteen-minute ECP checks per eight-hour shift on the MPA and document each check in the Security Forces blotter.

3.3.4. GOVs are authorized in the mass parking area and 900 ramp for official business only. Anyone driving a vehicle into the restricted area is responsible for ensuring that the vehicle has been checked and is free of unauthorized/dangerous articles or persons (items/persons detrimental to the safety/security of the priority resources). Large transportation vehicles with minimum maneuverability, such as 40K Loaders, may enter/exit the restricted areas at taxiway "K" or "J" via taxiway "N" provided TCP and the Security Forces Control Center (SFCC) are notified 15 minutes prior to their entry. If a Security Force patrol is available, monitor the entry to avoid unnecessary delays. During increased FPCON, these vehicles will use normal entry/exit procedures at established ECPs.

3.3.5. Rental vehicles used for official military duties in lieu of government vehicles and contractor/delivery company vehicles, whom the 60 AMW/CC has authorized entry are authorized to operate inside restricted areas.

3.3.6. POVs are prohibited from driving or parking within or around restricted areas containing PL 3 resources to include taxiways and the aircraft movement area (AMA) unless in possession of a valid TAFB flightline POV pass.

3.3.6.1. 60 OSS/OSA controls all POVs on the flightline and issues all POV flightline passes.

3.3.6.2. While operating a POV with a flightline pass on the flightline, the pass must be in plain view hanging from the vehicle's rear view mirror. The pass must be concealed out of sight when not operating on the flightline.

3.3.6.3. All POVs with a POV flightline pass must be searched by the member driving the vehicle for harmful materials prior to entering any restricted area.

3.3.6.4. Refer to TAFBI 13-103 for more information concerning TAFB flightline POV passes.

3.3.6.5. Contact the 60 SFCC and 60 OSS/OSA in the event of loss or theft of POV flightline pass.

3.3.7. Vehicle Searches. All vehicles will be searched prior to entering the MPA by the vehicle operator.

3.4. TCP. Area 1 must be open on the RAB for unescorted entry. During increased FPCON, an entry authority list (EAL) will be used in conjunction with the RAB for entry. The ATCP when activated is located in Building 977. A security guard will be posted for entry control at the TCP upon implementation of FPCON Charlie or when requested by the CAT director based on valid threat information.

3.4.1. For purposes of this instruction, the westernmost entry door with the attached entrapment area will be considered the main door to the facility.

3.4.2. Keep the combination of the cipher locks to the facility doors on a need to know basis. Do not issue the combination to anyone without a normal day-to-day need to enter the facility. Change cipher lock combination every quarter or when a compromise is suspected.

3.4.3. Support forces personnel will verify the identity of all persons requesting access who are not in possession of the cipher lock combination via closed-circuit television (CCTV) along with telephone prior to opening the outer door.

3.4.4. Support forces personnel will physically check all RABs prior to allowing entry through the outer door.

3.4.5. Keep the inner entrapment area door to the main door closed at all times.

3.5. Escorted Entry Control Procedures. Escorted entry applies to all personnel who have a one time need to enter a restricted area, but do not qualify for unescorted entry. Certain staff personnel, passengers under escort to airlift aircraft and official visitors are examples of such personnel. The investigation prerequisites explained in AFI 31-501 are not required for escorted persons. No visitor should approach an entry control point without an official escort.

3.5.1. Escort officials must keep personnel under escort in line of sight at all times and constantly be aware of the person's actions. At no time shall the line of sight between escort official and personnel under escort be broken. The escort may relinquish escort duty to another person with the applicable area open on their restricted area badge.

3.5.2. Escort Numbers. For TACAMO, ATACC and other PL 1 and PL 2 transient resources, escort officials may only escort five personnel at any given time. Groups larger than five must be separated into smaller groups and enter at different times, or multiple escort officials must be utilized.

3.5.2.1. For the PL 3 mass parking area and associated temporary restricted areas, TCP, and transient PL 3 resources, escort officials may only escort 10 personnel at any given time. Techniques specified in Paragraph **3.5.1.** also apply.

3.5.2.1.1. Exceptions: Public Affairs (PA) personnel escorting media for official Air Force tours or transportation buses transporting passengers to or from the passenger terminal to aircraft may escort the amount of personnel they may positively control.

3.5.3. TACAMO. Personnel requiring escorted entry into the TACAMO area will proceed to the established ECP and make telephonic contact with the EC if an escort official is not with them. They will not enter the pedestrian entrapment area until told to by either the EC or their escort official. Once their hand-carried baggage has been searched by the escort, the escort briefing has been given, and they are signed in on the AF Form 1109, **Visitor Register Log** by the escort, they may enter the area. **Note:** Positive identification for escorted personnel is validated through the use of two identifications.

3.5.3.1. Only GOVs are authorized in the TACAMO area. All vehicles of escorted personnel will be searched by the escorting official and a Security Forces member.

3.5.3.2. Escort officials for the TACAMO restricted area must have an "E" typed on their Travis-issued RAB on the inside (picture side) of the area 11. Personnel without an "E" typed

on their RAB may not perform duties as escort official. Personnel with a Tinker AFB-issued RAB may not escort into the TACAMO restricted area.

3.5.4. ATACC. Escort officials for the ATACC must have an "E" typed on their RAB on the inside (picture side) of the area 12. Personnel without an "E" typed on their RAB may not perform duties as escort official.

3.5.4.1. Personnel needing escorted entry into the ATACC will sign in on the AF Form 1109.

3.5.5. Mass Parking Area/900 Ramp/Hotel Ramp/Sugar Ramp (Spots 6-12)/Hangars. Anyone with area 4 open on their RAB may escort personnel in these areas. An "E" typed on the badge is not required during normal security operations.

3.5.6. TCP. Personnel without restricted area badges or who do not have area 1 open on their badges will be escorted. Any individual with area 1 open on their badge may perform escort duties. The escort is responsible to ensure all personnel without RAB remain in their control and in sight at all times. The escort may relinquish escort duty to another person with area 1 on their RAB after filling out the AF Form 1109.

3.5.6.1. When feasible, all visitor traffic should be directed through the main entry door.

3.5.6.2. Visitor's need to enter must be verified via their point of contact prior to allowing entry through the outer door.

3.5.6.3. Visitors will be signed in on an AF Form 1109 and be issued a visitor badge.

3.6. Crew Bus/Transportation into Restricted and Controlled Area Procedures. The senior ranking person in the mission crew must verbally vouch for all members of his or her party to the vehicle operator prior to entry into a restricted or controlled area.

3.6.1. If at any time a person is not known inside the vehicle, the individual must be verbally challenged by a member of the mission crew and identity verified.

3.7. Off Ramp Area. The entry control point will be clearly marked at the nose of each aircraft with signs, which read "ENTRY CONTROL POINT" and "RESTRICTED AREA." Security Forces entry controllers are periodically posted on a random basis at ECP to ensure compliance with entry requirements. An exception to normal circulation control procedures for the PL 3 aircraft restricted area is granted to the transient maintenance aircraft marshaler who must violate the restricted area boundary to properly guide an aircraft out of certain parking spots. Check credentials against an authenticated EAL maintained in SFCC. During actual emergency security postures, these officials are required to be escorted.

3.8. RAB Wear and Detaining Violators. All personnel will display their issued RAB on the outer-most garment above the waist at all times while inside the applicable restricted areas, even if inside a vehicle.

3.8.1. If in close proximity to a pre-flight or engine run, RABs may be stowed in such a manner as not to create a safety hazard, but must once again be displayed immediately upon termination of the event.

3.8.2. All personnel will stow their RAB when not inside restricted areas in a buttoned or zippered pocket with no portion of the RAB visible.

3.8.3. Support forces in the TACAMO aircraft parking area must verbally challenge anyone not displaying a RAB. If any individual is not in possession of a RAB, support forces must physically detain violators, remove them from the area, and contact Security Forces via the most expedient means available.

3.8.4. Support forces in the PL 3 aircraft parking areas and TCP must verbally challenge anyone not displaying a RAB. If any individual is not in possession of a RAB and is not under escort, support forces must verbally escort violators out of the restricted area and contact Security Forces via the most expedient means available.

3.8.4.1. In the event a perpetrator fails to heed verbal commands in PL 3 aircraft parking areas or TCP, support forces will keep perpetrators under observation and relay all pertinent information to responding Security Forces.

3.8.4.2. Under no circumstances will physical means be used by support forces to detain any perpetrator inside the PL 3 aircraft parking areas or TCP.

3.9. Emergency Entry Procedures: Emergency entry is gained when Security Forces have knowledge that an emergency situation/klaxon exists. Security Forces need to know the nature of the emergency, types of equipment, and number of personnel responding.

3.9.1. A security patrol along with owner/user personnel will maintain surveillance over responding personnel while within the confines of the area.

3.9.2. If the emergency occurs in the TACAMO area when the emergency has been terminated, all responding personnel will be logged in on AF Form 1109. If an ambulance needs to expedite its return to the hospital, a patrol will accomplish the AF Form 1109 at the hospital.

3.9.3. Emergency personnel and vehicles will exit the restricted area through established ECPs when the emergency is over.

3.9.4. TACAMO alert crew emergency entry to TACAMO: Crews shall utilize the aircraft sign/countersign to gain entrance into the restricted area and will use the same sign/countersign to gain access to the aircraft.

3.9.4.1. The aircraft sign/countersign will be published on a monthly basis and be given to all personnel with a need to know by 60 SFS/SFOSS.

3.9.4.2. Emergency entry by responding emergency forces will be accomplished via the sign/countersign.

3.9.4.3. SFCC will notify fire department and emergency room whenever the sign/countersign changes.

3.9.4.4. Security Forces will not allow entry into a restricted area strictly because emergency forces are responding Code 2 or Code 3. Prior notification from SFCC or knowledge of the incident is required.

3.9.5. Use the following procedures for use of the sign/countersign:

3.9.5.1. Visually pass the sign/countersign, if response is correct responding personnel proceed into the area.

3.9.5.2. If visual response is incorrect verbally pass the sign, if the verbal response is correct personnel proceed.

3.9.5.3. If verbal response is incorrect, stop the vehicle, conduct a badge check, if the person and the badge match crews proceed into the area.

3.9.5.4. If badge information and person do not match detain the personnel and implement emergency procedures.

3.10. Duress Codes. A duress code is a word or words that can be used during normal conversation to indicate duress. The words will be developed and disseminated to all VQ-3 personnel and Security Forces. The Office of Primary Responsibility (OPR) for the duress words is 60 SFS/SFOSS.

3.10.1. Duress codes will be established and changed every six months or when compromise is suspected. These codes will be revealed only to those personnel who have a need-to-know.

3.10.1.1. Only personnel with unescorted entry authority into PL1 and/or PL2 areas need to know the duress codes.

3.10.2. The exercise duress word will not be changed.

3.10.3. A duress phrase will be established and changed every six months for all personnel in the grade of O-6 or higher.

3.10.3.1. The OPR for the duress phrase is 60 SFS/SFOSE.

3.11. Free Zones. Within a restricted area, free zones may be established in connection with construction projects/military functions to facilitate the movement of equipment and personnel. A written request must be approved by 60 LG/CC and then staffed through 60 OSS/AM and 60 SFS/SFOS to establish the free zone.

3.11.1. TACAMO free zone requests will be submitted to the 60 AMW/CC for approval. The request must be coordinated through VQ-3 and 60 SFS.

3.11.2. All requests must be submitted sufficiently in advance of the start date to allow coordination and will contain the following information: Contract number, project number, name and address of contractor, expected start date, expected completion date, description of work to be performed, location of free zone (include map), number of contractor personnel, and proposed route of travel to and from free zone.

3.11.3. The boundary for the free zone will be clearly marked using ropes and stanchions, cones, or other available delineating equipment.

3.11.4. Surveillance over the boundary of the free zone will be maintained by the organization or agency associated most directly with the project, as determined by the Support Group Commander (60 SPTG/CC), and the installation chief, Security Forces (60 SFS/CC). The free zone will be closed and secured at the end of the normal working hours for project personnel.

3.11.5. No PL resources will be parked or placed within the boundaries of a free zone.

3.11.6. All Free Zones within PL 1/2 areas must be cleared by Security Forces at the end of the duty day.

3.12. Entry Control Points (ECPs). All personnel entering a restricted area will do so only through an authorized ECP. All ECPs are clearly marked with either a sign, a 4-6 inch white line, or both. The following are the active ECPs for each restricted area:

3.12.1. TACAMO. There is one active ECP for the TACAMO aircraft parking area. The ECP is fitted with a vehicle and pedestrian entrapment area.

3.12.2. MPA. There are five vehicle/pedestrian ECPs, one fuels only ECP, and one temporary pedestrian ECP within the MPA.

3.12.2.1. The pedestrian ECP located adjacent to aircraft parking spot 251 will only be utilized via prior coordination of TCP, 60 AMW Protocol, and SFCC.

3.12.3. The 900 ramp restricted area has two vehicle/pedestrian ECPs.

3.12.4. During periods of increased FPCON, ECP closure will be determined by the ISC.

3.13. Visiting Restricted Areas. Visitors are any personnel without a valid need to enter a restricted area to perform mission essential duties. Utilize the following procedures for unofficial visits and photography inside the following restricted areas:

3.13.1. TACAMO. All individuals wanting to escort visitors or take photos within the TACAMO area must be in possession of a signed letter from the VQ-3/OIC, and must show this letter to the EC upon entry to the area and the CIS prior to taking any photos.

3.13.2. Protection Level 3 Mass Parking Area. All individuals wanting to take visitors or photos within the MPA for non-official business purposes must first report to the Security Forces Control Center (SFCC) located in Building 380A.

3.13.2.1. The on-duty controller will verify unescorted entry privileges via the individual's RAB.

3.13.2.2. The controller will then contact the senior maintenance individual at the TCP via telephone. The senior maintenance person will approve a tour.

3.13.2.3. The controller will then grant permission to escort the visitors.

3.14. Mutilated RAB. A mutilated badge is defined as any badge where the data is unreadable or where the laminate has peeled to allow uninhibited access to the picture.

3.14.1. Report all instances of a mutilated RAB to your unit security manager immediately upon discovery.

3.14.2. If a mutilated RAB is confiscated by Security Forces personnel, a receipt of the AF Form 52 will be given to the bearer.

3.14.2.1. The hand receipt must be presented to the individual's unit security manager and a new badge must be issued.

3.14.3. A hand receipt for a confiscated RAB does not grant unescorted entry into a restricted area. If a RAB is confiscated, the individual must be escorted until a new RAB is issued.

3.15. Ramp Security. TCP will notify the SFCC in the event of maintenance stoppage and security change over. The Security Forces ESRT will conduct a check of the aircraft and all hangars with the senior maintenance supervisor on duty prior to assuming security.

3.15.1. All aircraft hatches must be secured during security change over. All aircraft hatches must be secured regardless of security status if no maintenance or launch is expected within a twelve-hour period.

3.15.2. Keep hangar doors secured and locked when not in use if PL resources are present. During security change over, all hangar access points must be secured and locked.

3.16. Travis AFB Security Education and Training (SET) Program. Each unit must assign in writing a security education representative and forward the letter to the Installation Security Constable.

3.16.1. Each unit will perform Phase I orientation for each individual prior to them acquiring a RAB.

3.16.1.1. Phase I orientation training will include all information contained in TAFB Pamphlet 31-101, *Security Education and Training* as well as reference telephone numbers to the HELPING HAND/COVERED WAGON hotlines, CRIMESTOP hotline, and 911 telephone reporting.

3.16.2. The Installation Security Constable will perform a minimum of seven random SET exercises per month inside TAFB restricted areas to assess the security awareness of support forces personnel.

3.16.3. SET exercises are graded on a GO/NO GO system.

3.16.3.1. SET exercise NO GO reports are immediately forwarded to the failing unit's commander for correction.

3.16.3.2. Monthly SET exercise reports for GO exercises are forwarded to the passing unit's commander for information.

3.16.4. Each unit will conduct Phase II refresher training on an annual basis as part of the unit's ancillary training program.

3.16.4.1. Phase II refresher will contain all information listed in Paragraph [3.16.1.1](#).

3.17. Photography, Video, and Audio Recordings. Official photography is permitted at all times with prior notification to TCP and SFCC.

3.17.1. Unofficial photography is permitted via a coordination letter through 60 AMW/PA, TCP, 60 OSS and 60 SFS/SFOS. A copy of this letter must be with the individual while taking photos. Also Security Forces will maintain another copy of this letter.

3.17.2. The letter will be in standard Air Force memorandum format and will include dates/times photography is requested and what will be photographed.

3.18. RAB Supporting Techniques. The following are the primary and alternate supporting techniques used to validate RABs at TAFB:

3.18.1. Primary method is *telephone or radio verification*

3.18.2. Alternate methods are *personal recognition, EAL, signature and credential check*

4. SECURITY REPORTING AND ALERTING SYSTEM

4.1. Security Reporting and Alerting System (SRAS). The security reporting and alerting system defends against widespread coordinated threats. All agencies or organizations possessing PL 1, 2, or 3 resources must implement procedures for up-channel reporting (HELPING HAND or COVERED WAGON) and for reception of a down-channel threat condition alerting message (TCAM). These pro-

cedures will ensure a rapid integration into the local and Air Force SRAS for all TAFB organizations possessing PL 1, 2, or 3 resources.

4.2. HELPING HAND Procedures. A HELPING HAND is an unclassified telephone message from anyone who detects an unusual incident, possibly hostile, that affects PL 1, 2, or 3 resources. TCP should not immediately relay the information to higher headquarters. Security Forces immediately investigates the situation.

4.2.1. The following are the manual hand signals for a HELPING HAND/COVERED WAGON situation:

4.2.1.1. Daylight hours: Personnel will wave their headgear or hand over their head in a circular motion and shout, "HELPING HAND or COVERED WAGON," as applicable.

4.2.1.2. Hours of darkness: Personnel will wave a flashlight in a circular motion and shout, "HELPING HAND or COVERED WAGON," as applicable.

4.2.2. Installation commander delegates the termination authority for HELPING HANDs down to the on-duty Security Force flight chief position. A HELPING HAND caused by duress at TCP goes up to the 60 SFS/CC, however, the flight chief may still terminate.

4.3. COVERED WAGON Procedures. A COVERED WAGON is an unclassified telephone message sent up the chain of command through the TCP to inform higher headquarters of an unusual incident, actual or probably hostile, that affects PL 1, 2, or 3 resources.

4.3.1. Upon execution of a COVERED WAGON, implement FPCON DELTA.

4.3.2. Installation commander delegates the terminating authority for COVERED WAGONs down to the CSF.

4.4. Down-Channel Reports. Down-channel reports are based upon higher headquarters evaluation along with current intelligence inputs. The system provides for rapid security alerting of all bases in the affected command, or if warranted, of all Air Force commands.

4.4.1. USAF Threat Condition Alerting Message (TCAM). This down-channel order is sent by Headquarters (HQ) USAF Operations Center to all Air Force commands in possession of or supporting PL 1, 2, or 3 resources. This order will be preceded by the command designation "USAF TCAM."

4.4.2. AMC TCAM. This down-channel order is sent by the command post of a major command to all of its bases. This order will be preceded by the command designation "AMC TCAM."

4.5. TAFB Reporting Procedures. All organizations possessing or supporting PL 1, 2, or 3 resources must develop procedures to up-channel reports of suspected or actual events affecting these resources. Notify SFCC of HELPING HAND or COVERED WAGON reports involving any PL 1, 2, or 3 resources.

4.5.1. TACAMO will develop and maintain procedures to alert SFCC by radio, telephone, or other means that an adverse event has been detected or has occurred. SFCC will notify the TCP that an adverse condition has occurred. TCP will up-channel COVERED WAGON reports to HQ AMC.

4.5.2. 60 AMW and 349 AMW will develop and maintain procedures to alert SFCC by radio, telephone, or other means that an adverse event has been detected or has occurred. SFCC will

notify the TCP that an adverse condition has occurred. TCP will up-channel COVERED WAGON reports to HQ AMC.

4.5.3. 60 SFS will develop, coordinate, and maintain procedures to alert the TCP by telephone or patrol of an alarm condition existing within a restricted area. HELPING HAND and COVERED WAGON logs will be maintained by SFCC. TCP will up-channel COVERED WAGON reports to HQ AMC.

5. PROTECTION LEVEL 4 RESOURCES:

5.1. Protection Level 4 (PL 4) designation is assigned to resources on TAFB which do not meet the definitions of PL 1, 2, or 3 resources, but for which the loss, theft, destruction, misuse, or compromise would adversely affect the operational capability of the Air Force. PL 4 resources are contained in controlled areas with owner/users being primarily responsible for security. Response is provided by Security Forces.

5.1.1. Controlled area designation should be limited to those areas requiring additional protective measures beyond the base's required positive circulation controls. The areas containing PL 4 resources are identified as, but not limited to, the facilities listed in AFI 31-101, Paragraph 22.2.5.

5.1.1.1. Areas that provide adequate protection through proper employment of circulation controls and areas that do not need the legal boundary provided by the controlled area designation sign should not be designated as controlled areas. These areas should use positive circulation control within the area.

5.1.2. Entry and circulation controls for individual controlled areas are the responsibility of the owning unit commander and must meet the requirements set forth in AFI 31-101.

5.1.3. Controlled areas must be designated in writing by the 60 AMW/CC.

5.1.3.1. 60 SPTG/CC is delegated the authority to designate munitions storage areas.

5.1.4. A facility designated as open storage for top secret material does not automatically qualify for a controlled area designation.

5.1.5. After designation as a controlled area, the facility must be marked IAW AFI 31-101. Only facilities designated by the 60 AMW/CC as controlled areas may display controlled area signs.

5.2. TAFB Controlled Areas. The following locations have been designated as controlled areas (NOT a priority listing):

5.2.1. A Bunker.

5.2.2. B Bunker.

5.2.3. Building 20, Control Tower.

5.2.4. Building 54, Base Switchboard.

5.2.5. Building 106, AFOSI Vault.

5.2.6. Building 241, WIN Room.

5.2.7. Building 24, Bays B and D, Alternate Tanker Airlift Control Center.

5.2.8. Building 241, C2 Systems/GDSS/Red Switch.

- 5.2.9. Building 241, Alternate Trans Comm.
- 5.2.10. Building 243, Base Communications Center.
- 5.2.11. Building 380A, Security Forces Control Center (combined Law Enforcement Desk/Central Security Control).
- 5.2.12. Building 381, Cashier Area, Finance.
- 5.2.13. Building 381, Vault, Finance.
- 5.2.14. Building 381, Room B511, 15 AF/DON Vault.
- 5.2.15. Building 381, Room B310a, Red Switch Room.
- 5.2.16. Building 381, Rooms F004, F005, and F006, 615 AMOG Intel Vault.
- 5.2.17. Building 680, Commissary Cashier's Cage.
- 5.2.18. Building 707, POL Fuels Lab.
- 5.2.19. Building 712, POL Bulk Storage.
- 5.2.20. Building 777, DGMC Medical Supply Vault.
- 5.2.21. Building 777, DGMC Pharmacies, first floor and second floor.
- 5.2.22. Building 828, Security Forces Armory.
- 5.2.23. Building 977, Multi-Pallet Cage.
- 5.2.24. Building 981, Special Handling Vault.
- 5.2.25. Building 1115, TACAN.
- 5.2.26. Building 1120, Glide Slope.
- 5.2.27. Building 1125, Radio Transmitter Site.
- 5.2.28. Building 1131, Localizer.
- 5.2.29. Building 1185 and 1186, RAPCON.
- 5.2.30. Building 1202, POL Management Offices and Vehicle Dispatch.
- 5.2.31. Building 1207, Localizer #2.
- 5.2.32. Building 1281, Glide Slope #2.
- 5.2.33. Building 1291, Inner Marker.
- 5.2.34. Building 1733, POL Bulk Storage.
- 5.2.35. Building 1769, POL Bulk Storage.
- 5.2.36. Building 1772, POL Bulk Storage.
- 5.2.37. Building 1773, POL Bulk Storage.
- 5.2.38. Building 1774, POL Bulk Storage.
- 5.2.39. Building 1775, POL Bulk Storage.
- 5.2.40. Building 1778, POL Bulk Storage.

- 5.2.41. Building 1795, POL Bulk Storage.
- 5.2.42. Building 1796, POL Bulk Storage.
- 5.2.43. Building 3701, VHF Omnidirectional Range (VOR).
- 5.2.44. Building P-1, Mobility Weapons Vault.
- 5.2.45. Building P-4, 60 OSS Intel Vault.
- 5.2.46. Building 787, Armed Forces Whole Blood Processing Lab (only if fully activated in support of a contingency).
- 5.2.47. 615 AMOG MARC Facilities.

5.3. Owner/User Responsibilities. All owner/user agencies will comply with all applicable chapters and Paragraphs of AFI 31-101.

- 5.3.1. Designate a primary and alternate controlled area monitor (CAM) and forward a copy of the designation letter, signed by the unit commander, to the Resource Protection Program Manager (RPPM). Update this letter annually or as additions or deletions of personnel occur.
- 5.3.2. Each unit will develop written operating procedures and coordinate through the RPPM before implementation.
- 5.3.3. Each unit will develop an entry authority list (EAL) to be used in conjunction with other positive entry and circulation control techniques. Forward a copy of the EAL, signed by the unit commander, to the RPPM. Update this letter annually or as additions or deletions of personnel occur.
- 5.3.4. CAM will notify the RPPM for any change in status of a controlled area, to include relocating to a new or existing facility, change in mission which would negate the need for controlled area designation, termination of mission, etc.
- 5.3.5. CAM will coordinate plans for free zone operations within the controlled area with the RPPM before implementation.
- 5.3.6. CAM will conduct initial and follow up controlled area training for personnel authorized unescorted entry to the controlled area. The RPPM will oversee the training process and assist as necessary.

5.4. IDE Requirements. All owner/user agencies will comply with all applicable chapters and Paragraphs of AFI 31-101.

- 5.4.1. Designate a primary and alternate alarm monitor (AM) and forward a copy of the designation letter, signed by the unit commander/store manager or designee to the RPPM. Update this letter annually or as additions or deletions of personnel occur.
- 5.4.2. Each unit will develop written alarm operating procedures and coordinate through the RPPM before implementation.
- 5.4.3. Each unit will develop an Authorization to Arm and Disarm Facility listing. Forward a copy of the letter, signed by the unit commander/store manager, to the RPPM. Update this letter annually or as additions or deletions of personnel occur.

5.4.4. Each AM will perform alarm checks on a quarterly basis and annotate these checks on an AF Form 2530, **Alarm Test Record**. These recordings will be maintained in the resource protection folder and inspected by the RPPM during resource protection surveys. The SFCC is not required to record these tests.

5.4.5. An alarm test/duress authentication matrix will be published on a quarterly basis by the RPPM.

5.4.5.1. The AM must ensure an updated copy is obtained and kept for authentication procedures.

5.4.5.2. The AM is responsible for training all IDE users on the use of the authentication matrix.

5.4.6. All facilities equipped with an IDE system must display AFVA 31-232, **Intrusion Detection Warning Sign** on all entry points to the area unless placement of the sign would compromise the security of the area.

5.4.7. The AM must contact the RPPM prior to moving any material stored in an alarmed area to preclude an impact or change to the IDE configuration, e.g., moving an large crate in such a manner as to create a "dead spot" with an interior sensor. Also, 60 CES Alarm Maintenance must contact the RPPM prior to changing any alarm system configuration or coverage.

5.4.8. IDE requirements apply to any facility with an installed IDE system.

5.4.9. If IDE is required for the security of the facility, in the event of an IDE failure, the owner user will provide security until complete correction of the IDE.

5.5. Alarm Activation/Anti-Robbery Procedures.

5.5.1. Dispatch an appropriate number of patrols to provide total visual coverage of all entrances to the facility.

5.5.2. Upon arrival and securing of the facility by responding patrols, the SFCC will attempt to contact personnel inside the facility via telephone.

5.5.2.1. If contact is made, verify status and take appropriate authentication actions.

5.5.2.2. If contact cannot be made, a patrol will conduct a walk around of the facility to check for possible intrusion.

5.5.2.2.1. SFCC will contact the responsible building custodian to respond to the facility.

5.5.2.2.2. If nothing appears to be out of the ordinary, the custodian and a responding Security Force member will conduct a walk-through of the facility to verify everything is in order.

5.5.3. Gate closure procedures. The installation entry points will be closed for the following:

5.5.3.1. Any time a suspect has been identified.

5.5.3.2. Alarm activation from an AA&E facility.

5.5.3.3. Alarm activation from the 615 AMOG Intel Vault/Office.

5.5.3.4. Alarm activation from any of the following funds facilities:

5.5.3.4.1. Travis Federal Credit Union, Travis Federal Credit Union Central Depository, Armed Forces Bank, Armed Forces Bank Annex, or the Finance Vault.

5.6. Funds Facility Procedures. The following guidance applies to all government-owned funds storage. It does not apply to petty-cash funds or other non-official funds storage such as snack-bars or booster club funds.

5.6.1. A controlled area designation will not be given to any facility storing less than \$100,000 on a routine basis.

5.6.2. Do not store funds, precious metals, jewels, or other items of high value in any container that stores classified material or AA&E.

5.6.3. Establish written procedures for safeguarding funds and ensure that all employees comply.

5.6.4. Reduce cash-on-hand to the lowest amount required for efficient operation.

5.6.5. Use GSA-approved security containers meeting Class 1 or higher specifications when storing \$7,500 or more.

5.6.5.1. Secure funds containers on casters or containers weighing less than 500 pounds to the premises.

5.7. On-Base movement of AA&E. The following guidelines apply to any on-base movement of the listed AA&E. Refer to AFI 31-101, Attachment 10 for specific Sensitive Conventional AA&E Security Risk Categories.

5.7.1. Category I. Each Category I conveyance or integrated grouping of five or fewer conveyances moved within a controlled area or through multiple controlled areas, shall be under the constant surveillance of at least one owner/user personnel. When the movement is outside of a controlled area where the areas are geographically separated, movement between these areas shall be under constant armed guard surveillance, with two drivers for each conveyance.

5.7.2. Category II. Each Category II conveyance, or integrated grouping of five or fewer conveyances moved within a controlled area or through multiple controlled areas, shall be under the constant surveillance of at least one owner/user personnel. When the movement is outside of a controlled area where the areas are geographically separated, movement between these areas shall be under constant owner/user surveillance, with at least two drivers for each conveyance.

5.7.3. Categories III and IV. Owner/user personnel shall maintain constant surveillance of the movement within a controlled area or through multiple controlled areas. When the movement is outside of a controlled area where the areas are geographically separated, movement between these areas shall be under constant surveillance of at least one owner/user personnel for each conveyance.

5.8. Classified Information Secure Room Requirements. The following requirements must be met prior to being utilized as a secure room:

5.8.1. Room standards: The walls, floor, and roof must be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials.

5.8.2. Windows: Windows less than 18 feet above the ground shall be constructed of or covered with materials which provide protection from forced entry. The protection provided need be no stronger than the strength of the contiguous walls.

5.8.3. Doors: The access door to the room shall be substantially constructed of wood or metal. The hinge pins of outswing doors shall be peened, brazed, or spot-welded to prevent removal. The entry door must be equipped with a built-in GSA-approved X-07 electro-mechanical three position dial lock meeting **Fed-Spec FF-L-2740**. All other entrances must be blocked or otherwise disabled as entry points. They must meet the same protection standards as the entry door, but must be equipped with a manual actuated bolt lock with at least a one-inch throw.

5.8.4. Openings: Utility openings such as ducts and vents should be kept at less than man-passable (96 square inches) size. Openings larger than 96 square inches will be hardened. (Refer to **MIL HBK 1013/1A**, *Military Handbook, Designing Guidelines for Physical Security of Fixed Land-Based Facilities*). Removable panels will not be used and windows and other openings will be made man-proof by covering with number nine gauge two inch square steel mesh or one half inch steel bars no more than six inches apart.

5.8.5. An intrusion detection system (IDS) with at least two levels of detection (penetration and motion detection) must be installed. Submit a work order to 60 CES requesting the installation. Coordinate with the RPPM for design and implementation requirements.

5.8.6. Coordination must be made through 60 SFS/SFAI prior to utilizing a facility as a secure room.

5.9. Controlled Area Construction Requirements. All controlled areas must meet the following physical construction requirements unless otherwise specified in higher instruction.

5.9.1. Building Requirements: The facility must be a permanent fixed structure on a concrete foundation or equivalent. Mobile trailers may be used on a temporary basis, not to exceed six months.

5.9.2. Room standards: The walls, floor, and roof must be of permanent construction materials; i.e., plaster, gypsum wallboard, metal panels, hardboard, wood or other materials offering resistance to, and evidence of unauthorized entry into the area. Walls shall be extended to the true ceiling and attached with permanent construction materials.

5.9.3. Windows: Windows less than 18 feet above the ground shall be constructed of or covered with materials which provide protection from forced entry. The protection provided need be no stronger than the strength of the contiguous walls.

5.9.4. Doors: The access door to the room shall be substantially constructed of wood or metal. The hinge pins of outswing doors shall be peened, brazed, or spot-welded to prevent removal. A cipher combination lock on the main entrance is recommended but not required. A deadbolt lock with a manual actuated bolt lock with a minimum of a one-inch throw is required on all doorways. All other entrances must be blocked or otherwise disabled as entry points. They must meet the same protection standards as the entry door.

5.9.5. Openings: Utility openings such as ducts and vents should be kept at less than man-passable (96 square inches) size. Openings larger than 96 square inches will be hardened. (Refer to MIL HBK 1013/1A). Removable panels will not be used and windows and other openings will be

made man-proof by covering with number nine gauge two inch square steel mesh or one half inch steel bars no more than six inches apart.

5.9.6. IDS is not required unless stipulated in higher guidance, however all controlled areas are recommended to have a minimum of one level of IDE (penetration).

5.9.7. Large open areas such as parking lots or POL/LOX storage areas must be fenced with a six foot chain link fencing with at least one outrigger.

5.9.7.1. The area should have manual or automatic vehicle/pedestrian gates that provide the same level of security as the fencing.

5.9.8. Lighting. All controlled areas that are entire Buildings or large open areas shall possess point lighting on all entry points. Area/boundary lighting must provide sufficient illumination to detect an unauthorized individual during hours of complete darkness prior to that individual's arrival at the resource.

5.10. Resource Protection Folder. Any facility that is designated a controlled area certified for open storage of classified or stores more than \$1,000 in government-owned funds will maintain a resource protection folder on the premises.

5.10.1. The resource protection folder will contain, as a minimum, the following applicable items:

5.10.1.1. A copy of the most recent resource protection survey.

5.10.1.2. A copy of the most recent anti-robbery exercise report.

5.10.1.3. Entry Authority List to the area.

5.10.1.4. AF Form 439, **Robbery Checklist** and AF Form 440, **Bomb Threat Aid**.

5.10.1.5. Resource protection training documentation.

5.10.1.6. Funds storage authorization letter.

5.10.1.7. Consolidated plan that includes, as a minimum, the following applicable items:

5.10.1.7.1. Entry/exit control procedures.

5.10.1.7.2. Funds handling procedures.

5.10.1.7.3. Bomb threat procedures.

5.10.1.7.4. Emergency evacuation procedures for fires, etc.

5.10.1.7.5. Owner/user personnel training requirements and where training is to be documented.

5.10.1.7.6. Internal circulation control procedures.

5.10.1.7.7. Anti-robbery procedures.

5.10.1.7.8. IDE system operation instructions.

5.10.1.8. Letters of appointment for the following positions:

5.10.1.8.1. Funds custodian.

5.10.1.8.2. Controlled area monitor.

5.10.1.8.3. Alarm monitor.

5.10.1.9. AF Form 2530, **Alarm Test Record**.

5.10.1.10. Controlled area designation letter signed by the installation commander.

5.10.1.11. Munitions/firearms storage designation letter signed by the Support Group Commander.

6. NORMAL SECURITY OPERATIONS:

6.1. Normal Security Operations. Normal security operations are those daily security activities implemented during non-emergency conditions in support of PL resources. A combination of Security Forces personnel, equipment aids, facilities, procedures and personnel of other units form resources supplying the normal security operations. Restricted areas are enclosed by physical barriers/red lines and are posted with restricted area signs at the entry point and on the perimeter boundary. Within each area, security is provided from available resources in accordance with applicable system security standards.

6.1.1. Contingency actions for normal and expanded security operations are included in ISP 31-99, *Installation Security/Resource Protection Plan*.

6.2. Assumptions. The following assumptions are made and apply to the normal security protection of TAFB and priority resources within.

6.2.1. The base threat analysis contains current enemy capabilities, intentions and limitations.

6.2.2. Protection level resources could be targets for sabotage by terrorist groups, individuals, or a general war enemy desiring to damage one or more of these resources for personal reasons or gains.

6.2.3. A general war enemy terrorist group or individual could engage in subversion, espionage, and intelligence gathering regarding priority resources.

6.2.4. A security system cannot be made totally infallible. It is impossible to design a security system to provide total protection for all operational resources from various types of attacks.

6.2.5. The base Physical Security Program must maintain a state of physical security for priority resources which will deter the initiation of hostile operations and counter the local threat.

6.3. Enemy. Refer to the ISP 31-99, Annex B.

6.4. Friendly. Federal, state, county and municipal law enforcement agencies provide direct support to Security Forces when requested and consistent with personnel available and statutory and jurisdictional limitations. Consideration must be given to the sensitivity (classification) of threat and intelligence information.

6.5. Mission. The mission of normal security operations is to provide security for PL resources assigned to or present on TAFB. The following capabilities must be maintained in support of priority resources:

6.5.1. Detection of Unusual Occurrences. Assigned personnel must be constantly alert to detect unusual, suspicious, and hostile occurrences within or near restricted areas.

6.5.2. Up-Channel Notification. Once an unusual, suspicious, or hostile act (HELPING HAND or COVERED WAGON) is detected, the initiation of an immediate alarm to the affected area and SFCC is required.

6.5.3. On-Scene Assessment. Responding Security Forces must assess the situation to determine if it is hostile or non-hostile and if further response is needed by Security Forces and other base agencies or units. If assessed as hostile, the appropriate threat condition (FPCON) and associated actions will be implemented. If assessed non-hostile, the situation will be terminated.

6.6. Execution.

6.6.1. Concept of Operations. Under normal security operations, Security Forces and other base agencies carry out their daily activities while Security Forces remain on a normal work schedule. All agencies and squadrons maintain the capability to fulfill the security capabilities as outlined in this instruction. Security Forces must provide adequate security for the priority resources possessed according to applicable system security standards.

6.6.2. Tasks.

6.6.2.1. Chief, Security Forces (CSF) will:

6.6.2.1.1. Ensure procedures are developed, assigned personnel are trained, proficiency is maintained through exercises and evaluations, and support aids (i.e., instructions, checklists, charts, operating instructions (OIs) and special security instructions (SSIs), as required) are developed to support normal security operations.

6.6.2.1.2. Implement a recall, when necessary.

6.6.2.2. 60 SFS Operations Officer (SFO) will:

6.6.2.2.1. Ensure procedures are developed outlining Security Forces actions in support of normal security operations.

6.6.2.2.2. Ensure assigned personnel are trained, unit proficiency is maintained through exercises and evaluations, and support aids (i.e., checklists, charts, OIs, SSIs, as required) are developed to support normal security operations.

6.6.2.2.3. Recall and form the Security Forces battle staff, when necessary.

6.6.2.3. Security Forces Control Center (SFCC), and Flight Chief (FC) will:

6.6.2.3.1. Implement appropriate checklists and up-channel COVERED WAGON and HELPING HAND reports.

6.6.2.3.2. Exercise command and control of all Security Forces.

6.6.2.3.3. Notify all posts and patrols, enroute teams, key agencies, and key personnel of any required security actions.

6.6.2.3.4. Coordinate and request civilian authority assistance, when needed.

6.6.2.3.5. Implement appropriate plans, regulations and operating instructions in support of normal security operations.

6.6.2.4. NCOIC, Security Forces Vehicle Section (SFTMV) will coordinate with the transportation squadron to ensure sufficient operational vehicles are available to support normal secu-

rity operations. Additionally, the vehicle Section is responsible to ensure required numbers of vehicles are made available to support expanded security operations contingencies outlined in ISP 31-99.

7. INSTALLATION ENTRY AND CIRCULATION PROCEDURES:

7.1. Installation Jurisdictions. TAFB operates under two types of jurisdictions: Exclusive and Proprietary.

7.1.1. Exclusive Jurisdiction. Exclusive jurisdiction gives the federal government the exclusive right to prosecute offenses occurring therein. Generally, the military will dispose of all cases involving military personnel for offenses committed in areas of exclusive federal jurisdiction. Civilians who commit offenses in areas of exclusive federal jurisdiction will be turned over to civilian Federal authorities for disposition.

7.1.1.1. Exclusive jurisdiction at TAFB includes the area south of Travis Avenue beginning with the sidewalk and the length of Travis Avenue; from the portion of Bodin Circle where it intersects with Hickam Avenue to the flightline to include the active runway and perimeter road. Command housing and the base water storage area also fall under exclusive jurisdiction.

7.1.2. Proprietary Jurisdiction. The military exercises the rights of property owner only. There has been no formal “granting away” of “acceptance” by the federal government of criminal jurisdiction over purchased or leased land. The military does have criminal jurisdiction (UCMJ) over military personnel in these areas.

7.1.2.1. Proprietary jurisdiction at TAFB includes the area north of Travis Avenue beginning where the roadway meets the sidewalk on the south side of Travis Avenue. This includes all of the housing with the exception of command housing, water treatment facility and the golf course.

7.2. Patrol Sectors: These are designed to aid in the command, control and sector coverage of the entire installation. Patrol sector(s) assignments will be given by the flight chief at guard mount and may be altered based on the number and availability of patrols.

7.2.1. Patrol Sector 1: Boundaries run from the Main Gate, encompassing areas northwest of Travis Avenue and First Street to Bradley Avenue. Zone includes the Water Storage Facility and Center School area.

7.2.2. Patrol Sector 2: Boundaries run northeast of Travis Avenue and First Street, through Bradley Street, encompassing Patriot Village, Command Housing, Collins Drive behind Vandenberg Housing to Vandenberg Drive, Airlift Drive, and Challenger to Travis Avenue.

7.2.3. Patrol Sector 3: Boundaries run southeast of Travis Avenue, bounded to the east by Challenger, bounded to the North by Hangar Avenue, and bounded to the west by the Aero Club.

7.2.4. Patrol Sector 4: Boundaries run south of Hangar Avenue, E Street, Vandenberg Drive, Collins Drive to Perimeter Road, encompassing South Gate, “B” Bunker and “A” Bunker.

7.3. Installation Entry Points. Travis AFB has five installation entry points with different operating hours.

7.3.1. Main Gate: Located at Air Base Parkway and Travis Avenue. This gate is open 24 hours a day, seven days a week.

7.3.2. Hospital Gate: Located on Parker Road adjacent to David Grant Medical Center. This gate is open from 0600 to 1800 hours, Monday through Friday. This gate is closed on weekends and holidays.

7.3.3. North Gate: Located on Burgan Boulevard adjacent to command officer housing. This gate is open from 0600 to 2100 hours, seven days a week.

7.3.4. South Gate: Located on Peterson Road adjacent to the hotel ramp. This gate is open from 0600 to 0800 hours and from 1530 to 1730 hours, Monday through Friday. All munitions laden vehicles are required to use this gate for deliveries to Travis AFB. This gate is closed on weekends and holidays.

7.3.5. Forbes Gate: Located on Forbes Street adjacent to Golden West Middle School. During the school year, this gate is open from 0630 to 0900 hours and 1330 to 1630 hours, Monday through Friday. This gate is closed on weekends and holidays and when school is not in session.

7.4. Normal Installation Entry Procedures:

7.4.1. Any vehicle with a valid and properly displayed DD Form 2220, **US Coast Guard Decal**, VA Decals/ID Cards/Appointment slips, Computer Generated Passes or AF Form 75 will be allowed entry. Vehicles possessing an expired DD Form 2220 will be stopped and the driver identified. If the driver does not possess any of the documentation listed in Paragraph **7.4.1.1.**, have the driver remove the DD Form 2220 from the vehicle. If the individual refuses to remove the decal deny the individual access to the base. Individual with proper credentials to gain unescorted entry will be directed to Pass and Registration, to renew the decal. At no time will the gate guard remove the decal from the vehicle due to liability reasons.

7.4.1.1. Drivers presenting a valid DoD, US government or military identification card will be allowed entry without a pass. Conduct a hands-on inspection of all ID media to detect expired or fraudulent ID cards.

7.4.2. Vehicles not displaying any documents indicated above:

7.4.2.1. Will be stopped and the operator identified.

7.4.2.2. Personnel must show a valid driver's license and be asked the purpose of their visit. Upon presentation of a driver's license and valid reason for entry, they will be instructed to proceed to the Visitor Control Center to obtain a computer-generated pass or AF Form 75. **Exception:** Visitors attending a "by invitation" organized event such as a wedding, club function, or reception do not need to produce a copy of the invitation. An authenticated guest list will be posted on the gate. However, if you feel something is not right, you may detain and verify with the SFCC.

7.4.3. The following will be allowed to proceed without a pass. **NOTE:** You can stop anyone if there is anything suspicious. If you identify something suspicious ensure you take the drivers license and/or ID card to reduce the risk of that individual fleeing. And if the situation warrants, take possession of the vehicle keys.

7.4.3.1. Clearly marked federal, state, and local government vehicles and their occupants while on official business. If serving a warrant, have them or SFCC contact base legal. Pride Industries (housing maintenance) and Baker Telephones vehicles are treated as government vehicles.

7.4.3.2. Marked taxis. **NOTE:** You may question a taxi driver if coming on base to pick up a fare, especially between 2300 and 0500. Verify the taxi driver's picture taxi license.

7.4.3.2.1. Commercial buses will be boarded. Passengers without some form of government/military identification will be briefed that they are to remain on the bus while transiting the base. Failure to comply with this instruction will be viewed as trespassing and they will be prosecuted for violating Title 18, USC, Section 1382/trespassing on a federal installation.

7.4.3.3. Clearly marked commercial and delivery vehicles. Ask vehicle drivers to see a bill of lading. The bill of lading may be a hard copy or a computer (laptop/palmtop) version.

7.4.3.4. Unmarked police/law enforcement vehicles will be allowed to proceed upon presentation of credentials (only if on official business). If serving a warrant, have them contact base legal.

7.4.4. Civilian emergency vehicles (such as ambulances and fire trucks) when "running code 3 (lights and sirens) will be stopped if the gate sentry has not received pre-notification from SFCC. Find out what the emergency is and relay to SFCC for verification. Do not delay longer than necessary.

7.5. Normal Installation Visitor Procedures:

7.5.1. The Visitor Control Center (VCC) is located on Air Base Parkway just prior to the Main Gate. The VCC is normally open from 0600 to 2200 seven days a week.

7.5.2. All visitors must have a sponsor (personnel with a valid DoD, VA, FBI, and/or diplomatic credentials do not need a sponsor and may enter any posted gate upon clearance from the entry controller). A sponsor is any active duty or retired military personnel (to include the spouse) and/or Department of the Air Force civilians. The sponsor will be responsible for the behavior and actions of their visitors while on the installation. The sponsor will contact the VCC in person or by telephone prior to the visitor's arrival and provide the name of the visitor and where they will be going. In order to receive a pass, the visitor must have a valid state approved photo identification, which will be physically inspected for validity. If driving a vehicle, the visitor must produce a valid driver's license and current registration.

7.5.3. The VCC will not issue passes exceeding six-months. Passes in excess of six-months will be issued at Pass and Registration, Building 381, Room C101. Personnel who do not reside on the installation will only be allowed to sponsor individuals for 24 hours. (Exceptions: Personnel conducting official business, for example contractors and medical patients.)

7.6. Base Entry/Exit Point Check (BEPC) Procedures: BEPCs are conducted to protect the security of the command and to protect government property.

7.6.1. BEPCs are conducted at the direction of the 60 AMW/CC, or designee (60 SPTG/CC) The information for example, time frame, location, and which method of random selection (e.g., every tenth vehicle) will be sent to the SFO who will then distribute the information through Security Forces Operations Branch to the Flight Chief. Flight Chiefs are responsible for ensuring the BEPC is conducted at the designated place and time.

7.6.2. All BEPCs will be annotated in the blotter as "Random Antiterrorism Measures/Base Entry or Exit Point Checks." Include all appropriate information, for example location, personnel

involved, and the results. If BEPCs are not conducted, the Flight Chief will document the reason in the blotter.

7.6.3. The BEPC may be cancelled at the Flight Chief's discretion based on inclement weather (raining) or if all of the patrols are tied up on priority dispatches that make continued checking impractical.

7.6.4. The BEPC will also be documented on the general purpose form provided by SFOS. When completed, forward the form to SFOS along with the shift's other daily paperwork.

7.6.4.1. Fill out the form with: Date/time, location, description of vehicle, identity of vehicle operator, name of personnel conducting checks and selection criteria for checks (i.e., every tenth vehicle, out).

7.6.4.2. Describe any discovered contraband finds. Write negative in "Results" column if there were no finds.

7.6.5. Conducting the BEPC.

7.6.5.1. The Flight Chief will designate the appropriate number of personnel (normally two with at least one NCO when available) to conduct the check.

7.6.5.2. MWD teams must be utilized if available.

7.6.5.3. The gate sentry who is conducting the vehicle count will advise the selected vehicle operator of the BEPC and instruct the driver where to pull over.

7.6.5.4. Prior to conducting the BEPC, patrolmen will identify themselves and brief the selected vehicle operator of the random entry or exit point checks. For their safety, and the safety of the SF personnel, brief the driver to turn off the engine, engage the parking brake, open up all doors and compartments and have all passengers exit the vehicle.

7.6.5.4.1. Instruct vehicle operators to open areas of concealment for inspection to include trunk, glove compartment, and any storage compartments.

7.6.5.4.2. Only the installation commander or 60th Support Group Commander/Deputy may approve forcible entry into locked compartments when probable cause exists for a search. This must always be coordinated first with SJA.

7.6.5.5. Also subject to inspection are any hand-carried parcels to include purses, backpacks, and briefcases. This applies even if the operator or passenger(s) takes the hand-carried parcels out of the vehicle.

7.6.5.6. Instruct all passengers and the driver to stand in a safe area away from traffic and other hazards.

7.6.5.6.1. Military Working Dog (MWD) handlers must warn all parties involved that an MWD is being used.

7.6.5.7. Vehicles will be inspected for illegal explosives, weapons, contraband and government property.

7.6.5.7.1. Personnel found to be transporting classified material on or off the installation must have an authorization letter from the unit commander and/or DD Form 2501, **Courier Authorization Card**, and an "Exemption Notice from Inspection" letter.

7.6.5.8. Government property will not be removed from the base without written approval of the individual's unit commander or designee. Personnel removing government property from the base must have in their possession either a government bill of lading or an AF Fm 1297, **Temporary Issue Receipt**. If the property has been issued to the individual (i.e., Security Forces equipment, etc.), a government bill of lading or AF Form 1297 is not required. If needed, the individual's unit can be contacted for verification.

7.6.5.8.1. If an MWD alerts on a vehicle, detain the driver and vehicle.

7.6.5.8.2. Conduct a walk around of the vehicle looking for contraband in plain view.

7.6.5.8.3. Ask the driver for consent to search the vehicle. If refused, contact SJA to confirm probable cause exists for search authorization.

7.6.5.8.4. After completing the inspection of the vehicle, resume your count to determine the next vehicle to stop.

7.6.6. Refusals:

7.6.6.1. Inbound vehicles:

7.6.6.1.1. For civilian controlled vehicles, ask the driver for identification and advise all occupants they can't enter the base unless the vehicle is examined.

7.6.6.1.2. Advise the driver that refusal to allow the check may result in loss of base driving privileges, revocation of base registration, barment from the base or other actions.

7.6.6.1.3. For civilian controlled vehicles, conduct a walk-around visual assessment of the vehicle to determine if any probable cause exists (contraband in plain view) to warrant further detention or search authorization. If no probable cause exists, the driver will be informed that a report AF Fm 3545, **Incident Report** will be accomplished and sent to the Installation Commander for action.

7.6.6.1.4. If refusal is still given, the patrolman will ask the driver to scrape the DD Fm 2220. If the operator refuses, the patrolman will scrape the decal.

7.6.6.1.5. A BOLO will be sent to all gates to deny the vehicle entry in case the operator attempts to reenter using a different gate.

7.6.6.1.6. Military operator: All military personnel will be advised that these checks were ordered by the 60th AMW Commander or SPTG/CC and failure to obey the order will result in their immediate apprehension for disobeying a lawful order.

7.6.6.1.7. If they still refuse, place them under apprehension and conduct a walk around of the vehicle looking for contraband/government property in plain view. Contact SJA to determine if probable cause exists to warrant search authorization.

7.6.6.2. Outbound vehicles:

7.6.6.2.1. Identify the driver and all occupants for subsequent action.

7.6.6.2.2. Advise the driver that refusal to allow the check may result in loss of base driving privileges, revocation of base registration, barment from the base or other actions.

7.6.6.2.3. For civilian controlled vehicles, conduct a walk-around visual assessment of the vehicle to determine if any probable cause exists (contraband on the floor, etc.) to warrant

further detention or search authorization.

7.6.6.2.4. Tell all occupants to exit the vehicle and open all locked compartments. Advise the occupants these directions constitute a lawful order based on the authority of the installation commander.

7.6.6.2.5. If not complied with, contact the SJA to determine if enough probable cause exists to seek search authorization. If SJA concurs, then contact the Support Group Commander for search authorization. (An AF Form 1176 will be completed.)

7.6.6.2.6. If the SJA does not concur with your request, then ask the driver to scrape the DD Form 2220. If the operator refuses, the patrolman will scrape the decal. Accomplish an AF Form 3545.

7.6.6.2.7. Military operator: All military personnel will be advised that these checks were ordered by the 60th AMW Commander and failure to obey the order will result in their immediate apprehension for disobeying a lawful order.

7.6.6.2.8. If they still refuse, place them under apprehension and conduct a walk around of the vehicle looking for contraband/government property in plain view. Contact SJA to determine if probable cause exists to warrant search authorization.

7.7. Base Barment Procedures.

7.7.1. Under the authority of 50 U.S.C. 797 and DoD 5200.8, installation commanders may deny access to the installation through the use of a barment order. Installation commanders may not delegate this authority. (Reference AFI 31-101, Paragraph 8.9.)

7.7.2. Once probable cause exists to request base barment of the individual, the process will start with an immediate removal from Travis AFB. 60 AMW/CC may delegate only the authority for immediate removal of an individual from the installation to the 60th Support Group Commander.

7.7.3. After the individual is removed from the installation, all paperwork will be forwarded to the 60th Security Forces Reports and Analysis Section (60 SFS/SFAA). SFAA will forward a formal package requesting barment to the 60 AMW/CC for review. Barment orders will be coordinated through the base legal office. Documentation supporting the barment must be kept for the period of the barment.

8. NORMAL TASKS FOR ASSIGNED UNITS:

8.1. Installation Commander. The installation commander establishes on-base restricted areas and provides protection for Air Force priority resources. The 60 AMW will participate in associate units' security exercises and inspections when requested and with prior coordination.

8.2. 60th Security Forces Squadron (SFS) Commander will:

8.2.1. Program for and maintain sufficient Security Forces and equipment for the protection of USAF priority resources and establish post priority lists. This list will include basic and contingency responses, apprehension, and suspect transport procedures. Should it become necessary, lower priority posts may be curtailed to man higher priority posts. ([Attachment 5](#))

8.2.2. Establish procedures to ensure the protection of classified publications located and controlled within the 60 SFS/SFCC. Duplicates of classified charts and publications required for unit staff work will be kept in approved classified containers within unit administrative offices.

8.2.3. Staff, create, update and maintain necessary OIs to implement the policies and procedures required by this instruction.

8.2.4. Establish and maintain locally planned verification features in the preparation of restricted area badges as a safeguard to preclude counterfeiting.

8.2.5. Ensure all requests for deviations are processed according to AFI 31-101.

8.2.6. Assist unit commanders in developing a tailored security education and motivational program meeting the needs of unit personnel, evaluate security awareness of base personnel, and assist commanders in resolving security awareness problems.

8.2.7. Adhere to and enforce aircraft security requirements identified within AFI 31-101 and this instruction.

8.3. 60th Air Mobility Wing Command Post (AMW/CP) will:

8.3.1. Notify all agencies possessing priority resources of any actual or simulated contingencies requiring implementation of terrorist threat conditions (FPCON) or defense conditions (DEFCON) changes and notify the CAT when activated.

8.3.2. Maintain primary responsibility for up and down-channel reporting.

8.3.3. Provide secure storage and maintain strict control over classified publications and material kept within the CP.

8.3.3.1. Maintain security for aircraft transient classified material.

8.3.3.2. Develop and maintain the capability to provide up and down-channel reporting to the National Military Command Center (NMCC).

8.3.4. Notify the SFCC of any changes to aircraft PL status due to contingency upgrades or maintenance status.

8.3.5. Notify the SFCC of all aircraft movement.

8.4. 60th Logistics Group Supply (60 LG/LGS) will:

8.4.1. Provide supply support as required by the 60 SFS.

8.4.2. Establish an operating schedule for the Fuels Service Station that will ensure Security Forces vehicles can remain at least 75% full.

8.5. 60th Civil Engineer Squadron (CES) Commander will:

8.5.1. Provide roads and ground maintenance in and around TAFB restricted areas, logistics movement routes, hot cargo pads and other identified areas where priority resources are located. Priority consideration will be given to repair discrepancies identified or noted.

8.5.2. Provide top priority maintenance for all existing security facilities, fences, gates, lights and other physical security aids within and surrounding all TAFB restricted areas.

8.5.3. Maintain a source of permanent power for the 60 AMW flightline restricted area and permanent standby electrical power to operate security lighting and intrusion detection systems for TACAMO.

8.5.4. Plan for, provide and deploy, physical security aids in support of base FPCON or DEFCON plans.

8.5.5. Ensure all vegetation within the TAFB restricted areas to include the 30-foot clear zone outside the area does not exceed eight inches.

8.5.6. Provide lighting support during darkness and periods of reduced visibility for the 60 SFS as required.

8.5.7. Provide fire department response as needed.

8.6. Explosive Ordinance Disposal (EOD) will:

8.6.1. Provide routine training to Security Forces personnel upon request about identification and precautions of improvised explosive devices (IED).

8.6.2. Provide emergency response to explosive incidents or bomb threats. EOD personnel will standby to respond to TACAMO during bomb threats.

8.6.3. Set up necessary instructions to implement the policies and requirements of this instruction.

8.7. 60th Air Mobility Wing Airfield Management (60 OSS/AM) will:

8.7.1. Visually survey all areas of the flightline on a regular basis and report all suspicious activity or unauthorized over-flights to either CP or SFCC.

8.7.2. Notify the SFCC of the arrival or planned arrival of any transient aircraft.

8.7.3. Notify SFCC via crash net of all in-flight, ground, and other emergencies affecting operational resources.

8.8. 60th Medical Group (MDG). 60 MDG will provide emergency medical support and services as determined by the director of base medical services.

8.9. TACAMO OIC, VQ-3 will:

8.9.1. Notify SFCC of any unusual occurrences or personnel within the TACAMO restricted areas.

8.9.2. Notify SFCC of aircraft arrivals and departures.

8.10. 60th Transportation Squadron (LGT) commander will:

8.10.1. Provide vehicles and priority maintenance for vehicles assigned to the 60 SFS.

8.10.2. Provide replacement vehicles to the 60 SFS to maintain mission essential levels.

8.10.3. Provide additional vehicles during Peons or during contingency actions as outlined in ISP 31-99.

9. INSTALLATION SECURITY COUNCIL (ISC):

9.1. ISC, acting on behalf of the installation commander, is responsible for identifying and establishing restricted areas; monitoring all ongoing security enhancement projects through completion;

reviewing and approving deviation requests; developing entry control procedures for free zones; and reviewing and approving TAFBI 31-101 and ISP 31-99. The ISC conducts an annual review of all security deviations within the calendar year and validates compensatory measures, costs, and estimated completion dates. All matters concerning existing restricted areas or the establishment of new restricted areas will be submitted to the installation commander through the 60th Security Forces Squadron commander (60 SFS/CC). The ISC will meet semi-annually.

9.2. ISC Membership. 60th AMW vice commander (60 AMW/CV) will chair the ISC.

9.2.1. ISC voting membership consists of the 60 AMW/CV; 349th AMW vice commander (349 AMW/CV), 60 SFS/CC as recorder; 60th Support Group commander (60 SPTG/CC); 60th Logistics Group commander (60 LG/CC); 60th Operations Group commander (60 OG/CC); 60th Medical Group commander (60 MDG/CC) (only a voting member on issues pertaining to MDG), and OIC, VQ-3 (only a voting member on issues pertaining to TACAMO).

9.2.2. Other agencies and subordinate squadrons may be invited to ISC meetings but will not hold a voting position (OSI, 60 CES, 60 CS).

9.3. The following personnel must brief at each ISC: OSI on threat analysis; NCOIC, Physical Security (60 SFS/SFOSS) on current security deviations and any future deviations, security trends; RPPM (60 SFS/SFOX) on crime trend analysis; and the Installation Security Constable (60 SFS/SFOSSC) on SET exercise trends and overall installation security awareness.

9.4. ISC Working Group. 60th Security Forces Squadron Force Protection Branch Operations Officer (60 SFS/SFO) will chair the ISC working group.

9.4.1. The ISC Working group consists of: 60 SFS/SFO, 60 SFS/SFOS, 60 SFS/SFOSS, SFOSA, OSI, SPTG, LG, OG, MG, CE, CS, SE, as well as representatives from agencies responsible for items of discussion. The ISC Working group will meet as a need arises or as determined by the chairperson.

10. WEAPONS REGISTRATION, STORAGE, AND TRANSPORTATION:

10.1. Privately Owned Weapons (POW) Registration. All weapons stored in government quarters or in the Security Forces Armory must be registered through the RPPM. The following does not apply to weapons stored off the installation.

10.1.1. Each owner of a POW will contact their unit orderly room and obtain an AF Form 1314, **Registration of Privately Owned Firearms** form.

10.1.1.1. Each weapon stored on the installation must be listed on AF Form 1314. This form must be updated any time a weapon is added or removed from the owner's collection.

10.1.1.2. AF Form 1314 must be signed by the owner's unit commander.

10.1.2. After signing by the unit commander, the AF Form 1314 will be transported by the owner to the RPPM for entry into the database. After entry, the form will be maintained with the RPPM.

10.1.3. Prior to out processing the installation, the owner must contact the RPPM in person to retrieve the AF Form 1314.

10.1.4. Any weapon defined as illegal to possess according to California law or local statutes must be stored IAW with this instruction.

10.1.4.1. If a person PCS's to Travis AFB with a weapon deemed illegal in the state of California, the weapon must be maintained in the SF armory.

10.1.4.2. The weapon may be withdrawn from the armory only upon PCS or separation orders. The orders must be reviewed by the armorer prior to the release of the weapon.

10.2. POW Storage. Dormitory residents are required to maintain their weapons inside the Security Forces Armory/Building 828. Armory personnel maintain AF Form 1314 on weapons they store until the individual leaves Travis AFB or removes the weapon permanently.

10.2.1. When a person wishes to store a POW the armorer will verify ownership by DD Form 2. After verifying ownership, the armorer receipts for the weapon(s) using AF Form 1297, **Temporary Issue Receipt** completed in duplicate copies, 1 for the individual and one copy per weapon. AF Form 1297 will include the make, model, caliber, serial number, discrepancies, locker and slot location and the owners name, rank, SSAN, and duty phone. The original AF Form 1297 is given to the owner and the copies are placed in the POW receipt book. Each weapon will have a tag attached with the owners last name and the corresponding number on the AF Form 1314.

10.2.2. The Armory is not sanctioned to store POW munitions. No POW munitions will be accepted. Owners will be instructed to dispose of the ammo properly.

10.2.3. The armorer stores the weapons in the POW locker and updates the content list. The armorer will fill out the AF Form 1314 in duplicate copies as done with the AF Form 1297 and inform the individual to report back to the armory with the completed AF Form 1314 signed by their commander within three (3) working days.

10.2.3.1. If the owner fails to report to the armory within three (3) working days, the owner or the owner's unit commander will be contacted to ensure the paperwork is properly completed.

10.2.4. Upon receipt of POW's for storage, the armorer ensures the owner has the following items in their possession:

10.2.4.1. DD Form 2 and their copy of the AF Form 1314 or AF Form 1297.

10.2.5. The armorer will place the POW in the POW locker, lock the locker and notify the NCOIC or ANCOIC and reseal the locker. Seal deletions/replacement will be annotated on the appropriate seal log.

10.2.6. The armorer will then:

10.2.6.1. Ensure that both the owner and the unit commander have signed the AF Form 1314.

10.2.6.2. Give the first copy of the AF Form 1314 to the owner and retain the copies to replace the AF Form 1297.

10.2.7. The Armory is for the storage of firearms only and will not be held accountable for any other items.

10.2.8. Temporary Issue: POWs may be temporarily issued, annotate the AF Form 1314 to reflect weapons that are temporarily issued out.

10.2.9. DO NOT ISSUE (DNI): If any information is received that personnel are barred from their weapons, the armorer will take the following actions:

10.2.9.1. Annotate name, rank, and the organization of the barred individual and individual

making notification.

10.2.9.2. The armorer will follow DNI procedures and will red tag the weapon with appropriate information.

10.2.9.3. Request written notification of barment, which will be posted in the DNI Section of the POW book.

10.2.9.4. A written notification from the individuals unit commander is required before they will be allowed access to their POW.

10.2.10. Inventory. Inventory will be conducted every time the seal is broken for additions or deletions.

10.2.10.1. Inventory records are maintained for 90 days.

10.2.11. Lost/Misplaced POW Reporting: In case of a lost or missing weapon, the NCOIC, Armory, SFCC, and Investigations will be notified immediately to initiate an investigation.

10.3. POW Transportation. Compliance with California law for POW transportation is mandatory.

10.3.1. A GOV may not be utilized for transportation of POWs at any time.

10.4. Government Owned Weapons (GOW) Transportation. Support Forces personnel must utilize government transportation to transport GOWs.

10.4.1. Security Forces personnel may transport marksmanship weapons in POVs. No GOWs may be taken into base housing in a POV for any reason.

11. Forms Prescribed: AF Form 2586, AF Form 1199, AF Form 52, AF Form 1109, AF Form 2530, AF Form 439, AF Form 440, AF Form 1297, AF Form 3545, AF Form 1176, AF Form 1314, DD Form 577, DD Form 2220, DD Form 2501, DD Form 2, AFVA 31-232.

JACK F. PETERS, Col, USAF
Director of Wing Staff

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

1. AF Policy Directive 31-1, *Physical Security*
2. DOD Directed 5200.8, *Security of DOD Installation and Resources*
3. Section 21, *Internal Security Act of 1950* (Act of September 1959; Chapter 1024, 64 Statute
4. 1005, 51 United States Code (USC) 797)
5. AFI 31-501, *Personnel Security Management Program*
6. TAFBI 13-103, *Vehicle Operations on the Flightline*
7. TAFB Pamphlet 31-101, *Security Education and Training*
8. MIL HBK 1013/VA, Military Hand book, *Designing Guidelines for Physical Security of Fixed Land Based Facilities*
9. 60 AMW ISP 31-99, *Installation Security/Resource Protection Plan*
10. Title 18, USC, Section 1382/*Trespassing on a Federal Installation*
12. DOD 5200.8, *Security of DOD Installation and Resources*

Attachment 2

EXAMPLE OF CALL SIGN-POST TITLE-WEAPON ARMED WITH, AND RADIO PRIORITY
FORMAT

Call Sign	Post Title	Weapon Armed With	Radio Priority (Highest to lowest priority)
Security 5	ECP TACAMO	M-16	1.
Security 1	CIS TACAMO	M-16	2.
Security 2	CIS TACAMO	M-16	3.
Security 3	CBS TACAMO	M-16	4.
Security 10	CBS TACAMO (IDS Compensatory Measure)	M-16	5.
Security 11	CBS TACAMO (IDS Compensatory Measure)	M-16	6.
Security 4	ISRT Leader (TACAMO)	M-16	7.
Security 4a	ISRT Member (TACAMO)	M-16	26.
SF Control	Controller #1	M-9	8.
Security 6	ESRT Leader (MPA)	M-16	9.
Security 6a	ESRT Member	M-16	27.
SF Control	Controller #2	M-9	10.
Security 7	ISRT Leader (MPA) (1-32 Acft on Station)	M-16	11.
Security 7a	ISRT Member	M-16	28.
Police 1	Senior Patrol	M-9	12.
Police 9	Main Gate	M-9	13.
Security 8	Security Patrol (MPA) (33-48 Acft on Station)	M-9	14.
Security 9	ISRT Leader (MPA) (49-64 Acft on Station)	M-16	15.
Security 9a	ISRT Member	M-16	29.

Call Sign	Post Title	Weapon Armed With	Radio Priority (Highest to lowest priority)
Police 2	Patrol	M-9	16.
Police 10	North Gate	M-9	17.
VCC	Visitor Control	M-9	18.
VCC	Visitor Control	M-9	30.
Police 3	Patrol	M-9	19.
Police 4	Patrol	M-9	20.
Police 9a	Main Gate Member/ Mobile	M-9	21.
Police 11	South Gate	M-9	22.
Police 8	Hospital Gate	M-9	23.
A-1/B-1/C-1/D-1	Flight Chief	M-9	24.
Police 12	Forbes Gate	M-9	25.

Attachment 3**HOW TO COMPLETE AF FORM 2586**

GENERAL INSTRUCTIONS: The AF Form 2586 must be typed or printed if using electronic form in duplicate. Handwritten AF Form 2586's will not be accepted. Sections I, II, III, and IV will be signed and coordinated, as applicable, prior to being hand carried to the Pass and Registration Section for issuance of an AF Form 1199. Facsimile signatures are not authorized. The original copy of the AF Form 2586 will be returned to the Unit Security Manager upon issuance of the AF Form 1199 and maintained on file.

SECTION I: Identification should match the individuals ID card. If ID card is not current, the individual must have ID card updated before issuance of AF Form 1199.

SECTION II: The unit commander, section commander, or the unit security manager must sign this section. The signature of one of these individuals indicates a favorable investigation was completed and that Security Education and Motivation Training was conducted. A DD Form 577 must be on file at the Pass and Registration Section for persons authorized to sign this Section, as well as Section IV.

SECTION III: Duty

- a. Duty: Give AFSC, job title, or duty position and need for access into the restricted area.
- b. List clearance type, and date of current security clearance.

SECTION IV: Restricted Area Coordination: List in numerical sequence the restricted area code numbers on the AF Form 2586. The area-coordinating official will indicate concurrence/nonconcurrence and date and sign the applicable part. This Section will be signed by the 60 AMW Commander or his/her designated representatives. (See Paragraph [2.3.2](#) for list of designated individuals.)

SECTION V: Restricted Area Badge Issue. Completed by AF Form 1199 issuing agency.

Attachment 4**COMPLETING DD FORM 577, SIGNATURE CARD**

The DD Form 577 is very important. The signatures in Sections II, IV, and the remarks Section (if adding or deleting an area or name change) on the AF Form 2586 are verified by the DD Form 577. An AF Form 2586 cannot be processed for a restricted area badges if signatures on both forms do not match.

1. NAME: Type last name, first name, middle initial, and title i.e., squadron commander or unit security manager.

2. PAY GRADE

3. DATE: Date the Form was completed and signed.

4. Your organizational address, to include your squadron, and your duty phone.

5. Signature of the person indicated in Block 1.

6. TYPE OF DOCUMENT OR PURPOSE FOR WHICH AUTHORIZED: Be specific. Include the Section(s) of the AF Form 2586 as well as the specific area(s), which the individual may sign for. For example, unit security managers complete Section I, II, and III of the AF Form 2586. Commanders or coordinating/approving officials complete Section IV of the AF Form 2586 and the restricted area(s) approved to sign for.

7. NAME OF COMMANDING OFFICER: Type commanding officer's last name, first name, and middle initial.

8. PAY GRADE

9. SIGNATURE OF COMMANDING OFFICER

NOTE: THE NAME THAT IS IN BLOCK 1, CAN NOT BE THE SAME AS IN BLOCKS 7 AND 9.

Attachment 5**(SAMPLE FORMAT FOR REPORTING LOST OR STOLEN RESTRICTED AREA BADGES)****(APPROPRIATE LETTERHEAD)**

01 Jun 00

MEMORANDUM FOR 60 SFS/SFOXI

FROM: (Security Manager's office symbol, grade, and last name, phone number)

(Address and Building #)

Travis AFB, CA (Zip Code)

SUBJECT: Report of Investigation -Lost Restricted Area Badge

1. Following is the report of investigation into the circumstances surrounding the loss of Restricted Area Badge #00-00, Card #P0***** which was issued to: SSgt William A. Doe, SSN XXX-XX-XXXX, 60 CES.
2. At approximately 1030 hours, 09 April 91, SSgt Doe reported to me the loss of his Restricted Area Badge. His RAB was lost while deployed to Desert Shield/Storm in Saudi Arabia, September 90 through March 91. He discovered the RAB missing before returning to duty at Travis AFB and continued to search for it.
3. A review of available unit documents revealed that the badge was issued to SSgt Doe on 28 April 89, and allowed him unescorted entry into areas 2, 4, and 11.
4. Security Forces Operations Control Center, Pass and Registration, and the local units who own, or are responsible for, the affected areas and resources therein, were notified as of 1100 hrs 09 April 91.
5. The forgoing actions constitute my investigation of the circumstances and facts surrounding the loss of SSgt Doe's RAB. All the information obtained thus far substantiates SSgt Doe's report of the situation. Therefore, I believe further investigation is unwarranted.

6. CONCLUSION: As a result substantiated by this investigation, I conclude that SSgt Doe, William A., did in fact, at unknown location in Saudi Arabia lose his RAB, and that he made a reasonable and diligent effort to locate the badge. There is no indication of either malicious intent or foul play. Therefore, I attribute the loss to SSgt Doe's failure to adequately secure the badge while he was deployed.

7. RECOMMENDATION: This being his first incident, I recommend that SSgt Doe be administered a written reprimand, to be entered into his personnel file.

8. The forgoing conclusion and recommendations completes this report.

JOHN E. MOORE, TSgt, USAF
Unit Security Manager

Attachments:

1. Original AF Form 2586
2. AF Form 1168 or individuals statement

1st Ind. ()

(DATE)

I concur with the findings and recommendations of the security manager.

FRED C. JONES, Colonel, USA

60 CES COMMANDER

Attachment 6**STATEMENT**

At approximately 0630, 9 May 99, I, SSgt Doe, entered echo ramp to paint equipment sheds. I remembered showing my restricted area badge to a Security Force member on Echo Ramp, and clipping it to my shirt pocket. I do not remember taking the badge off when I left the area. All I can remember is being concerned about taking a shower to remove the smell of paint from my self. I did not return to work on 9 May 99. Upon arriving for work on 10 Jul 99, I found that my Restricted Area Badge was missing. I returned to echo ramp but I could not find the badge; the personnel working in the area assisted in the search. Our efforts proved fruitless. The only possible place I can think of, where I could have lost it, was between the ramp and my home off base. I think my badge must have fallen off my shirt. I reported this incident to 1Lt Smith, who referred me to MSgt Williams. This statement is true and correct to the best of my knowledge.

Signature block here

Attachment 7

(SAMPLE FORMAT FOR LETTER IN LIEU OF AN AF FORM 2586)

(APPROPRIATE LETTEHEAD)

01 Jun 00

MEMORANDUM FOR 60 SFS/SFOXI

FROM: (Security Manager's office symbol, grade, last name, phone number)
(Address and Building #)
Travis AFB, CA (Zip Code)

SUBJECT: Letter in Lieu of AF Form 2586

1. This letter is to inform your office the AF Form 2586, Unescorted Entry Authorization Certificate for SSgt William Doe is missing. The Restricted Area Badge card # is P0***** and the Badge # is E00-***.
2. If there are any questions, feel free to call me at extension 4-****.

JOHN E. MOORE, TSgt, USAF
Unit Security Manager