

25 JULY 2002



Security

**INSTALLATION SECURITY INSTRUCTION/
RESOURCE PROTECTION**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: 6 SFS/SFOR (SrA McQueen)
Supersedes MACD Sup 1 to AFI 31-209,
10 March 1997

Certified by: 6 AMW/CC (Maj Gen (Sel) Hodges)
Pages: 61
Distribution: F

In accordance with Air Force Instruction 31-101, *The Air Force Installation Security Program*, each installation possessing or routinely supporting protection level resources must have an installation security instruction (ISI). The installation commander must issue, approve, and assure implementation of this instruction as an installation directive. This security instruction forms the foundation and directs procedures for normal day-to-day resource protection operations and the establishment of Protection Level 4/ Controlled area operations. The Privacy Act of 1974 affects this instruction, and is applicable to all military and civilian personnel assigned, attached, or detailed to duty at MacDill Air Force Base (AFB) who require access to the controlled areas assigned to MacDill AFB. This program requires the continuous attention of commanders, supervisors, and all other base personnel. This instruction also serves as the basis for security planners to develop checklists and operating instructions. Use this instruction in conjunction with AFI 31-101. Increased security operations and/or contingency actions are covered in MacDill AFB Operation Plan (OPLAN) 31-101, Installation Security Plan (ISP). The MacDill AFB installation commander issues this directive in accordance with the Internal Security Act of 1950 (50 U.S.C 797).

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Chapter 1—INSTALLATION SECURITY COUNCIL (ISC)	6
1.1. The Commander, 6th Air Mobility Wing (6 AMW/CC)	6
1.2. The following agencies are designated primary members of the ISC.	6
1.3. Special Voting Members.	6
1.4. The ISC is vital to the security planning process. The council will:	7

Chapter 2—LOCAL THREAT ASSESSMENT/VULNERABILITIES 8

- 2.1. This chapter discusses the local threat assessment and vulnerabilities associated with MacDill AFB. 8
- 2.2. Local Threat Assessment. 8
- 2.3. Vulnerabilities. 8

Chapter 3—RESOURCE PROTECTION PROGRAM 9

- 3.1. Resource Protection Program. 9
- 3.2. Unit Monitors. 9
- 3.3. Survey/Self-Inspections. 9
- 3.4. Survey Requirements. 9
- 3.5. Anti-robbery/Area Penetration Exercises. 9
- 3.6. Unit Responsibilities/Anti-robbery Procedures. 10
- 3.7. Bomb Threats. 10
- 3.8. Installation gates will be closed for all AA&E facilities alarm activation. 10

Chapter 4—SURVEY/INSPECTION PROCEDURES 11

- 4.1. This chapter establishes surveys/inspections procedures. 11
- 4.2. 6 SFS/SFOR and 6 CES will conduct an initial survey 11
- 4.3. 6 SFS/SFOR will conduct biennial surveys on all facilities 11
- 4.4. 6 SFS/SFOR will conduct annual anti-robbery exercises at all weapons facilities ... 11

Chapter 5—EQUIPMENT AND FACILITIES 12

- 5.1. Implement measures to protect Air Force equipment and facilities 12
- 5.2. Fencing. 12
- 5.3. Lighting. 12
- 5.4. Warning Signs. 13
- 5.5. Intrusion Detection Equipment (IDE). 13

Chapter 6—CONTROLLED AREAS 17

- 6.1. This chapter legally defines areas containing Protection Level 4 resources. 17
- 6.2. Controlled areas are established and in accordance with AFI 31-101. 17

Chapter 7—ALARMED FACILITIES 22

- 7.1. This chapter establishes which alarm systems will be installed in facilities as directed in AF and DoD directives and instructions. 22

7.2. Unit commanders will ensure all appropriate alarmed facilities are established as a controlled area in accordance with **Chapter 6** of this instruction and AFI 31-101. ... 22

7.3. The commander of the owning agency 22

7.4. Activating/deactivating alarms. 22

7.5. Testing Alarms. 22

Chapter 8—PROTECTION OF ARMS AMMUNITION AND EXPLOSIVES (AA & E) 24

8.1. This chapter explains what facilities may store arms, ammunition, or explosives ... 24

8.2. Requests for approval of AA&E storage will be forwarded to 6 AMW/CC 24

8.3. The following facilities are designated as controlled areas and are authorized to store AA&E as indicated: 24

Chapter 9—MUNITIONS ESCORTS 26

9.1. Upon receiving notification of a munitions escort 26

9.2. If the munitions escorted are category 1 or 2 26

9.3. Duty Hours: 26

9.4. Non-duty Hours: 26

9.5. If the munitions are category 3 26

9.6. Concept of Operations. 26

9.7. Definitions: 28

9.8. Tasks. 28

9.9. Coordinate instructions: 29

Chapter 10—PROTECTION OF FUNDS 30

10.1. This chapter discusses protection of funds. 30

10.2. Classified Material. 30

10.3. Controlled Area Designation for Funds Facilities. 30

10.4. Funds Storage. 30

10.5. Funds Storage Containers. 31

10.6. Operating Instructions. 32

10.7. Deviations. 33

10.8. Use of IDE. An effective IDE is a prime deterrent in preventing the loss of funds by theft. 33

Chapter 11—FUNDS ESCORTS 34

11.1. This chapter applies to all security forces 34

11.2.	Funds Escorts	34
Chapter 12—VEHICLE AND VISITOR INSTALLATION ENTRY AND RELATED TASKS		35
12.1.	This chapter establishes entry requirements for MacDill AFB	35
12.2.	Vehicle and Pedestrian Entry Requirements.	35
12.3.	Visitor Control.	38
12.4.	Safe Haven Procedures.	39
12.5.	Classified Shipments.	39
12.6.	Munitions Shipments.	39
12.7.	Newly Assigned Personnel.	39
12.8.	Foreign National Defector.	39
12.9.	Demonstrations.	39
12.10.	College Access Badges and Term Entry Passes.	39
Chapter 13—INSTALLATION PATROL DUTIES		42
13.1.	This chapter applies to all security forces	42
13.2.	Responsibilities:	42
13.3.	Vehicle Requirements.	43
13.4.	Installation Patrol Duties.	43
13.5.	Patrol Sectors.	43
Chapter 14—BASE ENTRY POINT CHECKS		44
14.1.	This chapter applies to all security forces	44
14.2.	Responsibilities.	44
14.3.	Procedures.	44
14.4.	Contraband.	45
Chapter 15—CONTROL OF PRIVATELY OWNED WEAPONS (POWS)		46
15.1.	This chapter discusses the control of privately owned weapons (POW) at MacDill AFB.	46
15.2.	Military or civilian personnel will not:	46
Chapter 16—JURISDICTION		50
16.1.	This chapter discusses military jurisdiction.	50
16.2.	MacDill AFB exercises exclusive jurisdiction	50

16.3. There are four entry points to MacDill AFB: Dale Mabry, MacDill, Bayshore, and Port Tampa gates. 50

16.4. Title 18, The United States Code, and the United States Constitution 50

16.5. All military members are subject to the UCMJ. 50

16.6. If you have any questions regarding the jurisdiction on MacDill AFB, contact the legal office. 50

Attachment 1—GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS 51

Attachment 2—OWNER/USER ANTI-ROBBERY PROCEDURES 54

Attachment 3—ALARM ACCESS AUTHORIZATION LIST 55

Attachment 4—REQUEST FOR A COLLEGE ACCESS BADGE 57

Attachment 5—REQUEST FOR A TERM ENTRY PASS (AF FORM 75) 59

Attachment 6—DESIGNATION OF CONTROLLED AREA LETTER 61

Chapter 1

INSTALLATION SECURITY COUNCIL (ISC)

1.1. The Commander, 6th Air Mobility Wing (6 AMW/CC), has combined the Installation Security Council (ISC) and the Resources Protection Executive Committee into one cohesive working group. The Vice Commander (6 AMW/CV) will chair the ISC and review and approve meeting minutes. The Chief, Security Forces (CSF), is designated as the recorder and will maintain all records and files pertaining to the ISC. The CSF will also prepare the ISC agenda and schedule all meetings. Membership will include a senior representative from each unit on base whose participation the commander deems necessary. The ISC will meet semiannually at a minimum or more frequently as required to address open items or other areas pertaining to the security of Protection Level resources.

1.2. The following agencies are designated primary members of the ISC. Primary members (or their designated alternates) will attend each ISC meeting.

Commander, 6th Medical Group (6 MDG/CC)
Commander, 6th Logistics Group (6 LG/CC)
Commander, 6th Support Group (6 SPTG/CC)
Commander, 6th Operations Group (6 OG/CC)
Commander, 6th Supply Squadron (6 SUPS/CC)
Commander, 6th Civil Engineer Squadron (6 CES/CC)
Commander, 6th Services Squadron (6 SVS/CC)
Commander, 6th Security Forces Squadron (6 SFS/CC)
Commander, 6th Communications Squadron (6 CS/CC)
Commander, 6th Operations Support Squadron (6 OSS/CC)
Commander, 6th Transportation Squadron (6 TRNS/CC)
Air Force Office of Special Investigations (AFOSI), Detachment 323
Safety (6 AMW/SE)
US Special Operations Command, Provost Marshall (USSOCOM/SMO)
US Central Command, Provost Marshall (USCENTCOM/CCPM)

1.3. Special Voting Members. These personnel will consist of commander/director level when issues directly affecting operations are addressed.

1.3.1. Units/Organizations that are affected will be notified prior to or decided upon through the permanent voting members. Approval authority for these issues must not extend below the deputy or vice level.

1.3.2. Issues affecting special voting members will most often only pertain to resource protection and security operations.

1.4. The ISC is vital to the security planning process. The council will:

- 1.4.1. Select and designate restricted areas, restricted area entry control points, and controlled areas.
- 1.4.2. Ensure the installation provides adequate personnel, equipment, and facilities for protection level resources.
- 1.4.3. Monitor on-going security enhancement projects.
- 1.4.4. Review and approve entry control procedures for free zones.
- 1.4.5. Review both the installation security plan (ISP) and the ISI Volume 1 and 2 annually.
- 1.4.6. Conduct annual reviews of all deviations in effect.
- 1.4.7. Authorize the installation CSF to task other base agencies through the 6th Air Mobility Wing Plans (6 AMW/XP) to prepare applicable annexes pertaining to contingency operations for the installation security plan (ISP).

Chapter 2

LOCAL THREAT ASSESSMENT/VULNERABILITIES

2.1. This chapter discusses the local threat assessment and vulnerabilities associated with MacDill AFB. Due to sensitivity of these items, the office of primary responsibility (OPR) and main source document is all that will be listed in this instruction.

2.2. Local Threat Assessment. The local AFOSI, Detachment 323, will prepare and update a local threat analysis annually. The threat assessment will be briefed at every ISC meeting. After annual review, the intelligence will be disseminated to the base security forces through the CSF. To review a copy of this assessment, contact AFOSI, Detachment 323. This threat will also be published in the ISP.

2.3. Vulnerabilities. The 6 SFS Antiterrorism/Force Protection Section will prepare and update the vulnerabilities associated with MacDill AFB based upon Joint Service Integrated Vulnerability Assessments (JSIVA). This document will be updated as required and incorporated into the local threat assessment and briefed at the ISC.

Chapter 3

RESOURCE PROTECTION PROGRAM

3.1. Resource Protection Program. This program is designed to protect Protection Level (PL) 4 and designated controlled area within the confines of MacDill AFB. The installation Resource Protection non-commissioned officer (NCO) (6 SFS/SFOR) is the OPR for all resource protection issues on the installation.

3.2. Unit Monitors. Unit security managers may also act as resource protection program monitors for agencies that do not handle, store, or process large volumes of classified information.

3.3. Survey/Self-Inspections. A representative from 6 SFS/SFOR will schedule program surveys. Units must conduct annual controlled area self-inspections and forward the results to 6 SFS/SFOR.

3.4. Survey Requirements. 6 SFS/SFOR, Resource Protection Manager, will conduct program surveys for any unit or agency at the request of the unit commander and will conduct periodic program surveys as follows:

3.4.1. Annually for all arms, ammunitions, and explosives (AA&E) facilities storing category I, II, or III arms or munitions. Facilities storing category IV AA&E may be surveyed annually along with category I, II, or III facilities or every 2 years if surveyed separately.

3.4.2. Annually for funds facilities storing \$100,000 or more and the 6th Comptroller Squadron (6 CPTS) Accounting and Finance Office. Funds facilities storing or maintaining less than \$100,000 are exempt from survey requirements and controlled area designation. However, custodians of minor funds are encouraged to contact 6 SFS/SFOR to obtain survey materials so they may manage their own programs.

3.4.3. All other controlled areas not included in paragraphs 3.4.1. and 3.4.2. above will be surveyed at a minimum rate of 25 percent per year or at least once every 4 years.

3.5. Anti-robbery/Area Penetration Exercises. Only authorized representatives from the 6 SFS/SFOR and 6 SFS Standardization Evaluation Section (6 SFS/SFE) can conduct and evaluate anti-robbery exercises for alarmed facilities monitored by the 6 SFS Security Forces Control Center (SFCC). Under no circumstances will an activity initiate an alarm at their activity to test the security forces response without first coordinating the exercise with 6 SFS/SFOR and SFOR. Anti-robbery and controlled area penetration exercises are conducted as follows:

3.5.1. Annually for category I, II, and III AA&E resources. Category IV AA&E facilities may be exercised along with category I, II, and III facilities or once every 2 years if done separately.

3.5.2. Funds facilities storing or maintaining over \$100,000 and the 6 CPTS Accounting and Finance Office will be exercised annually. Funds facilities storing or maintaining less than \$100,000 are exempt from exercise requirements. However, funds custodians are encouraged to request training exercises through 6 SFS/SFOR.

3.5.3. All other controlled areas will be exercised at a minimum rate of 25 percent per year, which equates to at least once every 4 years.

3.6. Unit Responsibilities/Anti-robbery Procedures. Units must develop anti-robbery procedures and coordinate them through the 6 SFS/SFOR before implementation. Unit custodians must train all personnel who work in areas that handle or store funds, precious metals, medical warehouse supply items, controlled substances, or arms, ammunition and explosives (AA&E) at least annually on anti-robbery procedures. Document the training and maintain records in unit files.

3.6.1. Units and individuals will be evaluated on their ability to complete the following anti-robbery procedures:

3.6.1.1. Remain as calm as possible.

3.6.1.2. Read the exercise card and state to an evaluator they understand the exercise. Unless the robber asks for it, keep the note as evidence (do not voluntarily hand it back).

3.6.1.3. Sound the alarm as soon as possible (i.e., activate duress alarm or call 911) without making noticeable movements that would tip off the robber.

3.6.1.4. Do nothing to jeopardize the safety of individuals being robbed or innocent bystanders.

3.6.1.5. Obtain an accurate description of the robber. As soon as possible after the robber departs, have all witnesses complete an AF Form 439, *Robbery Checklist*. Give completed forms to responding security forces personnel.

3.6.1.6. As soon as possible, notify coworkers and the on-duty supervisor of the situation.

3.6.1.7. Immediately after the robber departs the area, if feasible and without jeopardizing the safety of individuals, determine the direction of travel and mode of transportation. Do not follow immediately behind the robber.

3.6.1.8. Secure the area and prohibit entry to or exit from the area by personnel other than responding security forces.

3.6.1.9. Preserve the crime scene. Do not allow personnel to touch or walk around areas where the robber was.

3.6.1.10. Identify witnesses, but do not compare notes.

3.6.1.11. When told to do so by the Control Center Operator (CCO) or alarm monitor, designate a person to meet responding security forces outside the area.

3.7. Bomb Threats. AF Form 440, **Bomb Threat Aid**, must be readily available for each government telephone on MacDill AFB.

3.8. Installation gates will be closed for all AA&E facilities alarm activation. For all other alarm activation, gate closure will be determined by Chief, Security Forces or Security Forces Operations. Gate closure procedures are identified in 6 SFS FOI 31-1.

Chapter 4

SURVEY/INSPECTION PROCEDURES

4.1. This chapter establishes surveys/inspections procedures.

4.2. 6 SFS/SFOR and 6 CES will conduct an initial survey on all new or remodeled facilities prior to usage. Any facility that fails to meet the required standards will not be permitted to store any type of PL4 resource until standards are met and verified by SFOR and CES.

4.3. 6 SFS/SFOR will conduct biennial surveys on all facilities handling or storing under \$100,000, and all controlled areas that are not subject to more stringent standards. During the off year, these facilities will conduct self-inspections.

4.4. 6 SFS/SFOR will conduct annual anti-robbery exercises at all weapons facilities, controlled substance storage facilities, and funds facilities handling or storing over \$100,000. All other areas not falling under this criteria will be exercised one facility per month. Anti-robbery exercise reports will be completed by the Chief, Security Forces (CSF) and forwarded to the facility's staff agency chief through the appropriate commander. Replies to exercise reports will be submitted through the CSF to 6 SFS/SFOR not later than the established suspense date. Reports will remain on file until superseded. Anti-robbery exercises will be rated as indicated below.

4.4.1. *OUTSTANDING*. Performance or operation far exceeds mission requirements. Procedures and activities are carried out in a superior manner. Resources and programs are very efficiently managed and are of exceptional merit with no discrepancies noted. To obtain this rating, all criteria defined must be met.

4.4.2. *EXCELLENT*. Performance or operation exceeds mission requirements. Procedures and activities are carried out in a superior manner. Resources and programs are very efficiently managed and relatively free of discrepancies. To obtain this rating, all criteria defined will be met.

4.4.3. *SATISFACTORY*. Performance or operation meets mission requirements. Procedures and activities are carried out in an effective and competent manner. Resources and programs are efficiently managed. Minor discrepancies exist, but they do not limit mission accomplishment.

4.4.4. *MARGINAL*. Performance or operation does not meet some mission requirements. Procedures and activities are not carried out in an effective manner. Resources and programs are not efficiently managed. Discrepancies exist that could impede or limit mission accomplishment. Corrective actions taken by the resource facility will be reviewed by 6 SFS/SFOR within 5 days after receiving the report. Any repeat discrepancies will automatically result in this rating.

4.4.5. *UNSATISFACTORY*. Performance or operation does not meet mission requirements. Procedures and activities are not carried out in an adequate manner. Resources and programs are not adequately managed. Significant discrepancies exist that seriously limit mission accomplishment. A follow-up survey will be conducted by 6 SFS/SFOR within 30 days after receiving the report of corrective actions taken by the facility. Numerous repeat discrepancies will automatically result in this rating.

Chapter 5

EQUIPMENT AND FACILITIES

5.1. Implement measures to protect Air Force equipment and facilities by carefully integrating staffing requirements, procedures, and physical protection elements (fencing, lighting, locks, IDE, and so on).

5.2. Fencing. A fence (or any other natural barrier that offers equivalent protection) serves as a legal and physical demarcation of the area boundary. It provides an obstacle to entry that must be breached by an intruder. A breach of the barrier by anyone without authorization is a prima facie evidence of illegal entry. Since a fence serves as a deterrent to the casual intruder, and a legal definition of an area generally excluded to the public, it should be considered a primary aid for resource protection applications. Beyond these functions, a fence line of any other barrier that is not under periodic observation by owner/user personnel has very limited utility. Heavy investment beyond standard fence criteria contained in this instruction is usually not justified.

5.2.1. Controlled area fencing. The acquisition of fencing for protecting a controlled area will be governed by the following rules.

5.2.1.1. If the area or resource to be protected does not lend itself to the principles of “deterrence at the area boundary” or “surveillance of the area boundary,” then fencing is not effective and may be unnecessary. For example, a controlled area located within a building would not justify fencing the entire building. When fencing is impractical and the importance or value of the resource to be protected is significant, fencing is constructed or configured in accordance with AFI 31-101, Chapter 23.

5.2.2. Temporary Barriers. A temporary barrier may consist of nothing more than a rope barrier or demarcation line to call attention to the fact that passage is restricted.

5.3. Lighting. The psychological effect of lighting can be an invaluable aid to protecting resources. The following guidelines must be considered.

5.3.1. Design. Interior and exterior lighting systems, including fixtures, lamps, and associated primary and backup power and control components and wiring must be carefully designed. Engineering and security forces personnel must coordinate closely on each phase of lighting projects to ensure all requirements such as illumination levels, uniformity, color rendering, and energy conservation are adequately identified and addressed.

5.3.1.1. All lighting projects must be coordinated with the flying safety office if they might in any way affect night aircraft operations.

5.3.1.2. The effect on vulnerability to air attack and base blackout procedures must be considered in areas subject to air attack.

5.3.2. Types of lighting. Four basic lighting systems may be used depending on the location and type of resource to be protected. Often a combination of two or more types is necessary. Before determining the type of lighting system to be installed, analyze background shading and color differences. Dark backgrounds require more illumination than light colored surfaces. Security Forces physical security personnel should influence construction plans to achieve the most cost-effective shading for enhanced illumination.

5.3.2.1. **Boundary Lighting.** Boundary lighting is usually required when the resource to be protected justifies boundary fencing. Boundary lighting covers the area outside the fence or physical barrier so that it will not only expose anyone approaching, but will also limit or restrict the vision of anyone outside the area trying to look in.

5.3.2.2. **Area Lighting.** Area lighting is designed to illuminate the area within the fence or boundary or illuminate the exterior of a building to enhance visibility.

5.3.2.3. **Entry Point Lighting.** Entry point lighting is used when an entry control point is staffed. It must be especially well lit at an entry point where an entry controller may be required to see and recognize persons at some distance.

5.3.2.4. **Special Purpose Lighting.** Special purpose lighting may include portable lights, spotlights, searchlights, or ball park lights.

5.3.3. **Special Design Considerations.** Plan and design lighting systems, switches, power lines, and supporting equipment carefully. Each must be placed so that an intruder cannot defeat the lights by simply turning them off or cutting a power supply.

5.3.4. **Replacing Lights.** The using agency is responsible for identifying defective or burned out lights. The user will replace these lights within capability or notify civil engineering within 24 hours for repair.

5.4. Warning Signs. Warning signs are normally displayed at the boundary of each controlled area and at each entrance to a controlled area so they can be easily read by persons approaching on foot or in a vehicle.

5.4.1. **Placement of Signs.** Maximum spacing between boundary signs will usually not exceed 100 yards. However, exceeding this distance may be necessary when placement of a sign is not feasible due to terrain features.

5.4.2. **Sign Specifications.** The most commonly used signs are designated as Air Force Visual Aids (AFVA). The visual aids are mounted on aluminum, sheet wood, or metal backing. Locally designed, bilingual signs are authorized in foreign countries. Wording for these signs will comply with host nation agreements and local laws and should, to the extent possible, conform to color and design of the basic AFVA. Sizes and uses for AFVA are as follows:

5.4.2.1. AFVA 31-203, **Controlled Area Sign (18"x15")**, is used to post controlled area boundaries and personnel entry points such as cashier's cages, firearms facility doors, etc.

5.4.2.2. AFVA 31-204, **Controlled Area Sign (36"x30")**, is used to post vehicle entry control points and outdoor personnel entry points.

5.4.2.3. AFVA 31-205, **Controlled Area Sign (5"x7")**, is used to post interior personnel entry points as an alternative to AFVA 31-203.

5.5. Intrusion Detection Equipment (IDE). IDE funding is the responsibility of the unit that owns or is the primary user of the facility requiring the IDE. Use of commercially leased or purchased IDE is permitted, however, the IDE must meet or exceed all DoD standards. All requests for acquisition or modification of alarm systems must be coordinated through the ISC before contract tendering. **NOTE:** Coordinate all purchases of commercial IDE with the 6th Civil Engineer Squadron and 6th Communications Squadron

to ensure capability. Most civil engineering personnel are not trained on commercial systems, so a maintenance contract with the IDE installer is highly encouraged.

5.5.1. Other Considerations. The use of specific IDE must be planned to meet actual protection requirements. In making a decision on the acquisition of any given IDE, all factors must be considered that will affect its operation and usefulness. Some of these are as follows.

5.5.1.1. The known capabilities and limitations of the equipment being considered.

5.5.1.2. The facility design and areas to be protected.

5.5.1.3. The effects of weather, air conditioning systems, air and ground traffic.

5.5.1.4. The effects of the system on the day-to-day operations of the facility.

5.5.1.5. Whether the system will be effective against any undetected intrusion from any reasonable approach into the structure or area.

5.5.1.6. When the IDE malfunctions, it must be designed to transmit a line fault message to the annunciator panel.

5.5.1.7. The proposed configuration must lend itself to protection from tampering.

5.5.2. System Considerations. Basic IDE characteristics have been identified to ensure minimum protection standards. IDE will have the following features.

5.5.2.1. Must be capable of prompt detection of any attack on the area for which it is designed to detect.

5.5.2.2. Should have a high degree of salvage value so equipment may be removed and used elsewhere.

5.5.2.3. Continental United States (CONUS) installations should operate on 110-120 volt, 50-60 Hertz AC power and have a protected backup independent power source with automatic switch-over capability to allow for continuous emergency operation for at least four hours. OCONUS should operate on local voltage.

5.5.2.4. Must have an alarm annunciator panel located at a security forces control center or other facility continuously manned on a 24-hour basis capable of notifying responding forces.

5.5.2.5. Must be reasonably flexible, that is, used to protect large and small areas with small cost differences.

5.5.2.6. Must be able to register malfunctions.

5.5.2.7. Must have a nuisance alarm rate not to exceed one per facility per 24 hours.

5.5.2.8. Must have audible and visual alarm annunciation capabilities.

5.5.2.9. Must have a line fault indication if the system fails.

5.5.2.10. Must have on or off switches and access or secure switches located inside the alarmed area unless equipped with a keypad that may be located outside the facility.

5.5.2.11. Must have good quality, dedicated communications capable pairs for transmission of the encoded system.

5.5.3. System Performance. To make sure IDE operates properly, the installation procedures or maintenance contracts must provide for timely emergency maintenance. When IDE fails, the owner or user provides on-scene surveillance of the affected area unless an approved portable IDE can be installed. In such cases, the portable IDE must provide a level of protection equal to or better than that provided by the existing IDE.

5.5.4. Stages of Alarm Protection. There are three stages of alarm protection. Naturally, the more alarms used, the more protection is afforded.

5.5.4.1. Penetration Detection. There are two types of penetration detection.

5.5.4.1.1. Complete Penetration Detection. This stage of alarm detects penetration attempts into the secure area. This includes entry through doors, windows, walls, floors, ceilings, and any other opening in the room. This is the outermost level of detection capability or the “early warning” level. Application of the stage of alarm protection requires thorough evaluation of the structure to identify all possible points of attack.

5.5.4.1.2. Boundary Detection. This stage of alarm detects penetration attempts through any facility boundary opening such as doors, windows, vents, etc. It differs from complete penetration detection in that the walls, floors, and ceilings are not protected.

5.5.4.2. Motion Detection. This type of detection is also called volumetric or space detection. It is the detection of a person inside the protected area. This is an intermediate level of protection that is very effective against the stay behind intruder, the person who hides during hours of operation and carries out a theft after a room or facility has been secured. This alarm provides backup protection to penetration sensors.

5.5.4.3. Point Detection. This stage of alarm protection detects attempts at removal of protected items inside the secure area. This is the innermost stage of detection capability of the “last line of defense.” Point detection gives the least warning in terms of reaction time to response forces.

5.5.5. Duress Alarms. The duress alarm or sensor is not a component of the three stages of alarms discussed in paragraph 5.5.4. This capability is used when duty personnel are forced to yield protected items to unauthorized persons. The duress alarm must be configured to allow personnel on duty to activate it without arousing the intruder’s suspicion. Consequently, the activation switch must be located to permit surreptitious activation.

5.5.6. Replacing IDE. The normal life of IDE is about ten years. Plan to replace IDE accordingly.

5.5.7. Testing IDE. The owner/user must test IDE with Security Forces Squadron quarterly.

5.5.8. Posting IDE Warning Signs. For all facilities protected by IDE, post AFVA 31-232, WARNING!!! THIS FACILITY IS PROTECTED BY AN INTRUSION DETECTION ALARM SYSTEM (5x8). Mark entry points of large facilities containing numerous IDE, such as non-nuclear munitions storage area (NMSA).

5.5.9. IDE Protection Requirements. User must keep the IDE control unit inside the alarm area. If the system includes a keypad, you may locate it outside the alarm area. All IDE systems must include a line supervisory capability equal to the value, sensitivity, and technical sophistication of the resource being protected.

5.5.10. Nuisance Alarms. Two or more nuisance alarms from the same facility or structure within a 24-hour period require notification to alarm maintenance personnel.

5.5.11. Master Key Systems. Master key systems may be used for two or more weapon racks stored inside an approved area. Master key systems for two or more facilities, rooms, doors, storage areas, or vaults are prohibited.

Chapter 6

CONTROLLED AREAS

6.1. This chapter legally defines areas containing Protection Level 4 resources. Only authorized personnel, designated by a unit commander, have access to controlled areas. The designation "controlled area" carries the same legal and moral restrictions as a physical barrier. Unless physical barriers are specifically required, the actual effectiveness of a controlled area may depend entirely on the security awareness of the people working in it.

6.2. Controlled areas are established and in accordance with AFI 31-101.

6.2.1. The 6 AMW/CC has delegated authority to grant unescorted entry to controlled areas to the unit commander with ownership of the area.

6.2.2. Unit commanders will identify mission essential resources and provide physical protection for those resources.

6.2.3. The list of controlled areas is a limited distribution item and is on file with SFOR, SFOX, SFO, and SFA.

6.2.4. Unit commanders will designate, in writing, a controlled area monitor, funds or weapons custodians for each controlled area. The appointment letters will identify the individual, duty phone, and areas of responsibility. The original letter will be filed at the facility and a copy will be forwarded to 6 SFS/Resource Protection Program Manager (6 SFS/SFOR). A new letter will be accomplished each time the monitor is replaced.

6.2.5. Unit commanders must ensure personnel assigned to work in controlled areas are properly trained and aware of their responsibilities for protection of resources. Training for these personnel will consist of, as a minimum, reading the facility's operating instruction initially and follow up training. This training will be documented and maintained by the controlled area monitor.

6.2.6. Unit commanders are responsible for ensuring written instructions are completed which outline specific responsibilities and protection procedures under both normal and emergency conditions. These procedures will be coordinated through 6 SFS/SFOR and posted within the controlled area. These procedures will include the following:

6.2.6.1. Copy of most recent resource protection survey.

6.2.6.2. Copy of most recent anti robbery exercise.

6.2.6.3. Entry authority list (EAL).

6.2.6.4. AF Form 439, *Robbery Checklist*.

6.2.6.5. AF Form 440, *Bomb Threat Aid*.

6.2.6.6. Resource protection training documentation.

6.2.6.7. Consolidated plan that includes the following items:

6.2.6.7.1. Entry/Exit control procedures.

6.2.6.7.2. Funds handling procedures (if applicable).

- 6.2.6.7.3. Bomb threat procedures.
- 6.2.6.7.4. Emergency evacuation procedures.
- 6.2.6.7.5. Owner/user training requirements.
- 6.2.6.7.6. Internal circulation control procedures.
- 6.2.6.7.7. Anti-robbery procedures.
- 6.2.6.7.8. Intrusion detection equipment (IDE) operating instructions.
- 6.2.6.8. Letters of appointment for the following positions:
 - 6.2.6.8.1. Funds custodian (if applicable).
 - 6.2.6.8.2. Controlled area monitor.
 - 6.2.6.8.3. Alarm monitor.
- 6.2.6.9. AF Form 2530, **Alarm Test Record**.
- 6.2.6.10. Controlled area designation letter signed by the installation commander.
- 6.2.6.11. Munitions/Firearms storage designation letter signed by 6 SPTG/CC. **NOTE:** Owner/user personnel using an entry authority list (EAL) and authorized identification media will control entry to controlled areas.
- 6.2.6.12. A resource protection folder will be maintained on each facility by the controlled area monitor/custodian and the 6 SFS/SFOR. These folders will contain, as a minimum, the following:
 - 6.2.6.12.1. Letters of designation and appointment (controlled area monitor, EALs, lock and key custodians, alarm authorization access list, etc.) by unit commander.
 - 6.2.6.12.2. Storage limitation letters.
 - 6.2.6.12.3. Initial and most current survey.
 - 6.2.6.12.4. Current resource protection and anti-robbery exercise reports and replies of corrective action.
 - 6.2.6.12.5. Documentation of controlled area/anti-robbery training.
 - 6.2.6.12.6. Copies of deviations/waivers.
 - 6.2.6.12.7. Facility operating instructions.
 - 6.2.6.12.8. Recent diagram of the facility showing all entrances/exits, location of windows, funds/weapons containers, and alarm system installed. The diagram will be prepared in two copies on 8 ½ x 11 inch bond paper and marked "FOR OFFICIAL USE ONLY." One will be forwarded to the 6 SFS/SFOR to be maintained in the facility resource protection folder, and the other will be maintained in the controlled area monitor/custodian resource protection folder. This diagram will be updated whenever modifications/alterations are made to the facility.
- 6.2.6.13. Keys for controlled areas will be safeguarded in the following manner:
 - 6.2.6.13.1. A key and lock custodian will be designated in writing to 6 SFS/SFOR.

6.2.6.13.2. Using agency supervisors will establish written procedures for the controlling of keys to all locked doors and gates leading into controlled areas.

6.2.6.13.3. Keys will not be left unattended/unsecured. When not attended or used, the keys will be stored in a metal box/cabinet and secured with a General Services Administration (GSA) approved combination lock.

6.2.6.13.4. The AF Form 2432, **Key Issue Log**, will be used to record the issuance, turn-in, and inventory of keys. The AF Form 2432 will include the signature of the person receiving the key, the date, and hour the key was issued, and the signature of the person returning the key.

6.2.6.13.5. A list will be maintained for all accountable locks and keys and a semiannual inventory of all keys and locks will be conducted and annotated.

6.2.6.13.6. When keys are lost, misplaced, or stolen, all locks affected will be recylindereed or replaced.

6.2.6.14. During hours of darkness, exterior lighting at controlled areas (especially AA&E facilities) will be illuminated, to include any perimeter lighting.

6.2.6.15. All commercially laden vehicles will be inspected by owner/user personnel before entry into the NMSA.

6.2.7. Training personnel who work in controlled areas. All personnel who work in controlled areas receive initial and follow-on training from the controlled area custodian/monitor. This training includes, but is not limited to the following:

6.2.7.1. Controlled area custodians/monitors receive training materials from the ISS Resource Protection NCO to ensure they have current guidance. Documentation of training for personnel within the controlled area will be determined by the owner/user commander. Security forces armorers will receive controlled area training from the NCOIC, Armory and have the training documented by the CSF. Units employing a flight armorer program will ensure controlled area training is completed and documented for all personnel in the program.

6.2.7.2. Properly protecting controlled area badges if issued.

6.2.7.3. Proper wear of controlled area badges if issued.

6.2.7.4. Challenging any person that at a specific time or place appears questionable. Challenging procedures will include contacting a supervisor if there is any doubt as to another person's right to be in the area, and promptly requesting security forces assistance if a person's right to be in the area cannot be verified.

6.2.7.5. Bomb threat procedures.

6.2.7.6. Entry procedures for emergency response vehicles.

6.2.7.7. Emergency egress procedures.

6.2.7.8. For an unannounced alarm activation, SFCC will contact alarm/building custodian and instruct them to respond to their facility immediately. If the alarm cannot be reset, the custodian is responsible for security of their facility until the alarm is operational.

6.2.8. Controlled area entry requirements. There are two basic qualifications for entering a controlled area: qualification and authority.

6.2.8.1. In determining a system qualification, unit commanders must balance the need for stringent entry qualifications against normal operational requirements and the sensitivity of the protected resources. Basic qualifications can range from local file checks to special investigations.

6.2.8.2. Authority to enter controlled areas is delegated to the unit commander having jurisdiction over the protected resource. Authority to enter must be given only to those personnel who need access to the area to perform official duties on a continuing and regular basis. Personnel with authority must be identified by letter as specified in paragraph 6.2.9.4.

6.2.8.3. Unit commanders will develop criteria and grant authority to enter controlled areas under their responsibility. Publish these criteria in a unit operating instruction (OI) or equivalent. All personnel who work within the controlled area are responsible for knowing and complying with the procedures.

6.2.8.4. Unless using an approved badge system, entry to controlled areas will be made using the personal recognition system. When using personal recognition, unit commanders must identify by letter those personnel authorized unescorted access to the controlled area and a copy of the letter must be maintained in a conspicuous place inside the controlled area. Personnel who need escorted entry to perform official duties must be escorted from time of entry to time of departure and must show proof of identification in the form of a state or federal photo identification card. All visitors must be signed in on an AF Form 1109, **Visitor Log**. Personnel making deliveries or performing repair work must present their invoice, delivery slip, work order or other pertinent documents prior to entry.

6.2.8.5. Qualification and authority for a Sensitive Compartmented Information Facility (SCIF) is governed under DOD Directive 5105.21-M-1, The Security, Use and Dissemination of Sensitive Compartmented Information Facility, and AFM 14-304, The Security, Use and Dissemination of Sensitive Compartmented Information Facility and/or higher headquarters. Refer to that publication or its successor and local agreements governing entry into SCIFs. This publication is classified and may be obtained from the office of primary responsibility.

6.2.8.6. If entry into the controlled area is controlled by cipher combination lock, issue the combination key only to those personnel authorized by the owner/user commander.

6.2.8.7. Change cipher combinations for controlled areas semiannually. At a minimum, change the combination when someone with authorized access departs the installation.

6.2.9. Free zones for protection level 4 resources (controlled areas).

6.2.9.1. Free zones are established within controlled areas when construction projects and similar activities make it inappropriate or impractical to apply normal circulation controls. In such cases, establish a free zone corridor from some point on the controlled area boundary to work the project to aid in moving personnel and equipment.

6.2.9.2. As a minimum, commanders responsible for the area will establish free zone procedures, to include who performs entry control duties and how entry is controlled. Ensure you coordinate the establishment of free zones with security forces and other necessary work centers. Follow these guidelines:

- 6.2.9.2.1. Consider moving sensitive resources from the free zone area.
- 6.2.9.2.2. Allow entry to the project work area at some point on the boundary of the controlled area with a free zone corridor.
- 6.2.9.2.3. Ensure that the responsible activity maintains surveillance over the boundary of the free zone.
- 6.2.9.2.4. Close the free zone and secure the controlled area after normal work hours.
- 6.2.9.2.5. The organization or agency most associated with the project will maintain surveillance over the free zone boundary as determined by the commander responsible for the controlled area. **NOTE:** Security forces will not be used as escorts to control entry/exit to the free zone area.
- 6.2.9.2.6. If the temporary free zone inside a CA requires contractors to complete work around sensitive equipment or materials, owner/user personnel will be present any time contractors are in the area or will have the sensitive equipment or materials removed from the area.
- 6.2.9.2.7. If a contractor is doing the work, send the contractor a letter describing the procedures for using free zones during the project. The installation commander or designee must sign the letter. Ensure the letter explains that contract work may be delayed or terminated for short periods due to real-world security responses and military training exercises.

Chapter 7

ALARMED FACILITIES

7.1. This chapter establishes which alarm systems will be installed in facilities as directed in AF and DoD directives and instructions.

7.2. Unit commanders will ensure all appropriate alarmed facilities are established as a controlled area in accordance with **Chapter 6** of this instruction and AFI 31-101.

7.3. The commander of the owning agency must submit an alarmed facilities access authorization list to SFOR, reflecting all personnel who are authorized to activate/deactivate the alarm and authorized to receipt for alarm access codes. This letter will be updated every 6 months or immediately upon compromise or reassignment of personnel.

7.3.1. A DD Form 577, **Signature Card**, must be completed and on file at 6 SFS/SFOR for all personnel authorized to receipt for the alarmed access codes.

7.3.2. 6 SFS/SFOR will review all alarmed facilities access authorization lists for accuracy and check the authorizing signature against the DD Form 577.

7.4. Activating/deactivating alarms.

7.4.1. Facilities NOT equipped with a “card reader”: Prior to activating or deactivating an alarm of a facility not equipped with a “card reader”, the alarm custodian must contact the SFCC controller and properly authenticate, utilizing the Authentication Code. An alarm at the SFCC without proper authentication will result in security forces response.

7.4.1.1. Personnel requesting access to the alarmed facility will contact the SFCC, who will verify the individual's name on the alarmed facilities access authorization list, and respond with a letter or number as applicable.

7.4.1.2. The alarm custodian must respond with the corresponding letter or number, as applicable. Improper authentication will result in security forces response.

7.4.1.3. 6 SFS/SFOR Form 1, **Log of Opening/Closing of Alarmed Facilities**, will be utilized to record opening and closing of MARCENT, NAVCENT and the Armed Forces bank. All other alarmed facilities will be recorded by ADVANTOR and printed out monthly.

7.4.1.4. If there are any discrepancies (e.g., in access mode when it should be secure mode), the custodian will immediately contact the SFCC.

7.4.1.5. If all appears to be in order, the custodian will access/secure the alarm in accordance with system procedures/instructions.

7.4.1.6. All opening and closing of these facilities will be recorded by the alarm system computer.

7.5. Testing Alarms. Each month a complete check of all alarm systems must be performed. Prior to conducting an alarm check, the custodian must contact the SFCC and request to test the alarm system. After proper authentication, the custodian will begin testing the alarm system. Two owner/user personnel

are required to conduct an alarm test. One individual must be on the telephone with the SFCC controller as other individual will conduct the check.

7.5.1. The custodian will document the IDS check, AF Form 2530, **Alarm System Test Record**. Monitors of alarmed facilities will maintain a checklist listing the number of intrusion detection system (IDS) components that are installed and checked in the facility. The custodian will check off each item on the checklist as the component is checked. The custodian will maintain the completed list for 30 days or until superseded by the next alarm system check.

7.5.2. If there are any discrepancies, the custodian will submit a work order.

7.5.2.1. Lighting around alarmed facilities will be of sufficient intensity to afford recognition of illegal acts, such as breaking and entering. Light switches for exterior lights must be inaccessible to unauthorized individuals.

Chapter 8

PROTECTION OF ARMS AMMUNITION AND EXPLOSIVES (AA & E)

8.1. This chapter explains what facilities may store arms, ammunition, or explosives (AA&E) with specific approval of the 6 AMW/CC. All facilities that store AA&E will be designated as controlled areas. All AA&E facilities will comply with AFI 31-101.

8.2. Requests for approval of AA&E storage will be forwarded to 6 AMW/CC through the CSF and will include written recommendations from the CSF based on inspection of the facility and other security considerations. A copy of the request will be maintained by 6 SFS/SFOR.

8.3. The following facilities are designated as controlled areas and are authorized to store AA&E as indicated:

8.3.1. AA&E Storage Facilities are defined as facilities used for housing, on a routine basis, any number of Category I, II, or III AA&E items or more than 30 category IV items. There is no need to designate a facility that does not store Category I, II, or III items, or fewer than 30 category IV items as an AA&E facility or controlled area unless designated by the installation commander. The list of facilities authorized to store AA&E is a limited distribution item and is on file with SFO, SFOR, SFOX, SFOL.

8.3.2. Unit commanders will ensure all facilities used to store AA&E are established as a controlled area in accordance with **Chapter 6** of this Instruction and AFI 31-101.

8.3.3. The commander for all facilities that store AA&E must ensure:

8.3.3.1. A list that reflects the type, model number, manufacturer, and serial number of all firearms, is maintained separately from the weapons for which the commander is responsible.

8.3.3.2. Numbered seals are used to show signs of tampering and aid in inventories.

8.3.3.3. The AF Form 629, **Small Arms Hand Receipt**, is used as the primary verification of an individual's weapon qualification.

8.3.3.3.1. If the AF Form 1297, **Temporary Issue Receipt**, is used, it will show type of firearm, caliber, manufacturer, serial number, printed name, and signature of the person to whom the weapon is issued.

8.3.3.3.2. If a computer-generated product is used for weapons issued in bulk, ensure it reflects all information required by AFI 31-101.

8.3.3.4. Key control for facilities that store AA&E:

8.3.3.4.1. Metal boxes used to store facility keys will be fastened to the building to prevent easy removal. The box will be secured with a GSA approved three-position combination lock or equivalent.

8.3.3.4.2. When a facility is opened, padlocks will be locked to the staple or hasp to prevent theft, loss, or substitution.

8.3.3.4.3. Keys to facilities will be maintained separately from other keys and will be accessible only to authorized individuals.

8.3.3.4.4. A current roster of personnel who can sign for keys will be maintained and will be kept from public view. A properly authenticated alarm facilities access authorization list will fulfill this requirement.

8.3.3.4.5. The use of a master keying system or master keying of combination locks is prohibited.

8.3.3.4.6. Spare keys and high security padlock control keys will be maintained separately from primary keys.

Chapter 9

MUNITIONS ESCORTS

9.1. Upon receiving notification of a munitions escort, the installation entry controller will obtain the class of munitions to be escorted and notify the CCO. All munitions movements onto the installation will be directed to the Port Tampa gate.

9.2. If the munitions escorted are category 1 or 2, the installation entry controller will instruct the driver to pull into the far right lane and stand by for an escort. If the vehicle is a tractor-trailer, the entry controller will place traffic cones behind the vehicle and redirect all traffic through the left inbound lane. The CCO will make notifications in accordance with munitions escorts checklist.

9.3. Duty Hours: The CCO will dispatch at least one patrol to conduct the escort. When the patrol arrives on-scene, escort the munitions to the hardstand (29.2/AP.9) for inspection. Use the primary munitions escort route identified in FOI 31-1. From Dale Mabry gate to North Boundary right onto the airfield access road. Stop the vehicle where "Suspect Vehicle Holding Area" is painted in red on the pavement. The CCO will notify personnel from Traffic Management Office (TMO) who will respond and inspect the shipment. Initialize munitions escorts checklist.

9.4. Non-duty Hours: The patrols will escort the munitions to the hardstand (29.2/AP.9). The escorted vehicle will remain at the hardstand area until the next duty day. On the next duty day, TMO personnel will respond and inspect the shipment. The driver of the shipment will be advised that he/she will be responsible for providing security for the shipment until TMO personnel have inspected the shipment.

9.5. If the munitions are category 3, the installation entry controller will direct the driver of the most direct route to the shipments destination during duty hours. During non-duty hours, the installation entry controller will instruct the driver to return during duty hours.

9.6. Concept of Operations. Persons issued or in the possession of AA&E are responsible for protecting these items while entrusted to their care. Unless directed otherwise by this Instruction or by the 6 AMW/CC, all drivers and escorts will be provided by the owner/user.

9.6.1. The categories of AA&E used in this Instruction are defined in DoD 5100.76M.

9.6.2. All AA&E will be transported in an enclosed, locked government vehicle, CONEX, or similar container, as applicable. AA&E will not be transported in privately owned vehicles (POV).

9.6.3. Escort requirements for on/off AA&E movements:

9.6.3.1. Category I Weapons and Munitions. Moved under the protection of armed guard surveillance (AGS) (refer to paragraph **9.6.1.** for definition) and security escort vehicle service (SV) (refer to paragraph **9.6.2.** for definition). During the movement, these items will be in the custody of a commissioned officer, enlisted person grade E-6 or above, or an Air Force civilian of equivalent grade or higher. If military, the custodian may be one of the assigned drivers. Civilians WILL NOT be armed. Unless directed otherwise, all drivers and escorts will be provided by the owner/user.

9.6.3.2. Category II Weapons and Munitions:

9.6.3.2.1. Sixteen or more Category II weapons will be moved under the protection of AGS (refer to paragraph 9.6.1. for definition).

9.6.3.2.2. Fifteen or less Category II will be moved under the protection of constant surveillance service (CSS) (refer to paragraph 9.6.3. for definition).

9.6.3.3. Category III and IV Weapons and Munitions:

9.6.3.3.1. Sixteen or more Category III or IV weapons will be moved under the protection of dual driver protective system (DDPS) (refer to paragraph 9.6.4. for definition).

9.6.3.3.2. Fifteen or less Category III or IV weapons and all Category III and IV munitions will be moved under the protection of constant surveillance service (CSS) (refer to paragraph 9.6.3. for definition).

9.6.3.4. The 6 AMW/CC or 6 SPTG/CC will approve the arming of USAF personnel to perform duties off base.

9.6.3.5. After determining the escort requirement (in accordance with paragraph 9.4.2.), the owner/user will contact the SFCC and give them information indicated below.

9.6.3.5.1. Name of escort and driver.

9.6.3.5.2. Description of AA&E being moved (risk category and number).

9.6.3.5.3. Starting and terminating location of movement.

9.6.3.5.4. Route of travel.

9.6.3.5.5. Time of departure.

9.6.3.5.6. Estimated time of arrival.

9.6.3.5.7. Mode of transport. Include vehicle description, make, model, color, and registration number.

9.6.4. If the movement is off base, the owner/user must also coordinate with applicable civilian agencies (e.g., law enforcement, county sheriff) prior to the movement being initiated. If possible, a courier service can be used to fulfill the escort requirements.

9.6.5. The SFCC controller will record all the required information in the security forces blotter and monitor the movement. If the movement is not terminated within the allotted time (estimated time of arrival) or there is a robbery or attempted robbery, the SFCC controller will initiate anti-robbery procedures.

9.6.6. The escort and all drivers will proceed directly to the designated termination location and, as soon as they arrive, notify the SFCC of termination.

9.6.6.1. If the movement is delayed, the SFCC will be contacted and given the new estimated time of arrival and reason for the delay.

9.6.6.2. If there is a robbery or robbery attempt, the owner/user will implement anti-robbery procedures in accordance with **Attachment 2** of this instruction, attempt to get the best description as possible of all the suspect(s), and contact the SFCC as soon as it is safe to do so.

9.7. Definitions:

9.7.1. Armed Guard Surveillance (AGS). Constant surveillance by two qualified drivers, one of which must be armed. Both individuals must be awake and within 10 feet of the AA&E items at all times. Military custodians may be armed and assigned as the driver. Civilians will not be armed, but may be drivers. The drivers must be capable of contacting law enforcement or other emergency agencies for assistance.

9.7.2. Security Escort Vehicle Service (SEVS). A separate trail vehicle to maintain discreet surveillance of the vehicle transporting the AA&E and provide emergency assistance by contacting appropriate law enforcement agencies when needed. Trail vehicles will be capable of maintaining two-way communications with the cargo vehicle and of contacting law enforcement or other emergency agencies for assistance.

9.7.3. Constant Surveillance Service (CSS). Constant and specific surveillance (within 10 feet and in unobstructed view) by one individual. The individual must have the capability of contacting law enforcement or other emergency agencies for assistance.

9.7.4. Dual Driver Protective Service (DDPS). Continuous responsibility, attendance, and surveillance (within 10 feet and in unobstructed view) by two qualified drivers. The driver will be capable of contacting law enforcement or other emergency agencies for assistance.

9.8. Tasks.

9.8.1. Owner/User:

9.8.1.1. Ensure all AA&E movements are completed in accordance with this instruction.

9.8.1.2. Coordinate all off-base AA&E movements with civilian authorities.

9.8.1.3. Unless directed otherwise by this Instruction or the 6 AMW/CC, provide all drivers and escorts for AA&E movements.

9.8.1.4. Implement additional procedures as directed.

9.8.2. Security Forces Control Center (SFCC) Controller:

9.8.2.1. Record the required information in the blotter, monitor all movements, and initiate anti-robbery procedures in accordance with FOI 31-1 chapter 9.

9.8.2.2. Ensure all AA&E movements are conducted in accordance with this Instruction.

9.8.2.3. Implement additional procedures as directed.

9.8.3. All Escorts/Drivers:

9.8.3.1. Conduct AA&E movements in accordance with this Instruction. If separate vehicles are used, follow the AA&E vehicle as close as possible.

9.8.3.2. Proceed directly to the termination point and notify the SFCC of any delays or problems.

9.8.3.3. Maintain the ability to contact the 6 SFS/SFCC and/or local civilian authorities (e.g., radio, telephone).

9.8.3.4. In the event of an attempted or actual robbery, immediately notify the 6 SFS/SFCC and implement anti-robbery procedures in accordance with **Attachment 2** of this instruction. If the movement is off base, also notify the civil authorities immediately.

9.8.3.5. At no time display any weapon to the public view except under extreme emergency or robbery situations.

9.8.3.6. Implement additional procedures as directed.

9.9. Coordinate instructions: All units/agencies will support this instruction when implemented.

Chapter 10

PROTECTION OF FUNDS

10.1. This chapter discusses protection of funds.

10.2. Classified Material. Do not store classified with funds or high cash value items.

10.3. Controlled Area Designation for Funds Facilities. All Air Force accounting and finance offices and funds facilities handling or storing \$100,000 or more will be designated as controlled areas. The decision to designate other funds facilities as controlled areas rests with the ISC, but is discouraged.

10.4. Funds Storage. Personnel must obtain written approval from the 6 AMW/CC and CSF for funds storage authority, limitations, and locations. Unit/staff agencies will not store/handle funds at a facility without approval of the CSF and 6 AMW/CC.

10.4.1. All funds custodians must complete a Funds Operating and Storage Limitation Authorization Letter and send it to 6 SFS/SFOR. 6 SFS/SFOR will conduct an inspection of the facility and forward the letter, with their recommendations to the CSF for review.

10.4.1.1. If approved by the CSF, the letter will be sent to the 6 AMW/CC for final approval.

10.4.1.2. If disapproved by the CSF, the letter will be sent back to 6 SFS/SFOR who will inform the requesting agency as to the reason(s) the request was disapproved.

10.4.2. Facilities handling/storing less than \$50,000 will meet the following protection criteria:

10.4.2.1. Doors and doorframes leading into a funds storage room will be solid wood core or metal doors with the hinges mounted on the interior of the room.

10.4.2.2. Doors will be equipped with, as a minimum, locks and hasps meeting MIL-P-17802 standards, or key actuated deadbolt with at least a 1-inch throw. Hinges that are exposed will have fixed pins or spot welding, or otherwise protected to prevent removal.

10.4.2.3. Walls will be a minimum 8 feet high and above the existing ceiling.

10.4.3. Funds Storage Limits/Requirements:

10.4.3.1. Funds less than \$100 will be secured in a metal cash box, inside a lockable desk drawer.

10.4.3.2. Funds in excess of \$100 but less than \$1,000 will be secured in:

10.4.3.2.1. A metal box which is constructed of 9-gauge steel (hasps and hinges of the container must afford the same degree of protection as the container). The container must be secured with a GSA approved, three-position, changeable combination lock.

10.4.3.2.2. A GSA approved container constructed of heavy metal and has a three-position, built-in, changeable combination lock.

10.4.3.2.3. A GSA field safe.

10.4.3.2.4. A GSA approved filing cabinet secured by a lock bar and a GSA approved, three-position combination lock.

10.4.3.3. Funds in excess of \$1,000 but less than \$7,500 will be secured in a GSA approved container constructed of metal and have a three-position, built-in, changeable combination lock. The container will be stored inside a locked room.

10.4.3.4. Funds in excess of \$7,500 but less than \$25,000 will be secured in:

10.4.3.4.1. A GSA approved security container meeting class 1 or higher specifications. Intrusion Detection System (IDS) is recommended.

10.4.3.4.2. An approved funds storage room meeting the requirements identified in paragraph **10.4.** of the basic instruction. IDS is recommended.

10.4.3.5. Funds in excess of \$25,000 but less than \$50,000 will be secured in one of the manners identified in paragraph **10.4.** above. However, IDS is required.

10.4.3.6. Funds in excess of \$100,000 will be secured as indicated in AFI 31-101.

10.5. Funds Storage Containers. Funds custodians must ensure containers used to store government funds are certified for their capability to protect funds. These containers must be GSA approved for funds storage. If the container does not meet GSA specifications, ensure it has an underwriter's laboratory (UL) label (or foreign equivalent) designating it as a burglar-resistant safe.

10.5.1. If assistance is required in certifying new funds containers, contact the 6 SFS Resource Protection Manager (828-2373). Facilities with funds containers must post and annotate an SF Form 700, **Security Container Information** (inside container), SF Form 701, **Activity Security Checklist, SF Form 702, Security Container Check Sheet**, and AFTO Form 36, **Maintenance Record**.

10.5.2. Funds Storage Container Requirements:

10.5.2.1. All funds storage containers will be certified by the 6 SFS/SFOR.

10.5.2.2. The combination to all security containers will be changed on a semiannual basis or upon the relief, transfer, discharge, or separation of anyone who knows it or when it is compromised.

10.5.2.3. The combination to security containers will not be stored outside of the unit.

10.5.2.4. All openings and closings of containers will be recorded on the SF 702 or applicable AAFES form which will be attached to the container.

10.5.2.5. All containers will have an SF 700 posted on the inside. This form will be complete and accurate at all times.

10.5.3. Unit commanders will designate, in writing, a Funds Custodian for each funds storage facility (the controlled area monitor may fulfill this position.). The appointment letters will identify the individual, duty phone, and areas of responsibility. The original letter will be filed at the facility and a copy will be forwarded to 6 SFS/ SFOR. A new letter will be accomplished each time the custodian is replaced.

10.5.4. Unit commanders must ensure personnel assigned to work in funds storage facilities are properly trained and aware of their responsibilities for protection of resources. Training for these personnel will consist of, as a minimum, reading the facility's operating instruction initially and follow up training. This training will be documented and maintained by the funds custodian.

10.5.5. Unit commanders are responsible for ensuring written instructions are completed which outline specific responsibilities and protection procedures under both normal and emergency conditions. These procedures will be coordinated through 6 SFS/SFOR and posted within the storage area. These procedures will include the following:

10.5.5.1. Secure/closing procedures.

10.5.5.2. Alarm system operations (if applicable).

10.5.5.3. Procedures for operating and safeguarding the area.

10.5.5.4. Key control.

10.5.5.5. Anti-robbery/emergency procedures.

10.5.5.6. Entry control procedures.

10.5.5.7. Security of cash registers. Cash register drawers are closed/locked when unattended. Funds will be removed from cash registers and drawers are left open during non-operational hours.

10.5.5.8. Cashier responsibilities.

10.5.6. 6 SFS/SFOR will maintain a folder on each funds storage area that will contain, as a minimum, the following:

10.5.6.1. Letters of designation and appointment (funds custodian, controlled area monitor, EALs, etc.).

10.5.6.2. Storage limitation letters.

10.5.6.3. Current resource protection and anti-robbery exercise reports and replies of corrective action.

10.5.6.4. Copies of deviations/waivers.

10.5.6.5. Local operating instructions.

10.5.6.6. Resource protection checklist.

10.5.6.7. Copy of current AFI 31-101 and all supplements.

10.5.6.8. Copy of this Instruction.

10.6. Operating Instructions. Publish a local operating instruction, outlining procedures for the following, as a minimum:

10.6.1. Use of AF Form 439, **Robbery Checklist**, and actions to take in the event of a robbery.

10.6.1.1. Steps to reduce cash on hand.

10.6.1.2. Control of alarm systems key boxes if applicable.

10.6.1.3. Training procedures.

10.6.1.4. Bomb threat procedures.

10.6.1.5. Funds escort procedures.

10.6.1.6. Controlled area entry and escort procedures.

10.6.1.7. Emergency entry and egress procedures.

10.7. Deviations. Prepare and coordinate all deviations to protection standards using AF Form 116, **Request for Deviation From Security Criteria.**

10.8. Use of IDE. An effective IDE is a prime deterrent in preventing the loss of funds by theft. The following funds activities must be protected by IDE.

10.8.1. Accounting and Finance Offices.

10.8.2. Facilities Storing \$100,000 or more.

10.8.3. Facilities storing \$100,000 or more will comply with AFI 31-101, Chapter 25.

10.8.4. Duress Alarms. In addition to IDE protection for unattended storage of funds, accounting and finance cashier cages will be equipped with a duress alarm.

Chapter 11

FUNDS ESCORTS

11.1. This chapter applies to all security forces, security forces augmentees, individual mobilization augmentees, reservists, and air national guardsmen required to perform escorts at MacDill Air Force Base.

11.2. Funds Escorts

11.2.1. Vehicle Escort: Upon notification of a vehicle escort, the CCO will obtain the escort information and dispatch a patrol, using the spot code card, to conduct the escort.

11.2.2. The patrol will contact the escortee and verify all pertinent information (i.e., personal data, vehicle information, and route of travel) and brief the CCO, via telephone, prior to departing the facility.

11.2.3. The patrol will trail the escort vehicle with their vehicle, and will continually have the escort vehicle in their view.

11.2.3.1. If an emergency occurs along the route of travel, the escort will not leave the funds vehicle. The patrol will radio the CCO and have another patrol respond.

11.2.3.2. If the funds vehicle is involved in an accident and can be moved, finish the escort. If the escort vehicle cannot be moved, place the escort and funds in the patrol vehicle and finish the escort.

11.2.4. When the escort vehicle arrives at its destination, the patrol will exit their vehicle and physically escort the individual and funds safely to the appropriate agency.

11.2.5. The patrol will terminate the escort by notifying the CCO and authenticate their status using the 6 SFS authentication card.

11.2.6. Foot Escort: Upon notification of a foot escort, the CCO will obtain the escort information and dispatch a patrol.

11.2.7. The patrol will contact the escortee and verify all pertinent information (i.e., personal data and route of travel) and brief the CCO via telephone, prior to departing the facility.

11.2.8. The patrol will notify the CCO prior to departing the facility and authenticate their status. The patrol will either walk along side of or behind the funds and at no time will the patrol handle the funds.

11.2.9. When the patrol arrives at the final destination and the funds have been safely delivered to the appropriate agency, the patrol will terminate the escort and authenticate their status using the 6 SFS authentication matrix.

11.2.10. The CCO annotates all escorts on the AF Form 3136, **General Purpose Form**.

Chapter 12

VEHICLE AND VISITOR INSTALLATION ENTRY AND RELATED TASKS

12.1. This chapter establishes entry requirements for MacDill AFB and provides procedures for various situations, which could occur at an installation entry gate. References for this chapter include AFI 31-101, *The Air Force Installation Security Program*, and AFI 31-204, *Air Force Motor Vehicle Traffic Supervision*.

12.2. Vehicle and Pedestrian Entry Requirements.

12.2.1. During Force Protection Condition Normal, immediate entry will be granted to vehicles and pedestrians possessing the following: **(CHANGES IN FPCONS MAY REQUIRE MODIFICATION OF ENTRY REQUIREMENTS THAT ARE APPROVED VIA POLICY LETTER).**

12.2.1.1. DD Form 2: **Military ID Card** for active duty, retired, reservist, Dept of Health and Human Services and NOAA Corps.

12.2.1.2. DD Form 1173: **Dependent ID Card** (also issued to active duty OSI agents).

12.2.1.3. DD Form 1173-1: **Reserve Dependent ID Card**.

12.2.1.4. AF Form 354: **Civilian Employee ID Card** (also issued to civilian OSI agents).

12.2.1.5. DD Form 2574: **AAFES Employee ID Card**.

12.2.1.6. Optional Form 55: **Commissary Employee ID Card**.

12.2.1.7. DLA Form 1486: **Defense Contract Management Agency**.

12.2.1.8. **Civil Air Patrol Card** .

12.2.1.9. CDA Form 1602: **US Army Civilian ID Card**.

12.2.1.10. AF Form 75: **Visitor's Pass** with current date.

12.2.1.11. SFS Form 75: **Visitor Pass** issued to visitors and contractors on station for over 30 days.

12.2.1.12. College access badges and term entry passes issued by the VRF.

12.2.1.13. Protocol passes: issued by protocol.

12.2.1.14. Department of Commerce identification.

12.2.1.15. AFOSI credentials.

12.2.1.16. Individuals in possession of an agent letter issued by 6 SVS with a valid drivers license and the ID card of the sponsor.

12.2.1.17. State and federal police agencies with credentials and are on official business. On-duty civilian police armed with a duty weapon will be allowed to attend college classes when in possession of the AF Form 75. No pass is required when law enforcement personnel are en route to the firing range.

12.2.1.18. Personnel listed on an authenticated special function listing at the gate. Lists are properly authenticated by the VRF, flight chief, or higher 6 SFS authority.

12.2.1.19. Active duty foreign military on orders to MacDill AFB, USCENTCOM Coalition ID card and who have been sponsored on by 6 AMW, USSOCOM, or USCENTCOM.

12.2.1.20. Canadian military ID card holders (active duty and retired).

12.2.1.21. All personnel listed on the base driving revocation listing are prohibited from operating a motor vehicle on the installation. Personnel wishing to gain access onto the installation who are listed on the barment listing will not be allowed access. Title 18, Section 1382 of the US Code authorizes the installation commander to order persons off the installation, and order them not to re-enter. Personnel in possession of a valid letter authorizing them use of services on base will be allowed to proceed upon verifying the individual with a picture identification credential. Any attempt to violate the barment order will be reported via AF Form 3545, **Incident Report**.

12.2.2. Vehicle Entry Requirements. All personnel wishing to drive a vehicle onto the installation must have one of the forms of ID stated in para 12.2.1., a valid state drivers license, current proof of insurance, and current vehicle registration. Individuals must also wear seatbelts. All children under the age of 4 not exceeding 50 pounds in weight must be placed in a child restraint seat. If seatbelts are inoperative or child restraint seats are not used, deny the vehicle entry and issue a citation. Installation ECs will advise vehicle operators with RADAR detectors that they are not authorized to use them on military installations. Entry will be granted to all vehicles:

12.2.2.1. Vehicles displaying a current and properly affixed DD Form 2220, **DOD Registered Vehicle**, from any military installation.

12.2.2.1.1. Red - enlisted personnel.

12.2.2.1.2. Gold - noncommissioned officer.

12.2.2.1.3. Blue - commissioned officer.

12.2.2.1.4. Green - civilian employee.

12.2.2.1.5. White - contractor

12.2.2.2. All US government vehicles.

12.2.2.3. Pre-announced civilian emergency vehicles will be escorted by 6 SFS patrols.

12.2.2.4. Vehicles identified as commercial will be instructed to use Port Tampa gate. Commercial and local delivery vehicles displaying company logos permanently affixed to the vehicle that are recognizable (i.e., Coke, Frito Lay) must have bill of lading, invoice, or work order stating their destination with verification of EAL.

12.2.2.5. Vehicle and operators must be in possession of a valid AF Form 75 for the vehicle they are driving. **NOTE:** The pass serves as both a vehicle and visitor pass and both must be checked and matched before allowing entry. Every vehicle occupant must possess a picture ID and all contractors must a valid AF Form 75 or be on an authentication EAL. These individuals should be driving the vehicle listed on the pass. However, there may be instances where they are not. In these cases, ECs will direct the individual to the VRF if open. When the VRF is closed, verify the vehicle's registration and insurance are current and issue an AF Form 75 valid until 0700 of the next duty day. If the vehicle's registration and/or insurance are not current, the vehicle can not come on the installation however, the individual can.

12.2.2.6. Contracted armored vehicles with valid company ID.

12.2.2.7. Rental vehicles being used for official business by military or DoD personnel. Vehicle must be registered via AF Form 75 for the length of the contract period. Check the driver's installation entry credentials and rental agreement, and if all is in order, allow them to proceed in the same manner as a marked government vehicle.

12.2.2.8. Civil/federal police on official business upon presentation of police credentials.

12.2.3. The following individuals are authorized to sponsor guests on base.

12.2.3.1. Active duty military.

12.2.3.2. Reserve members.

12.2.3.3. Retired military.

12.2.3.4. Dependents who are 18 years or older.

12.2.3.5. DoD civilian employees who are 18 years or older and in the grade of GS-5, WG-5 or equivalent and higher.

12.2.3.5.1. For FPCON Charlie or Delta, personnel deemed as "mission essential" only may sponsor guests on base.

12.2.3.6. Contractor supervisors may vouch temporary hire personnel onto the installation. The contractor supervisor must have "supervisor" annotated on the AF Form 75. During duty hours, contract supervisors need to process their day workers through the VRF.

12.2.3.7. Individuals must be present at the installation ECP or VRF in order to sponsor a guest on base.

12.2.4. The following are other instances when vehicles/visitors are authorized on base.

12.2.4.1. Commercial busses. ECs will physically board all commercial buses and check all passengers requesting access onto the installation for one of the authorized credentials. If there are personnel on the bus that do not possess the proper credentials, inform the passenger they must depart the bus and wait until the bus has completed its run on base. Once the bus departs the installation, the passenger can re-enter the bus. Handicapped individuals will be allowed to remain on the bus.

12.2.4.2. Taxis entering the installation to drop off passengers. The passenger must have one of the authorized credentials in order to proceed.

12.2.4.2.1. Taxis entering the installation to pick-up a passenger: The EC will check dispatch documentation and allow them to proceed. If the taxi has no documentation, direct them to the VRF. When the VRF is closed the EC will contact the sponsor prior to allowing entry.

12.2.5. News media personnel.

12.2.5.1. The installation entry controller will:

12.2.5.2. Direct them to the VRF, pending the arrival of public affairs, who will assume duties as escort officials.

12.2.5.3. Notify the CCO anytime news media personnel arrive at the gates.

12.2.5.4. If asked questions by news media personnel about installation events inform them you are not authorized to release any information and instruct them to contact the public affairs office/ representative.

12.2.5.5. CCO will contact public affairs and brief them on the news media.

12.2.6. Tow Trucks.

12.2.6.1. Direct tow trucks to the VRF. When the VRF is closed, the Dale Mabry EC will verify sponsorship for the tow truck via CCO and allow them to proceed. The CCO will notify the EC when the sponsor is an on-duty security forces.

12.3. Visitor Control.

12.3.1. During the hours of operation, all vehicles and personnel not having proper credentials will be directed to the VRF. VRF personnel will ensure the visitor has valid credentials and issue an AF Form 75.

12.3.2. When the VRF is closed, the Dale Mabry EC will be responsible for processing visitors. For all visitors wishing to gain access onto the installation, the sponsor must be present at the Dale Mabry gate. Base sponsors of visitors must be in a position to assume responsibility of the visitor for the duration of the visit. **Ensure the visitor has valid credentials.** After all measures have been completed, log all of the visitor's information on the visitor log and issue them an AF Form 75. Visitors may only be sponsored in at the Dale Mabry gate. If an individual wishing to gain access onto the installation approaches Bayshore or MacDill gate, direct them to Dale Mabry gate via an off base route.

12.3.3. The gate will not accept preannounced visitor phone calls. However, in person sponsorship is authorized at Dale Mabry gate.

12.3.4. ECs will direct personnel wishing to authenticate special functions lists and visitation letters to the VRF. During non-duty hours, ECs will direct the sponsor to the SFCC.

12.3.5. All minors (under the age of 16 years) wishing to gain access onto the installation after curfew hours must be accompanied by his/her military sponsor, parent, guardian or other person age 18 or older with the approval of the minor's parent or guardian. Curfew hours are Sunday - Thursday, from 2200-0500 hours and Friday - Saturday, from 2400 - 0500 hours. If the minor is on an emergency errand, or returning home from an off base activity, school, employment, religious, entertainment or recreational activity, or any other lawful assembly that began prior to curfew hours, the minor will be allowed to proceed. All curfew violators will be detained and transported to their residence. Curfew violators will not be released on their own recognizance and can only be released to a sponsor, parent or legal guardian. An AF Form 3545 will be accomplished for all curfew violators.

12.3.6. Identification checks. One hundred percent identification check of vehicle operators will be conducted by all installation ECs. **NOTE:** "ID Check in Progress" will be placed in the sign holder affixed to the gate retaining wall. The purpose of the check is to ensure only authorized personnel identified in paragraph 13.2.1. of this instruction are allowed entry to the installation. All entry controllers will report any incidents in which a vehicle operator is unable to effectively operate a motor vehicle.

12.4. Safe Haven Procedures.

12.4.1. If a vehicle approaches the Dale Mabry installation entry control point and the operator relates he/she is requesting a non-nuclear safe haven; the EC will implement safe haven checklist.

12.5. Classified Shipments.

12.5.1. When notified of a classified material shipment, the EC will have the courier display a copy of their Armed Forces Courier Service (ARFCOS). The ARFCOS lists personnel authorized to conduct ARFCOS shipments. The EC will verify the names, social security numbers, and signatures with the courier's identification credentials. All personnel requesting to store overnight classified material will be directed to the 6 AMW Wing Operations Center.

12.6. Munitions Shipments.

12.6.1. All ECs will direct category 1, 2 or 3 munitions to Port Tampa gate. Once the driver approaches the entry control point and advises the EC of a category 1 or 2 movement, the EC will implement munitions escort checklist.

12.7. Newly Assigned Personnel.

12.7.1. When newly assigned personnel approach the EC for assistance, the EC will direct them to Building 373, 6th Mission Support Squadron (6 MSS), during duty hours. During non-duty hours, direct them to Building 411, Lodging, and inform them lodging has a listing of all sponsors.

12.8. Foreign National Defector.

12.8.1. If an individual from a foreign country approaches the installation entry control point, and states they want to defect to the US, the EC will immediately have the individual enter the gate and contact the SFCC to initiate the foreign national defector checklist.

12.9. Demonstrations.

12.9.1. Entry controller will report the demonstration to the CCO. If demonstrators are not interfering with normal operations, continue to process traffic. If demonstrators become violent or interfere with normal operations, notify the CCO of the situation and prepare to close the gate when directed to do so. If demonstrators approach the entry control point and make demands, do not make promises or give the demonstrators misleading ideas. Contact the CCO immediately.

12.10. College Access Badges and Term Entry Passes.

12.10.1. All personnel without military affiliation attending classes on MacDill AFB must be issued college access badges as well as term entry passes. These devices will be used to gain access to the installation for the purpose of attending college classes during the time periods requested. Non-DoD affiliated foreign nationals are not authorized access to the installation for purposes of college classes. Permanent resident aliens, meaning those in possession of applicable INS documentation, will be allowed.

12.10.2. The program coordinator from each college will identify in writing via DD Form 577, **Signature Card** (see [Attachment 4](#)), individuals (not to exceed 4) to be authorized to request college access badges and term entry passes. The DD Form 577 must be signed by the Chief, Education Ser-

vices Flight, 6 MSS, and will remain on file at the 6 SFS Visitor Reception Facility (VRF) for a maximum of one year. Upon expiration or departure of one of the designated requestors, a new DD Form 577 must be accomplished. It is the responsibility of the program coordinator to inform the VRF of any changes and/or updates to the DD Forms 577.

12.10.3. The designated school requestors are responsible for obtaining pertinent information and completing all requests for college access badges (**Attachment 4**) and term entry passes (**Attachment 5**). A DD Form 577- authorized requestor must sign all requests. Failure to provide needed information will result in college badge not being issued. The following information **MUST** be provided on the application:

- 12.10.3.1. Name (last, first, MI).
- 12.10.3.2. Date of birth.
- 12.10.3.3. Social Security Number.
- 12.10.3.4. Expiration date of badge (not to exceed one year)/pass (not to exceed 100 days).
- 12.10.3.5. Days authorized (Mon, Tue, Wed, etc.) on term entry pass.
- 12.10.3.6. Times authorized (1800-2100, etc.) on term entry pass.

12.10.4. Students/faculty requesting college access badges and term entry passes **MUST** hand-carry original application to the VRF for processing unless other arrangements have been made between the college and the installation. All personnel requesting the college access badge must obtain a background check through the Florida Department of Law Enforcement (FDLE). The local FLDE office is located at 4211 North Lois adjacent to Hillsborough Community College. Required fingerprinting can be accomplished at local law enforcement agencies. Once the package is completed and forwarded per instructions for processing, it should take approximately two weeks for the completed background check to return to the applicant. There is a \$15 non-refundable fee for each check conducted. If the schools would like to contact FDLE, the number is 850-410-8106 for the headquarters in Tallahassee. Students/faculty who have recently undergone a background check must provide some form of proof that shows date, time and name of organization that conducted the background check. Anyone having an outstanding warrant will be apprehended and turned over to the jurisdiction issuing the warrant. In addition to the badge/pass request forms and completed background investigation, the student/teacher must also bring the following credentials:

- 12.10.4.1. Valid stateside drivers license (driving passes).
- 12.10.4.2. Valid state ID (non-driving pass).
- 12.10.4.3. Valid vehicle registration/proof of insurance.
- 12.10.4.4. Proof of class registration.

NOTE: Failure to bring required documentation will only delay processing of the badge/pass.

12.10.5. College access badges/term entry passes are only valid for whom they are issued and are only authorized for commuting to and from class. Transiting other areas outside of those authorized will result in trespassing charges. Students/teachers are not authorized to transport unauthorized passengers (individuals without approved base access) in their vehicles onto the installation for pick-up and drop-off. All personnel and their personal property are subject to search and all federal and Flor-

ida state laws apply while on the installation. Violators will be issued citations and, depending on severity of violation, may be barred from further entry to the installation.

Chapter 13

INSTALLATION PATROL DUTIES

13.1. This chapter applies to all security forces, security forces augmentees, individual mobilization augmentees, reservists, and Air National Guard personnel required performing installation patrol duties at MacDill AFB.

13.2. Responsibilities:

13.2.1. Installation patrols (IP) must be thoroughly familiar with all funds/weapons storage facilities, protection level resources, and buildings listed on the building checklists. IPs must also be knowledgeable of flightline vehicle operations, flightline incident procedures (Helping Hand/Covered Wagon), aircraft security, and provide armed response capability.

13.2.2. IPs will conduct building security checks as directed during non-duty hours, weekends, and holidays or as random antiterrorism measures (RAM).

13.2.3. All doors, windows, and locks must be physically checked by the IP. Immediately report any facility found unsecured to the CCO. For further information, refer to FOI 31-14, *Building/Structure Security Checks*.

13.2.4. IPs can be dispatched to emergency and very sensitive incidents. All IPs will be courteous, tactful, fair but firm in their decisions. Utilize experience and judgment to assist in making decisions during unusual situations. All IPs will represent the Security Forces career field in the utmost professional manner at all times. **NOTE:** Request flight chief assistance on-scene whenever necessary.

13.2.5. Forms required to be accomplished by installation patrolmen: IPs will maintain forms listed in paragraphs **13.2.5.1.** and **13.2.5.12.** in their possession while on patrol.

13.2.5.1. AF Form 3545 – **Incident Report.**

13.2.5.2. DD Form 1408 – **Armed Forces Traffic Ticket.**

13.2.5.3. DD Form 1806 – **Federal Court Violation Notice.**

13.2.5.4. AF Form 1168 – **Statement of Suspect/Witness/Complainant.**

13.2.5.5. AF Form 1361 – **Pick Up/Restriction Order.**

13.2.5.6. AF Form 52 – **Evidence Tag.**

13.2.5.7. AF Form 3322 – **Authority to Apprehend in Private Dwelling.**

13.2.5.8. AF Form 1364 – **Consent to Search and Seize.**

13.2.5.9. AF Form 1176 – **Authority to Search and Seize.**

13.2.5.10. AF Form 1800 – **Government Vehicle Checklist.**

13.2.5.11. SF Form 1668 – **Field Interview Card.**

13.2.5.12. SF Form 840 – **Minor Vehicle Accident Report.**

13.3. Vehicle Requirements.

13.3.1. IPs will inspect their assigned vehicles and document appropriate discrepancies on AF Form 1800. All police equipment discrepancies will be radioed in to the control center and annotated in the blotter. IPs are responsible for maintaining all appropriate fluid levels in their vehicles. IPs will ensure vehicles are refueled and cleaned inside and out, prior to shift change.

13.3.2. All vehicle discrepancies will be reported to the on-coming and off-going flight chief and recorded in the security forces blotter. If a vehicle must be taken to base transportation for repairs, the ending mileage and reason for deadlining the vehicle will be given to the control center operator (CCO) and the vehicle NCO will be notified.

13.3.3. Prior to assuming patrol duties, a systems check of the RADAR unit will be conducted. Discrepancies will be reported to operations support superintendent.

13.4. Installation Patrol Duties.

13.4.1. Respond to incidents or complaints, restoring and maintaining order at the scene, and reporting critical information as needed to the control center operator.

13.4.2. Conduct initial investigations of incidents, complaints and traffic accidents. Provide follow-on assistance to security forces investigators to include taking statements, conducting interviews, accomplishing reports, securing crime scenes, collecting evidence, and accomplishing field interviews.

13.5. Patrol Sectors.

13.5.1. Sector #1: From Dale Mabry gate along N. Boundary Blvd. to Bayshore Blvd. to Florida Keys Ave. along Florida Keys. Hangar Loop Drive to Zemke to Dale Mabry along Taxiway Zulu and hardstands within the flightline. From Florida Keys to Operations Court to Taxiway N to Dale Mabry gate. Sector includes DV Spot 1, Hangars 1 and 2, the WOC and all of the north ramp.

13.5.2. Sector #2: From Florida Keys south along Bayshore Blvd to McClelland Ave, across to Marina Bay Drive/Hangar Loop Drive and Sector 1 bordering Florida Keys. Sector includes Hangars 3, 4, and 5, Transient Ramp from fuel pit 16 to 30 and Bravo ramp and CAL docks.

13.5.3. Sector #3: From McClelland Ave to the base marina, across North Golf Course Ave. This includes Taxiways Kilo and Mike on the airfield.

13.5.4. Sector #4: From North Golf Course Rd to North Boundary Blvd to South Shore Rd. This includes Taxiway Lima and November on the airfield and Building 71.

13.5.5. Remain in designated sectors or areas assigned by the flight chief.

Chapter 14

BASE ENTRY POINT CHECKS

14.1. This chapter applies to all security forces, security forces augmentees, and individual mobilization augmentees, reservists, and Air National Guard personnel performing base entry control point checks at MacDill AFB.

14.2. Responsibilities.

14.2.1. A base entry point check is the examination of a vehicle without the foundation for a search. Installation commanders direct and establish procedures for base entry point checks of randomly selected vehicles entering or leaving the base under their jurisdiction, whether the owner is military or civilian. This authority is delegated to the 6th Support Group Commander.

14.2.2. The 6 SFS has been authorized by the installation commander to conduct random base entry control point checks at installation entry control points in accordance with Title 18 of the United States Code, Section 1382.

14.2.3. A BEPC is an examination, not a search. The examination is not based on probable cause, but is a tool used by the installation commander to protect government property.

14.2.4. When conducting BEPCs, security forces personnel will be acting in the capacity of a sentinel, safeguarding a military installation and protecting government property while preventing theft.

14.2.5. The time, location, and number of vehicles to be inspected will be directed by the 6 SPTG/CC.

14.2.5.1. At no time will security forces personnel deviate from the predesignated times, locations, or vehicle count.

14.2.5.2. The flight chief should consider postponement or discontinuation during the following situations: inclement weather, serious traffic jams, or incidents. A blotter entry must be made explaining the circumstances.

14.3. Procedures.

14.3.1. There will be a minimum of two security forces personnel conducting the checks.

14.3.2. The security forces will stop the predesignated vehicle and have the vehicle operator park the vehicle clear of traffic to the side of the roadway.

14.3.3. The security forces will instruct the vehicle operator to turn off the engine and set the parking brake.

14.3.4. The security forces will advise the vehicle operator of the following:

14.3.5. "I am _____, and I stopped your vehicle because we are conducting random base entry control point checks, authorized by the installation commander. Do I have your permission to inspect your vehicle?"

14.3.6. If the vehicle operator/owner agrees to the inspection, obtain a valid driver's license, vehicle registration, and insurance.

14.3.7. The security forces will annotate this information on the BEPC check sheet. The check sheet will be maintained on the SFCC.

14.3.8. If the operator/owner does not possess the proper credentials, do not let them operate the vehicle on the installation and cite the operator accordingly.

14.3.9. Instruct the operator to open all vehicle doors, trunk, hood, and any other compartments.

14.3.10. The security forces will then initiate a simple and systematic examination of the entire vehicle.

14.3.11. When possible, a military working dog (MWD) will be used to conduct the inspection.

14.3.12. Use of the MWD will not replace the visual inspection conducted by the security forces, but will serve to increase detection capability.

14.3.13. If no contraband is found, thank the operator/owner, and let the vehicle proceed.

14.4. Contraband.

14.4.1. If contraband is found (i.e., stolen property, weapons, drug paraphernalia), immediately stop the examination, secure the contraband and vehicle, and apprehend or detain personnel involved.

14.4.2. All contraband or evidence will be receipted for via AF Form 52 and stored in the SFOI acquired property locker at the SFCC.

14.4.3. Advise suspects of their rights and attempt to obtain consent to search from the operator.

14.4.4. If the individual refuses consent to search, contact the legal office or on-call SJA. The SJA will determine if enough probable cause exists to obtain authority to search from the magistrate.

14.4.5. If the owner/operator is civilian and refuses to have his/her vehicle examined, advise the operator/owner that failure to submit to a BEPC could result in revocation of base driving privileges or base barment actions or both.

14.4.5.1. If the civilian owner/operator still refuses, conduct a walk-around of the vehicle for plain-view evidence that may be used as legal foundation for the authority to search and seize. Consult with legal and security forces chain of command for additional guidance.

14.4.5.2. If the owner/operator is military and refuses to allow his/her vehicle examined, conduct a walk around of the vehicle for plain view evidence. Consult with legal and Security Forces chain of command for additional guidance. **NOTE:** Military members can be lawfully ordered through the base commander to submit to the examination.

14.4.6. If the vehicle is entering the installation and the owner/operator refused the BEPC, the vehicle will not be granted entry.

14.4.7. An AF Form 3545 and blotter entry will be accomplished when personnel refuse consent to a BEPC or when contraband is discovered.

Chapter 15

CONTROL OF PRIVATELY OWNED WEAPONS (POWS)

15.1. This chapter discusses the control of privately owned weapons (POW) at MacDill AFB.

15.2. Military or civilian personnel will not:

15.2.1. Possess any of the following weapons, unless specifically authorized by the 6 AMW/CC:

15.2.1.1. Switchblade knives/

15.2.1.2. Blackjacks, billy clubs, brass knuckles, nunchukas, or throwing stars.

15.2.1.3. Any weapon capable of discharging a chemical agent or tear gas.

15.2.1.4. Any other weapon or instrument used to inflict grievous bodily harm or fear through threat of its use (e.g., straight razors, gas, or compressed air pistols/rifles, or knives with blades in excess of 3 inches, etc.)

15.2.2. Take into or store POWs, ammunition, gunpowder, primers, or black powder other than as directed in this Instruction.

15.2.3. Engage in horseplay involving weapons.

15.2.4. Carry, handle, use, or transport weapons while under the influence of alcoholic beverages or drugs.

15.2.5. Possess or transport loaded firearms.

15.2.6. Leave weapons unattended, except within an authorized storage area.

15.2.7. Take into or store POWs, to include hunting knives, swords, martial arts weapons, archery bows and arrows, pellet/BB guns, and firearms in dormitories or billeting quarters.

15.2.7.1. Weapons maintained for use in martial arts performance by dormitory residents and billeting guests will be stored by the individual's unit.

15.2.7.2. Persons residing in family housing may store their martial arts equipment at their residence.

15.2.7.3. Personnel living in dormitories or family housing may possess their martial arts equipment when in transit to/from martial arts classes.

15.2.8. Firearms Registration. All firearms stored on MacDill AFB will be registered by using AF Form 1314, **Firearms Registration**, at member's unit orderly room. The AF Form 1314 will be typed, legible, and completed as follows:

15.2.8.1. When completing the AF Form 1314, ensure the type, manufacturer, caliber/gauge, and serial number for each firearm being stored is annotated. Housing occupants must put their address on the form and can enter five weapons per card. Individuals storing weapons in the consolidated private weapons depository (CPWD) can only annotate one weapon per form.

15.2.8.2. The squadron commander will sign the AF Form 1314.

15.2.8.3. The orderly room will maintain the original form; the owner will maintain the first copy, and the unit orderly room will send the second copy to 6 SFS/SFTA to be included in the security police automated system (SPAS). For storage in the security forces armory, the individual will bring the completed form to the armory. The armorer will sign it, document it, and distribute the copies.

15.2.8.4. Any changes in member's status (e.g., additions, deletions, PCS, duty phone, etc.), will be coordinated through the individual's orderly room.

15.2.8.5. The unit orderly room will file AF Forms 1314 for each POW on any person assigned to their squadron storing weapons in the CPWD or in base housing. The AF Form 1314 will be stored in a separate location from other forms. The orderly room will file the original copy of the AF Form 1314.

15.2.9. Storage of POWs. POWs will be stored on MacDill AFB under the following provisions:

15.2.9.1. Storage by Dormitory (BOQ/VOQ/VAQ/TLF) Residents. The retention of firearms, ammunition, and other weapons in bachelor male or female living quarters (dormitories) is prohibited. These items must be stored in either the CPWD or by the individuals unit.

15.2.9.2. Personnel residing in base housing, the trailer court and Coons Creek Fam Camp are authorized to retain their firearms/ammunition in their quarters provided each firearm is registered with their orderly room. **NOTE:** Fam Camp residents will register their weapon(s) with the camp director.

15.2.9.2.1. These weapons must be stored in a safe and secure location within their residence and be registered on base.

15.2.9.2.2. The first sergeant/commander of an individual storing POWs in his or her on-base residence and who should not be handling weapons is responsible for ensuring the weapons are removed.

15.2.10. Storage in the CPWD. The CPWD is located in the security forces armory and is the only authorized, on-base storage area for privately owned firearms and ammunition of personnel who reside in dormitories on MacDill AFB. Only small arms ammunition will be stored in the CPWD. There will be no black powder/smokeless powder/primers in any form stored in the CPWD. Ammunition will be stored in a sealed ammo can and issued on an AF Form 1297, *Temporary Issue Receipt*.

15.2.11. Issue of Private Weapons and Ammunition. The CPWD is manned 24 hours a day; therefore, issuing and receiving privately owned weapons and ammunition registered with the CPWD may be done anytime during the week, excluding security forces weapons issuing and turn-in times.

15.2.12. Routine firearm checkouts will be for a maximum of 4 days except when an individual departs on leave, TDY, or the weapon is going to a shop for maintenance. If an individual is going on leave, they need to bring a copy of their leave form to the CPWD for verification.

15.2.13. The day shift armorer will check each day for POWs signed out for more than the authorized time. If there is a POW overdue, the armorer will notify the individual at their duty phone. If the armorer cannot reach the owner, a letter will be sent by the CPWD to the individual's commander.

15.2.14. When firearms are to be stored in the CPWD, the security forces armorer will inspect each firearm component for damage before accepting it for storage. Damage includes scratches on stocks and barrels or broken and missing parts, etc. All damages will be recorded on the AF Form 1314 by

the armorer accepting the firearm. The owner will verify, by their signature on the AF Form 1314, that there is no other external damage to the weapon. The security forces armorer, only upon presentation of the AF Form 1314 and a valid identification card, will issue privately owned firearms.

15.2.15. If the first sergeant/commander of an individual storing POWs in the CPWD feels an individual should not be handling weapons, he or she must contact the CPWD (SF Armory). In this case, the individual's POWs will not be issued until clearance is obtained from either the first sergeant or commander. A "Do Not Arm" letter must be completed by unit within 24 hours.

15.2.16. The CPWD **is not** a designated storage facility for privately owned knives, bows and arrows, pellet/BB guns, or other dangerous weapons. Unit commanders must provide a secure storage facility for these items. Items will be stored in the unit orderly room/first sergeant's office, or suitable area away from the dormitory.

15.2.16.1. These weapons (privately owned knives, bows and arrows, pellet/BB guns, or other dangerous weapons) must be stored in a steel filing cabinet that can be locked with a key lock. These containers will also be secured with an additional padlock and hasp or GSA approved changeable combination padlock.

15.2.16.2. Commanders must develop procedures for issue and accountability of these weapons and ensure they are promptly returned at termination of the checkout period. The use of the AF Form 1314 is suggested.

15.2.17. Transportation of Privately Owned Weapons. POWs will be transported on MacDill AFB under the following provisions:

15.2.17.1. No individual will carry a concealed POW on his or her person or in the vehicle unless authorized by this paragraph.

15.2.17.2. POWs will be unloaded and in plain view while being transported. **EXCEPTION:** POWs may be transported in the luggage compartment or behind the seat of a pick-up truck if the passenger compartment is full. In these cases, the operator must ensure that if contacted by security forces (e.g., ID checks, traffic stops), they immediately notify security forces of the POWs location.

15.2.18. POWs will only be transported to and from place of storage to the Dale Mabry gate or base facility where its use is authorized. This includes weapons such as archery bows and arrows, pellet/BB guns, and paintball guns. **EXCEPTION:** Personnel competing in a shoot at the trap & skeet range may temporarily store their shotgun in a vehicle on the day of the event only. The shotgun **MUST** be transported in accordance with paragraph 17.2.17.2. and, when the vehicle is not in motion, it will be stored "out of sight" in a locked compartment (e.g., trunk or behind the seat in a pick-up truck). The shotgun must remain unloaded at all times and the ammunition must be stored separately.

15.2.19. Authorized Shooting Areas. Discharging POWs and/or hunting/target shooting with any firearm, pellet/BB gun, paintball gun, bow and arrow, crossbow, or similar weapons within the confines of MacDill AFB is prohibited, unless addressed below.

15.2.19.1. Skeet shooting (shotgun only) will be permitted at the skeet range under supervision of range personnel.

15.2.19.2. Bow and arrows and pellet/BB guns are permitted only at the trap and skeet archery range.

15.2.19.3. Use of on-base firing range will be coordinated with the 6th Security Forces Squadron/ Combat Arms Training and Maintenance (6 SFS/CATM). Use of this range will be at the discretion of the range officer, and this privilege may be revoked for any violation of rules or damage to the range.

15.2.19.4. Paintball guns will only be used at the authorized outdoor adventure program (OAP) area or designated security forces training area.

Chapter 16

JURISDICTION

16.1. This chapter discusses military jurisdiction.

16.2. MacDill AFB exercises exclusive jurisdiction within the legal boundaries of the installation, as defined by the installation perimeter fence, with the exception of approximately 3000 square feet south of the Dale Mabry gate.

16.3. There are four entry points to MacDill AFB: Dale Mabry, MacDill, Bayshore, and Port Tampa gates.

16.4. Title 18, The United States Code, and the United States Constitution authorize the detention of civilians for offenses committed on a military installation. Since civilians are not normally subject to the UCMJ, refer civilian violators to a US Magistrate for judicial disposition or to the local civil authorities having jurisdiction.

16.5. All military members are subject to the UCMJ.

16.6. If you have any questions regarding the jurisdiction on MacDill AFB, contact the legal office.

WILLIAM W. HODGES, Maj Gen (Sel), USAF
Commander

Attachment 1**GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS*****References***

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

DOD 5105.21-M-1, *The Security, Use, and Dissemination of Sensitive Compartmented Information Facility*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information Facility*

AFI 31-101, *The Air Force Installation Security Program*

AFI 31-204, *Air Force Motor Vehicle Traffic Supervision*

MacDill AFB OPLAN 31-101, *Installation Security Plan (ISP)*

6 SFS FOI 31-1

6 SFS FOI 31-14, *Building/Structure Security Checks*

Abbreviations and Acronyms

AA&E—Arms, Ammunition, and Explosives

AAFES—Army and Air Force Exchange System

ACC—Air Combat Command

AECS—Advanced Entry Control System

AFI—Air Force Instruction

AFMAN—**Air Force Manual**

AFO—Accounting and Finance Office

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFRES—Air Force Reserve

AFVA—Air Force Visual Aid

ANG—Air National Guard

C4—Command, Control, Communications, and Computers

CUDS—Commercial Interior Intrusion Detection System

COCO—Contractor-Owned, Contractor-Operated

CONUS—Continental United States

CPTED—Crime Prevention Through Environmental Design

DeCA—Defense Commissary Agency

DCID—Director of Central Intelligence Directive
DIS—Defense Investigative Service
DFARS—Defense Federal Acquisition Regulation Supplement
DoD—Department of Defense
DoDD—DoD Directive
DV—Distinguished Visitor
EECS—Electronic Entry Control Systems
FOUO—For Official Use Only
GSA—General Services Administration
GSU—Geographically Separated Unit
GWEN—Ground Wave Emergency Network
GOCO—Government-Owned, Contractor-Operated
HQ—Headquarters
HQ AFISA—HQ Air Force Intelligence Support Agency
HQ AFOSI—HQ Air Force Office of Special Investigations
HQ AFSPA—HQ Air Force Security Police Agency
HQ ESC—HQ Electronic Systems Center
HQ USAF/SP—HQ United States Air Force, Chief of Security Police
ICIDS—Integrated Commercial Intrusion Detection System
ICSP—Installation Chief of Security Police
IDE—Intrusion Detection Equipment
IRPP—Installation Resource Protection Plan
J-SIIDS—Joint-Service Interior Intrusion Detection System
MAJCOM—Major Command
MMV—Mobile Maintenance Van
MWRS—Morale, Welfare, Recreation and Services
NAVAID—Navigational Aids
NMSA—Nonnuclear Munitions Storage Areas
OTH-B—Over-the-Horizon-Backscatter Radar
RCS—Report Control Symbol
RPEC—Resource Protection Executive Committee
RPP—Resource Protection Program

SCI—Sensitive Compartmented Information

SCIF—**SCI** Facility

SP—Security Police

SPAR—Security Police Administration and Reports

SPAS—Security Police Automated Systems

UCMJ—Uniform Code of Military Justice

UL—Underwriter's Laboratory

Attachment 2**OWNER/USER ANTI-ROBBERY PROCEDURES**

Remain as calm as possible.

Sound the alarm as soon as possible (i.e., activate duress alarm or call 911) without making noticeable movements that would tip off the robber.

Do nothing to jeopardize the safety of individuals being robbed or innocent bystanders.

Obtain an accurate description of the robber. As soon as possible, after the robber departs, have all witnesses complete an AF Form 439, Robbery Checklist. Give completed forms to responding security forces personnel.

As soon as possible notify coworkers and the on-duty supervisor of the situation.

Immediately after the robber departs the area, if feasible and without jeopardizing the safety of individuals, determine the direction of travel and mode of transportation. Do not follow immediately behind the robber.

Secure the area and prohibit entry to or exit from the area by personnel other than responding security forces.

Preserve the crime scene. Do not allow personnel to touch or walk around areas where the robber had been.

Identify witnesses, but do not compare notes.

When told to do so by the CCO or alarm monitor, designate a person to meet responding security forces outside the area.

Attachment 3

ALARM ACCESS AUTHORIZATION LIST

MEMORANDUM FOR 6 SFS/SFOR

FROM: Facility Designation

SUBJECT: Alarm Access Authorization For (List Facility Name/Bldg # And Phone Number To Call If Alarm Activates During Business Hours)

1. Persons to contact in an emergency (have at least 2 listed):

NAME	ADDRESS	HOME PHONE
------	---------	------------

2. Custodians (have at least 2 listed. If same as above, state "same as above").

NAME	ADDRESS	HOME PHONE
------	---------	------------

3. Receipt For Authentication Codes:

NAME	SSAN	DUTY PHONE
------	------	------------

4. Activate/Deactivate alarmed facility (if same as #3 above, state "same as #3, above").

NAME	SSAN	DUTY PHONE
------	------	------------

(Personal information contained on this document is to be protected by the Privacy Act of 1974.)

5. Security hours (these are the hours/days the facility is closed).

6. This letter supersedes alarm access list dated _____.

SIGNATURE BLOCK OF COMMANDER

6 SFS/SFOR SIGNATURE BLOCK OR
PERSON DESIGNATED TO SIGN

NOTE: THIS IS THE ONLY FORMAT THAT WILL BE ACCEPTED. WE WANT COMPLETE CONTINUITY ON THESE LETTERS BETWEEN FACILITIES. THIS WILL ENSURE SECURITY FORCES PROVIDE QUICK AND EFFECTIVE SERVICE.

(Personal information contained on this document is to be protected by the Privacy Act of 1974.)

Attachment 4

REQUEST FOR A COLLEGE ACCESS BADGE

MEMORANDUM FOR 6 SFS/SFO

FROM:

SUBJECT: Request for a Long Term College Badge

1. Request a badge be issued to the individual listed below. The individual signing below assumes responsibility while the individual is on base. The individual signing below must also have a DD Form 577, **Signature Card**, on file at the visitor reception facility. The following information is provided:

TYPE OF BADGE: (Check one) _____ **COLLEGE/STUDENT**
_____ **COLLEGE/TEACHER**

NAME: _____ **SSAN:** _____

DOB: _____

SCHOOL/UNIVERSITY: _____

DESTINATION ON BASE: Education Office Bldg. # _____

2. Request the badge be issued with an expiration date not to exceed ONE (1) year. The requested expiration date of this badge will be: _____.

3. If an extension is required, another form will be completed.

4. The individual listed above has been thoroughly briefed on entry procedures and conduct while on MacDill AFB. Please call the undersigned at _____ if there are any questions.

Your Original Signature:

Your typed name: _____ Today's date: _____

THE PERSON SIGNING IT MUST FILL OUT THIS FORM!!!

**(Personal information contained on this document is to be protected
by the Privacy Act of 1974.)**

Attachment 5

REQUEST FOR A TERM ENTRY PASS (AF FORM 75)

MEMORANDUM FOR 6 SFS/SFO

FROM:

SUBJECT: Request for a Term Entry Pass (AF Form 75)

1. Request a pass be issued to the individual listed below. The individual signing below assumes responsibility while the individual is on base. The individual signing below must also have a DD Form 577, *Signature Card*, on file at the visitor reception facility. The following information is provided:

TYPE OF PASS: (Check one) _____ COLLEGE/STUDENT
_____ COLLEGE/TEACHER

NAME: _____ SSAN: _____

DOB: _____

SCHOOL/UNIVERSITY: _____

DAYS/HOURS AUTHORIZED: M/W _____
(circle all that apply) T/TH _____
SA/SU _____

(example 0600-1800 hrs)

DESTINATION ON BASE: Education Office Bldg. # _____

2. Request the pass be issued with an expiration date not to exceed ONE HUNDRED (100) days.
The requested expiration date of this pass will be: _____.

3. If a change or extension is required, another form will be completed.

4. The individual listed above has been thoroughly briefed on entry procedures and conduct while on MacDill AFB. Please call the undersigned at _____ if there are any questions.

Your Original Signature:

Your typed name: _____ Today's date: _____

THE PERSON SIGNING IT MUST FILL OUT THIS FORM!!!

(Personal information contained on this document is to be protected by the Privacy Act of 1974.)

Attachment 6

DESIGNATION OF CONTROLLED AREA LETTER

Date

MEMORANDUM FOR ALL CONTROLLED AREAS

FROM: UNIT/CC

SUBJECT: Designation of Controlled Area

1. Your area (room #), located at Bldg #, is designated a controlled area in accordance with AFI 31-101, paragraph 22.2.1. This designation is due to ??.
2. Any questions regarding this matter may be directed to the Control Area Monitor, ?? at ext 8-????.

COMMANDER'S NAME, Rank, USAF
Commander, Unit Name