

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE INSTRUCTION 31-201**



**30 MARCH 2009**

**AIR COMBAT COMMAND  
Supplement**

**28 MAY 2010**

**Security**

**SECURITY FORCES STANDARDS AND  
PROCEDURES**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at <http://www.e-publishing.af.mil> for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication

---

OPR: HQ AFSFC/SFOP  
Supersedes: AFI31-201, 4 December  
2001

Certified by: HQ USAF/A7S  
(Mr. David R. Beecroft)  
Pages: 60

**(ACC)**

OPR: HQ ACC/A7SOP  
Supersedes: AFI 31-201\_ACCSUP1, June  
2006

Certified by: HQ ACC/A7S  
(Colonel Clifford E. Day)  
Pages:4

---

This instruction implements AFPD 31-2, *Air Provost Operations*. It provides guidance on general Security Forces duties and law enforcement operations. Compliance with this instruction is mandatory and applies to Department of the Air Force military, civilian, Reserve Command, Air National Guard, military and civilian personnel from other US military branches assigned or attached to Air Force units, contract Security Forces, and government-owned, contractor-operated (GOCO) and contractor-owned, contractor operated (COCO) facilities. The terms "must," "shall," and "will" denote mandatory actions in this instruction. This instruction requires the collection and maintenance of information protected by the Privacy Act of 1974 authorized by 50 United States Code 797. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command. Any organization may supplement this instruction. This publication requires the collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain the records prescribed in this publication are Title 10 *United States Code*, Section 8013 and DoD Directive 7730.47. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does

not imply endorsement by the Air Force. **Records Disposition:** Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims>.

**(ACC) AFI 31-201, dated 30 March 2009, is supplemented as follows:** It provides guidance pertaining to general security forces duties and law enforcement operations. and applies to Department of the Air Force military, civilian, Reserve Command, Air Combat Command (ACC)- gained Air National Guard personnel in Title 10 status, military and civilian personnel from other US military branches assigned or attached to ACC units, contract security forces, and government-owned/contractor-operated (GOCO) and contractor-owned/contractor operated (COCO) facilities. This publication requires the collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain the records prescribed in this publication are Title 10 United States Code, Section 8013 and Department of Defense Directive 7730.47. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afrims/afrims/>. Contact supporting records managers as required. Send comments and suggested improvements to this supplement on an AF Form 847, *Recommendation for Change of Publication*, to ACC Security Operations (HQ ACC/A7SO), 129 Andrews Ave, Suite 256, Langley AFB VA 23665-2796.

### ***SUMMARY OF CHANGES***

This document is substantially revised and must be completely reviewed. This revision corrects administrative and typographical errors throughout the text. This document changes all references from Security Police to Security Forces with exception to those referring to the Security Police Shield. This document includes the Security Forces general orders to represent three basic orders all security personnel must follow in performance of their duties. Changes the section responsible for evaluation of SF equipment to HQ AFSFC/SFXR and adds the term Allowance Source Code (ASC) to the acquisition process. The document adds what is a standard requirement for security forces vehicles to include equipment to be contained within the vehicle. This includes video systems contained within SF vehicles, which must be approved by MAJCOM SFs. Additionally, the Installation SJA must coordinate in writing, on the use, presentation, securing and disposition of recorded data obtained by video system. This document also expands on the definition and responsibilities of guardmount and installation entry control. This document identifies the requirement for each SF unit to establish a SF duty officer program. That SF SNCOs and Officers will be appointed to perform post checks, observe exercises, inspect equipment/ facilities, and provide feedback, in writing, to the commander on unit readiness and areas of concern. This document expands on jurisdictional sources that provided SF members jurisdiction, limitations and liability of the laws they are entrusted to enforce. Information and the approval process is also included regarding the authority of

deputization by state and local governments of uniformed law enforcement personnel under the authority of the Air Force, including Security Forces, civilian police, and/or security guards. This document includes Non-lethal weapon information and that the installation Chief of Security Forces will ensure that Security Forces members armed with the handgun, as a primary duty weapon will also carry at least one non-lethal weapon. Because of its effectiveness to and ensure all tools are available to SF members the kneeling search is included as an authorized search method for subjects unable to stand or for safety purposes. All references to the Air Force Law Enforcement Terminal system were removed and replaced by the National Law Enforcement Terminal System (NLETS) and National Crime Information Center (NCIC), which are access systems to computerized law enforcement data. They allow the prompt exchange of law enforcement information between Security Forces and other law enforcement officials. This document also recommends the installation Chief of Security Forces authorize NCIC checks for all visitors entering the installation and if NCIC is not used to screen visitors, the installation Chief of Security Forces should implement a policy so that the screening is done based on set, non-discriminatory criteria, similar to Installation Entry Point Checks. This document defines responsibilities for high-risk incidents, including those of federal, state and local government and the installation commander and installation Chief of Security Forces. This document incorporated changes to the Security Forces After Action Report program and identifies requirements when providing an after action report.

**(ACC) This document is substantially revised and must be completely reviewed.** This supplement has been revised as follows: All paragraphs have been renumbered to reflect AFI 31-201; added Department of the Air Force civilian information for uniforms and equipment will be IAW instructions developed for this purpose; added name only background checks are authorized on those applying for housing on a military installation and current residents who have not already been subjected to a background check; added the requirement for units to submit reports for weapons and ammunition to HQ ACC/A7SOP NLT 24 hours after the incident occurs; added requirements for sending AF Form 3545A when distributing by electronic means.

<b>Chapter 1—FUNCTIONAL RESPONSIBILITIES</b>	<b>8</b>
1.1. Air Force Director of Security Forces (AF/A7S). .....	8
1.2. Headquarters Air Force Security Forces Center (HQ AFSFC). .....	8
1.3. Major Command (MAJCOM) Chief of Security Forces. ....	8
1.4. Installation Commander. ....	8
1.5. Installation Chief of Security Forces (CSF). ....	8
<b>Chapter 2—SECURITY FORCES PERSONNEL</b>	<b>9</b>
2.1. Security Forces Code of Conduct. ....	9
2.2. Duties and Responsibilities. ....	10
<b>Chapter 3—SECURITY FORCES DRESS AND EQUIPMENT</b>	<b>11</b>
3.1. General Information. ....	11
3.1. (ACC) General Information. ....	11

- 3.2. The Security Police Shield. .... 11
- 3.3. Force Protection Function Badge. .... 11
- 3.4. Resources and Equipment. .... 12
- 3.5. Land Mobile Radio (LMR) Systems. .... 12
- 3.6. Telephone Systems. .... 13
- 3.7. Vehicle Equipment. .... 13
- 3.8. SF Vehicle Identification Markings. .... 14
- 3.9. Speedometer Calibration. .... 14
- 3.9. (ACC) Speedometer Calibration. .... 14
- 3.10. Vehicle and Vehicle Equipment Care. .... 15
- 3.11. Vehicle-Mounted Video Surveillance Systems. .... 15

**Chapter 4—SECURITY FORCES ACTIVITIES 16**

- 4.1. Security Forces Guardmount. .... 16
- 4.2. Installation Entry Control. .... 16
- 4.3. Post Checks. .... 16
- 4.4. Post Visits. .... 17
- 4.5. Post Reporting. .... 17
- 4.6. Security Forces Duty Officer Program. .... 17

**Chapter 5—JURISDICTION, LIMITATIONS, AND LIABILITY 18**

- 5.1. Jurisdiction. .... 18
- 5.2. Jurisdiction Sources. .... 18
- 5.3. Jurisdiction Application. .... 19
- 5.4. Jurisdiction Types. .... 20
- 5.5. Security Forces Authority. .... 20
- 5.6. Probable Cause/Reasonable Grounds. .... 21
- 5.7. Posse Comitatus Act. .... 22
- 5.8. Deputization of Air Force Law Enforcement Personnel by State and Local Governments.  
..... 22
- 5.9. Off-duty employment as civilian police officers. .... 23
- 5.10. Support to the US Secret Service (USSS) and US Department of State (DOS). ... 23
- 5.11. Personal Liability. .... 23
- 5.12. Vehicle Operation. .... 23
- 5.12. (ACC) Vehicle Operation. .... 24

<b>Chapter 6—APPREHENSION, DETENTION, AND CUSTODY</b>	<b>25</b>
6.1. Apprehension on Military Installations. ....	25
6.2. Off Installation Patrols. ....	25
6.3. Custody. ....	25
6.4. Searches. ....	25
6.5. Rights Advisement. ....	25
6.6. Use of Force. ....	26
6.7. Transporting Apprehended or Detained Persons. ....	27
<b>Chapter 7—SEARCH, SEIZURE, AND EVIDENCE</b>	<b>28</b>
7.1. Search. ....	28
7.2. Probable Cause Search. ....	28
7.3. Search Incident to Apprehension. ....	28
7.4. Search with Consent. ....	28
7.5. Search of and by the Opposite Sex. ....	29
7.6. Personnel Searches. ....	29
7.7. Off-Installation Searches. ....	29
7.8. Searches Outside the United States, US Commonwealths, and US Territories. ....	29
7.9. Searches Conducted by Foreign Nationals. ....	29
7.10. Entry Point Inspections and Searches. ....	30
7.11. Preserving Evidence. ....	30
<b>Chapter 8—NATIONAL LAW ENFORCEMENT TERMINAL SYSTEM (NLETS) AND     NATIONAL CRIME INFORMATION CENTER (NCIC)</b>	<b>31</b>
8.1. Program Definition. ....	31
8.2. Program Responsibilities. ....	31
8.3. Acquiring and Installing NLETS/NCIC. ....	31
8.4. Training. ....	31
8.5. Providing System Protection. ....	32
8.5. (ACC) Providing System Protection. ....	32
8.6. Criminal History Data. ....	32
8.7. Validation System and Records Maintenance. ....	33
8.8. Agencies Receiving NLETS/NCIC Service. ....	33
<b>Chapter 9—HIGH RISK SITUATIONS</b>	<b>34</b>
9.1. Air Force Philosophy. ....	34

9.2.	Duties and Responsibilities. ....	34
9.3.	Lead Agency Concept. ....	35
9.4.	Off-Installation Incidents. ....	36
<b>Chapter 10—EMERGENCY SERVICE TEAMS (EST)</b>		<b>37</b>
10.1.	Requirements for EST. ....	37
10.2.	Goals. ....	37
10.3.	Capability. ....	37
10.4.	Assignment. ....	37
10.5.	Emergency Medical Skills. ....	38
10.6.	Intelligence. ....	38
10.7.	Interagency Cooperation. ....	38
10.8.	Employment. ....	38
10.9.	Uniforms and Equipment. ....	38
10.10.	Crisis Negotiation Team (CNT). ....	38
10.11.	Planning Considerations. ....	39
10.12.	Initial EST Training. ....	39
10.13.	Military Working Dog (MWD) Team Use. ....	40
10.14.	Reporting Requirements. ....	40
<b>Chapter 11—CRIME PREVENTION</b>		<b>41</b>
11.1.	Definition. ....	41
11.2.	Objectives. ....	41
11.3.	Connection to Integrated Defense. ....	41
11.4.	Role of Security Forces. ....	41
11.5.	Basic Crime Prevention Programs. ....	43
11.6.	Situational Crime Prevention. ....	45
<b>Chapter 12—SECURITY FORCES LESSONS LEARNED</b>		<b>46</b>
12.1.	Purpose. ....	46
12.2.	Types of Reports. ....	46
12.3.	Types of Actions. ....	46
12.3.	(ACC) Types of Actions. ....	46
12.4.	Reporting Requirements. ....	47
12.5.	Reporting Procedures. ....	48

<b>Chapter 13—SECURITY FORCES FORMS</b>	<b>49</b>
13.1. AF Form 52, Evidence Tag. ....	49
13.2. AF Form 53, Security Forces Desk Blotter. ....	49
13.2. (ACC) Blotter distribution is controlled by SF. ....	49
13.3. AF Form 75, Visitor Pass. ....	49
13.4. AF Form 1109, Visitor Register Log. ....	49
13.5. AF Form 1168, Statement of Suspect/Witness/Complainant. ....	49
13.6. AF Form 1176, Authority to Search and Seize. ....	49
13.7. AF Form 1313, Driver Record. ....	49
13.8. AF Form 1315, Accident Report. ....	49
13.9. AF Form 1361, Pick Up/Restriction Order. ....	49
13.10. AF Form 1364, Consent for Search and Seizure. ....	49
13.11. AF Form 3226, Authority to Apprehend in Private Dwelling. ....	50
13.12. AF Form 3907, Security Forces Field Interview Data. ....	50
13.13. DD Form 460, Provisional Pass. ....	50
13.14. DD Forms 2708 and 2708 PA, Receipt for Prisoner or Detained Person. ....	50
13.15. AF Form 3545A, Incident Report. ....	50
13.15. (ACC) AF Form 3545A, Incident Report. ....	50
13.16. Prescribed and Adopted Forms. ....	50
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>52</b>
<b>Attachment 2—USAF SECURITY FORCES MODEL VEHICLE OPERATION POLICY</b>	<b>55</b>
<b>Attachment 3—SECURITY FORCES RESPONSE AND BREVITY CODES</b>	<b>58</b>
<b>Attachment 4—BLOODBORNE PATHOGENS EXPOSURE CONTROL PLAN</b>	<b>59</b>
<b>Attachment 5—SECURITY FORCES LESSONS LEARNED REPORT FORMAT</b>	<b>60</b>

## Chapter 1

### FUNCTIONAL RESPONSIBILITIES

- 1.1. Air Force Director of Security Forces (AF/A7S).** Provides and develops policy and guidance for Security Forces programs in order to protect Air Force installations from terrorism, criminal acts, sabotage and acts of war. HAF/A7S also provides policy and guidance to organize, train and equip Security Forces.
- 1.2. Headquarters Air Force Security Forces Center (HQ AFSFC).** Provides Air Force commanders with guidance on implementation of Security Forces programs.
- 1.3. Major Command (MAJCOM) Chief of Security Forces.** Establishes command unique programs and policies to ensure protection of command installations, personnel, and resources.
- 1.4. Installation Commander.** Establishes base programs and policies to provide a reasonable level of protection to personnel and resources.
- 1.5. Installation Chief of Security Forces (CSF).** Designs Security Forces programs to protect the installation personnel and resources.

## Chapter 2

### SECURITY FORCES PERSONNEL

#### 2.1. Security Forces Code of Conduct. Here are general guidelines for SF performance:

2.1.1. Exercising Authority. On-duty Security Forces and DAF civilian police and guards, are the visible representatives of the US Government, the Air Force, the installation commander, and the installation Chief of Security Forces. It is the duty of Security Forces to accept the authority entrusted to them and to use the authority impartially, firmly, and in a manner that commands respect from the public.

2.1.2. Professional Demeanor. The enforcement of laws and regulations brings Security Forces and DAF civilian police and guards into direct contact with the public. Treat everyone in a dignified and respectful manner.

2.1.3. Personal Appearance. Maintain a high standard of appearance IAW AFI 36-2903, *Dress and Personal Appearance of Air Force Personnel*. Set the example for all to follow.

2.1.4. Personal Attitudes. Perform duties in an impartial, just, friendly, and helpful manner. The Air Force does not tolerate discrimination based on race, color, religion, national origin, or sex.

2.1.5. Assistance to Others. Render assistance to the public. Promptly assist any injured or ill individuals.

2.1.6. Attention to Duty. Remain mindful of duty commitments. Do not consume any form of intoxicant while on duty or within eight hours of a duty tour. Remain alert and vigilant on post at all times.

2.1.7. Seeking Favors. Do not seek personal advantage through status as a Security Forces member. Don't try to gain favor or popularity by showing favoritism, overlooking violations, or otherwise failing to enforce the law. In addition, SF personnel cannot accept any advantage, gratuity, or reward for performing official duties.

2.1.8. Punishment of Offenders. Security Forces have the authority only to apprehend or detain, based on probable cause, but not to punish offenders. Use discretion to correct, caution, or warn someone for minor violations of the law, but do not admonish or reprimand.

2.1.9. Apprehension of Suspects. Protect the health and welfare of all apprehended suspects. Use force according to AFI 31-207, *Arming and Use of Force by Air Force Personnel*. The USAF will not tolerate the intentional or negligent mistreatment of apprehended suspects. Do not use abusive, profane, or insulting language toward a suspect or show disregard for the suspect's valuables, personal property, or physical well being.

2.1.10. Dealing with Intoxicated Persons. Security Forces will apprehend individuals that appear to be intoxicated. Make every effort to avoid verbal and physical confrontations.

2.1.11. Off Duty Conduct. Security Forces must remain above reproach, including in their off-duty conduct.

2.1.12. Protection of Privacy. Security Forces must protect private information. Do not discuss offenses or incidents, except in the line of duty.

**2.2. Duties and Responsibilities.** Security Forces duties and responsibilities vary greatly by installation and post. Each installation Chief of Security Forces will define the duties and limits of Security Forces posts, in local duty or post instructions. The three basic Security Forces General Orders are always the same. They are:

2.2.1. I will take charge of my post and protect personnel and property for which I am responsible until properly relieved.

2.2.2. I will report all violations of orders I am entrusted to enforce and will call my superior in any case not covered by instructions.

2.2.3. I will sound the alarm in case of disorder or emergency.

## Chapter 3

### SECURITY FORCES DRESS AND EQUIPMENT

**3.1. General Information.** Security Forces must wear a distinctive uniform for quick identification. Because Security Forces are constantly in the "public eye," they must set the highest standard of dress and appearance. AFI 36-2903, *Dress and Personal Appearance of Air Force Personnel*, contains guidance on proper wear of Security Forces uniforms.

**3.1. (ACC)General Information.** Although Department of the Air Force civilians are part of the security forces (SF), information for uniforms and equipment will be IAW instructions developed for this purpose.

**3.2. The Security Police Shield.** Only uniformed Security Forces members wear the Security Police shield. Do not abuse this symbol of authority. AFI 31-206, *Security Forces Investigations Program*, establishes procedures for display of the shield by Security Forces investigators not in uniform. The following guidelines apply to the issue and wear of the Security Police shield:

3.2.1. Issue metallic shields IAW Table of Allowance (TA) 016, *Table of Allowances for Special Purpose Clothing and Personal Equipment*.

3.2.2. The Security Police shield is considered a controlled item and will be safeguarded and monitored when issuing.

3.2.3. Reissue serviceable shields.

3.2.4. Wear the metallic shield only on the blue uniform combinations.

3.2.5. Security Forces members who are retraining or separating from the service will turn-in their Security Forces shield to the installation Chief of Security Forces.

3.2.6. The installation Chief of Security Forces may elect to present the shield to retiring Security Forces or the next of kin to Security Forces who die while on active duty.

3.2.7. As the Air Force specialty most closely associated with the enforcement of good order and discipline on an installation, Security Forces Airmen and DAF civilian police and guards of all grades must set the example for others to follow on/off duty. The conduct of Security Forces members must be above reproach at all times. Should a member's on- or off-duty conduct not conform to this standard and have the chain of command question the individual's trustworthiness to execute the authorities vested in that individual, the commander may temporarily or permanently prohibit the member from wearing the Security Police shield and beret. Grounds for removal of the shield, beret, and Force Protection qualification badge include violations of the SF Code to include the (Chapter 2). This action is not punishment; however, it may be associated with administrative, non-judicial, or judicial action. **NOTE:** To permanently remove an Airman's AF Specialty Code, commanders should refer to AFI 36-2626, *Airman Retraining Program*, para 4.3.

**3.3. Force Protection Function Badge.** Chiefs of Security Forces may authorize persons in their command to wear this badge. HAF/A7S may authorize appropriate persons to wear the badge. Award this badge to military personnel who acquire certain skill levels and demonstrate

honorable service in the Security Forces career field. Award the badge according to AFI 36-2903, *Dress and Personal Appearance of Air Force Personnel*.

3.3.1. Allied nation, other US service, and other USAF personnel performing instructor or liaison duty with an Air Force Security Forces organization wear the qualification badge commensurate with time requirements listed in AFI 36-2903.

3.3.2. Airmen assigned to the US Air Force Reserve (USAFR) or ANG are eligible for award of the qualification badge.

3.3.3. Once approved, present the badge at an appropriate ceremony.

3.3.4. The installation CSF may rescind the badge anytime the bearer loses their Security Forces AFSC for misconduct.

**3.4. Resources and Equipment.** HQ AFSFC/SFXR identifies and evaluates commercially available and government-developed equipment necessary to support Service-wide needs for Security Forces personnel. SFXR:

3.4.1. Serves as the central point of contact for Security Forces logistics and requirements throughout the Air Force.

3.4.2. Disseminates Security Forces equipment information, test reports, and material deficiencies.

3.4.3. Monitors new and emerging technologies for Security Forces applications.

3.4.4. Manages, monitors, or provides approval authority, as appropriate, for the following Allowance Source Code (ASC) dealing with Security Forces equipment:

3.4.4.1. ASC 001 -- *Master Equipment Management Index*.

3.4.4.2. ASC 002 -- *Monthly Allowance Notice (Update)*.

3.4.4.3. ASC 009 -- *Small Computers and Equipment*.

3.4.4.4. ASC 012 -- *Vehicles*.

3.4.4.5. ASC 016 -- *Clothing*.

3.4.4.6. ASC 538 -- *Security Forces Equipment (General) and Weapons*.

3.4.4.7. ASC 629 -- *Audio Visual*.

3.4.4.8. ASC 660 -- *Communications Equipment*.

3.4.5. SFXR conducts a semi-annual Air Force Security Forces Equipment Weapons Configuration Board (ECBW) to update equipment listings, provide a forum to work Security Forces-related equipment problems and issues, and work logistics detail issues with MAJCOM Security Forces staff representatives.

**3.5. Land Mobile Radio (LMR) Systems.** The LMR system is the primary means of communication used to control Security Forces operations. MAJCOMs determine requirements for "secure voice" equipment (refer to AFI 31-101, *Integrated Base Defense* for further information).

3.5.1. Security Forces use standard practices to ensure the radio net operates smoothly during normal and emergency situations. Do not use slang language. Military radio

transmissions must comply with Federal Communications Commission (FCC) regulations. The Allied Communication Publication (ACP) 125 (F), dated 5 September 2001, prescribes procedures for Security Forces using two-way radios.

3.5.1.1. The FCC regulates communications by wire and radio. Military radio transmissions are subject to FCC monitoring and regulation.

3.5.1.2. FCC regulations prohibit:

3.5.1.2.1. Use of profane or obscene language in wire or radio communication.

3.5.1.2.2. Use of false or deceptive signals or communications unless otherwise directed for intelligence operations.

3.5.1.2.3. Operation of an unlicensed station.

3.5.1.2.4. Operation of a station by unauthorized personnel.

3.5.2. Net Control Station. When three or more two-way radios use a single radio net (frequency), establish a net control station according to the local installation communications officer's direction.

3.5.3. Commanders ensure a positive Communications Security (COMSEC) program exists for radio communications when they:

3.5.3.1. Use standard response codes to identify the urgency of each radio dispatch. (See attachment 3)

3.5.3.1. (ACC) If additional standard response or brevity codes are developed, publish them in an appropriate local operating instruction.

3.5.3.2. Devise local duress or signal codes to indicate an emergency or duress situation when they do not wish to alert any unauthorized listeners.

3.5.3.3. Decode data encryption system equipped radios before servicing.

3.5.3.4. Decode vehicle radios before releasing the vehicle to any maintenance activity.

3.5.4. Consider equipping the law enforcement desk with a two-way radio capable of communicating on the local civilian police emergency frequency. If a two-way radio is not available or practical, use a mutually agreed upon system that facilitates rapid emergency notification to civilian police like E-911. Negotiate for and fund such equipment at the installation level. Set up operating instructions according to local civilian police regulations.

**3.6. Telephone Systems.** Commercial and tactical telephone systems augment the LMR. Connect all fixed Security Forces posts to the law enforcement desk, central security control, Emergency Control Center (ECC), or Base Defense Operations Center (BDOC) by dial or direct telephone lines.

**3.7. Vehicle Equipment.** TAs and technical orders (TO) establish authorized equipment and markings. As a minimum, equip permanently assigned non-tactical vehicles with the following (exceptions may include posting/investigation vehicles):

3.7.1. Warning Light System. Use a warning light system in the form of a magnetic or permanent mount-type single or multiple flashers, rotating, or strobe light system. Mount the system either on the vehicle roof, on a "roof bar," on the dashboard and rear window

platform, or on the front bumper and the rear window platform. Do not mount lights inside the vehicle front grill.

3.7.2. Siren System. Mount the siren in concert with a roof-mounted warning light system or under the vehicle hood.

3.7.3. Public Address System. Use either a portable system ("bullhorn") or a permanent system. Mount the system in concert with a roof-mounted warning light bar system or under the vehicle's hood.

3.7.4. Spotlight. Use either a portable spotlight (battery-operated or cigarette lighter plug-in type) or a permanently mounted spotlight. If a permanent-mount type is used, mount the spotlight on the vehicle roof, "roof bar," or on the driver's side door frame pillar.

3.7.5. Land Mobile Radio. Use a permanently mounted multi-channel mobile or "portamobile" radio. Install radios so the driver has easy access to all radio controls and microphones and so radio equipment does not interfere with safe vehicle operation.

3.7.6. A general purpose first aid kit (FSN 6545-00-922-1200 or equivalent).

3.7.7. Extinguisher – a 2 1/2 pound ABC rated dry chemical fire extinguisher.

3.7.8. Bloodborne Pathogen Protective Kit (required in all Security Forces vehicles). Contents must include one-way respiratory cardio-pulmonary resuscitation (CPR) mask, surgical gloves, eye protective goggles or glasses with side shields, surgical mask, and surgical gown. The installation Chief of Security Forces and installation medical officer determine other contents of the kit. Train those personnel determined to have occupational exposure to bloodborne pathogens to use kit contents. Attachment 4 contains the requirements for a Bloodborne Pathogen Exposure Control Plan.

3.7.9. Remove unit level equipment before turning in for maintenance.

**3.8. SF Vehicle Identification Markings.** Refer to TO 36-1-191 for guidance on marking Security Forces vehicles.

3.8.1. **(Added-ACC)** SF vehicles with magnetic marking signs may not be operated in areas with active aircraft operations. This reduces the potential for foreign object damage to aircraft.

3.8.2. **(Added-ACC)** Do not permanently mark tactical vehicles as SF vehicles.

**3.9. Speedometer Calibration.** Calibrate the speedometers of all traffic patrol vehicles at least semiannually or sooner if local (city, county, state) laws are more stringent. Recalibrate the vehicle's speedometer any time there are major maintenance repairs to a traffic patrol vehicle's transmission, differential, speedometer, or after tire replacement.

**3.9. (ACC)Speedometer Calibration.** The "calibration" process is to document true vehicle speed. True vehicle speed will be documented in 5 mile per hour (MPH) increments up to the maximum speed safe for the installation, but not to exceed 60 MPH. Post results in each calibrated vehicle. SF units do not "calibrate" their vehicles; however, they may validate speedometer accuracy using stationary radar. All radar units require calibration as designated by the company requirements to ensure accuracy. If vehicle calibration is not correct then vehicle must be turned back in to vehicle management flight for repair.

3.9.1. See local laws on how to calibrate speedometers.

3.9.2. If local (city, county, state) law does not have any standards, develop local procedures and coordinate with SJA to ensure legal requirements are satisfied.

**3.10. Vehicle and Vehicle Equipment Care.** Before each tour of duty, inspect vehicles and vehicle equipment for safety and maintenance deficiencies. Test all warning lights, sirens, public address systems, spotlights, etc. Report deficiencies to the on-duty flight chief/commander. And annotate all discrepancies and deficiencies on the AFTO Form 1800 assigned to that vehicle. If the deficiency is a safety issue, do not operate the vehicle until the deficiency is repaired or corrected. Vehicles should always present a clean appearance, weather permitting.

**3.11. Vehicle-Mounted Video Surveillance Systems.** Units may use vehicle-mounted video surveillance systems as a tool to enhance their law enforcement and public safety role. Carefully evaluate the cost and the need before buying video systems. The following guidelines apply:

3.11.1. MAJCOM SFs approve unit requests for video systems.

3.11.1. (ACC) Units may request the use of vehicle-mounted video surveillance systems after coordination with the installation Staff Judge Advocate (SJA) to ensure compliance with state and local laws. Send these coordinated requests to the ACC Law Enforcement - Provost Marshall Office (HQ ACC/A7SOP) for approval.

3.11.1.1. Installation SJA must coordinate in writing, on the use, presentation, securing and disposition of recorded data. However, as a minimum, the vehicle-mounted video system will only be used when actively engaged in patrol activities (which includes traffic stops or any contact with a person, not on traffic accidents) and cannot be in use when the vehicle is parked and unattended in a non-enforcement function. Recorded data must be processed, maintained and documented in accordance with paragraph 7.11, Preserving Evidence.

3.11.1.2. Vehicle-mounted video surveillance system recorded data must be stored/housed in a locked, tamper proof container with access only by the on duty flight sergeant or flight commander.

3.11.2. There is no centrally managed procurement program. Units must determine needs locally and procure the appropriate system that best meets their needs. Consult MAJCOM, state and local requirements for possible restrictions prior to procurement of any system.

3.11.3. Follow standard supply acquisition procedures.

## Chapter 4

### SECURITY FORCES ACTIVITIES

**4.1. Security Forces Guardmount.** Guardmount is an official military function conducted at the start of the Security Forces shift. Use guardmount to determine the readiness of personnel, to include their appearance and mental and physical condition. Use guardmount to conduct roll call, announcements, security status briefing, weapons inspection, and post assignments. Conduct open ranks inspections at least once per work cycle and annotate it in the Security Forces blotter. Guardmount is also an appropriate opportunity for recognition of deserving personnel.

**4.2. Installation Entry Control.** Controlling entry to the installation is a fundamental Security Forces task. SF control entry to facilitate vehicle and pedestrian access in an orderly, safe, and secure manner, and to provide controls to help protect the installation's resources. Effective entry control begins off the installation with coordination and planning with civil or host nation law enforcement agencies. Entry control is a multi-disciplinary effort incorporating perimeter controls, entry point design, screening, searches, sentry procedures, and consequence management. Commanders at all levels are responsible to understand the integrated nature of installation entry control and mitigate risks. All Airmen are responsible to do their part in controlling authorized entry and preventing unauthorized entry to Air Force installations, particularly as sponsors of base visitors.

4.2.1. The installation entry controller is a symbol of the professionalism and readiness of an Air Force installation. Entry controllers represent the most senior authority on base --usually the installation commander. They are normally the first contact the public has with the Air Force installation, and serve as the Air Force's "ambassadors to the public." This professional SF image is also a key element in deterring criminals and terrorists from even approaching a gate.

4.2.2. A professionally constructed gatehouse is essential, with supporting features such as lighting, traffic calming devices, final denial barriers, and protection from adverse weather. Safety and security for people transiting the gate must be inherent in its design. The entry point should also present an image, which reflects the pride of the installation's mission and the professionalism of the Air Force. Staff the gatehouse with sharp, energetic, and courteous entry controllers.

4.2.3. Installation entry controllers are a key line of defense. Installation entry points are where SF first contacts persons entering the installation. Among many other tasks, the installation gate is the prime spot for SF to stop: unwanted persons, weapons, and contraband from entering the installation; fleeing criminals and stolen property from exiting the installation; and unsafe, uninsured, and unlicensed vehicles and drivers from entering/exiting the installation (including drunk/drugged drivers).

**4.3. Post Checks.** Unit leadership and on duty supervisory personnel will conduct post checks to ensure posted personnel remain alert and are knowledgeable of assigned duties and responsibilities. Post checks also include inspection of Security Forces facilities, vehicles, individual and post-related equipment. Post checks must be documented in the SF blotter.

**4.4. Post Visits.** Post visits are a means for officials to visit on-duty Security Forces. These officials include senior Security Forces representatives, Senior Wing/Base Leaders, First Sergeants, chaplains, etc. Post visits can be used to verify the SF member's job knowledge and performance in their work environment, inspect facilities, take questions, ascertain the welfare of personnel, and build their morale. Post visits should be conducted during both day and night hours.

**4.5. Post Reporting.** Security Forces report the status of their post to the senior person conducting the post check or visit.

**4.6. Security Forces Duty Officer Program.** SF Commanders will establish a SF duty officer program. SF SNCOs and Officers will be appointed to perform post checks, observe exercises, inspect equipment/ facilities, and provide feedback, in writing, to the commander on unit readiness and areas of concern.

## Chapter 5

### JURISDICTION, LIMITATIONS, AND LIABILITY

**5.1. Jurisdiction.** Military jurisdiction is the authority, capacity, power or right to apply the law. This authority involves the right to charge a person with an offense, try him/her in a court and make a final determination of his/her case through courts of appeal. The installation Staff Judge Advocate is the focal point for determining Security Forces jurisdiction. Security Forces members must know the jurisdictions on their installation.

5.1.1. Security Forces are representatives of the US Government, the US Armed Forces, the installation commander, and the installation chief of Security Forces. The Manual for Court-Martial, Rules for Court-Martial (RCM), Rule 302(b)(1), gives the authority to apprehend individuals. Carry out this important duty in a fair, impartial and firm manner.

5.1.2. The Uniform Code of Military Justice (UCMJ), Article 136(b)(6), gives Security Forces the authority to administer oaths to witnesses and suspects, as necessary, in the performance of their duties.

**5.2. Jurisdiction Sources.** There are three sources of military jurisdiction.

5.2.1. U.S. Constitution. The US Constitution established a system of fundamental laws and principles that prescribe the nature, function and limits of our government. Simply said, Security Forces powers are constitutionally founded. The specific provisions of the Constitution relating to military jurisdiction are found in the powers granted to Congress, in the authority vested in the President and in a provision of the Fifth Amendment. This jurisdiction is designed to operate outside of the federal court system. The efficient operation of military law requires a separate judicial system geared to the needs of the military.

5.2.1.1. Article 1, Section 8, authorizes the US Congress to make rules for the government and regulation of the land and naval armed forces. Under this authority, the US Congress enacted the Articles of War and the Articles for the Government of the Navy. The UCMJ was later written for all branches of the US Armed Forces and replaced the early Articles.

5.2.1.2. Article 2, Section 2, provides for the President of the United States to be Commander-in-Chief of the US Armed Forces. Under this authority, the President issues executive orders affecting the US Armed Forces. The UCMJ, Article 36, further states the President of the United States can prescribe rules for court-martial procedure. By virtue of his/her authority under the Constitution and the UCMJ, the President of the United States, by Executive Order, has prescribed the Manual for Courts-Martial (MCM).

5.2.2. Federal Statutes. The second source of jurisdiction is US federal statutes – laws passed by the US Congress. Most of the statutes that directly affect the Air Force are compiled in Title 10, United States Code (U.S.C.).

5.2.3. International Law. The third source of jurisdiction is international law. Military jurisdiction derived from international law is difficult to precisely define. However, civilized nations have observed certain rules in their relationships with each other.

5.2.3.1. The sources of international law are customs, written agreements among nations and the writings of authorities. The Law of Armed Conflict is also included under international law (e.g., citizens of a foreign nation may be tried by military court-martial or commission for certain offenses during wartime).

5.2.3.2. The Law of Armed Conflict is derived from agreements between nations in such international gatherings as The Hague and Geneva Convention's. These conventions spell out the conduct of participants in warfare. The purpose of the law is to restore order and to protect both combatants and noncombatants from unnecessary suffering. It defines the rights of prisoners-of-war, the sick and injured and civilians in occupied territories.

**5.3. Jurisdiction Application.** Jurisdiction applies to persons, places and offenses.

5.3.1. Person. Article 2 of the UCMJ states exactly who is subject to military jurisdiction. Those personnel subject to military jurisdiction that Security Forces personnel are likely to come in contact with include:

5.3.1.1. Members of the regular component of the Armed Forces.

5.3.1.2. Cadets, aviation cadets and midshipmen.

5.3.1.3. Members of the reserve components while on inactive training, but in the case of the Army National Guard or the Air National Guard, only when in federal service.

5.3.1.4. Retired, regular component members of the military entitled to pay.

5.3.1.5. Retired, reserve component members receiving military hospitalization.

5.3.1.6. Members of the fleet reserve and the fleet marine reserve.

5.3.1.7. Persons in Armed Forces custody serving a sentence imposed by court-martial.

5.3.1.8. Prisoners of war in custody of the Armed Forces.

5.3.1.9. In time of war, persons with or accompanying the Armed Forces in the field. However, this is only in time of war and subject to certain limitations.

5.3.1.10. Members of the National Oceanic and Atmospheric Administration, Public Health Service, and other organizations, when assigned to and serving with the armed forces.

5.3.1.11. Subject to any treaty or agreement which the United States is or may be a party to any accepted rule of international law, persons serving with, employed by, or accompanying the armed forces outside the United States and outside the Canal Zone, the Commonwealth of Puerto Rico, Guam, and the Virgin Islands.

5.3.1.12. Subject to any treaty or agreement which the United States is or may be a party to any accepted rule of international law, persons within an area leased by otherwise reserved or acquired for use of the United States which is under the control of the Secretary concerned and which is outside the United States and outside the Canal Zone, the Commonwealth of Puerto Rico, Guam, and the Virgin Islands.

5.3.2. Place. Article 5 of the UCMJ states that the Code applies in all places, and there is no restriction on where the case may be heard. The military has jurisdiction to prosecute any offense committed on or off base.

5.3.3. Offenses. The last element is that the offense be subject to court-martial jurisdiction. As Rules for Courts-Martial (RCM) 203 states, "To the extent permitted by the Constitution, court-martial may try an offense under the code..." However, in determining whether subject-matter jurisdiction exists, it is necessary to look at the service member's status at the time the offense is committed. If the service member is lacking a military status at the time of the offense, there is no jurisdiction over that offense, regardless of whether the offense violates any UCMJ article.

**5.4. Jurisdiction Types.** Four types of jurisdiction apply to military installations and facilities.

5.4.1. Exclusive Jurisdiction. The federal government has total or complete jurisdiction of offenses occurring on federal lands. Exclusive jurisdiction gives the federal government the exclusive right to prosecute offenses occurring therein. If persons commit an offense under the UCMJ, they are tried solely by the military, unless the crime also violates some other federal statute. Generally, the federal government will dispose of all cases involving military personnel for offenses committed in areas of federal exclusive jurisdiction. Civilians who commit offenses in areas of federal exclusive jurisdiction can be prosecuted and/or turned over to civilian federal authorities.

5.4.2. Concurrent Jurisdiction. Both the federal and state governments have authority to enforce law on the installation. If there is a potential conflict regarding exercise of jurisdiction, SFS should consult their Staff Judge Advocate for guidance.

5.4.3. Reciprocal (Partial) Jurisdiction. Both the federal and state governments have some authority, but neither has exclusive power. For example, a state may have retained criminal jurisdiction over an installation or part of an installation (housing areas, for example).

5.4.4. Proprietary Jurisdiction. The military exercises the rights of a property owner only. The military does have criminal jurisdiction (UCMJ) over military personnel in these areas. The military exercises no criminal jurisdiction over the area with civilians. Examples include some housing areas and some recreational retreat areas.

5.4.5. Martial Law. The term "martial law" means "the temporary military government of a civilian population." Declaring US federal martial law might require the US to exercise jurisdiction over the civilian population. In time of an emergency, military jurisdiction over the civilian population extends beyond the restoration of law and order. It provides relief and rehabilitation of the people, the resumption of industrial production, the re-establishment of the economy, and the protection of life and property.

**5.5. Security Forces Authority.** Rule 302 of the Manual for Courts-Martial and Article 7(b) of the UCMJ give Security Forces authority to apprehend any person subject to trial by court-martial if the Security Forces member is executing security/law enforcement duties. Security Forces have four authorities: to detain, apprehend, report and correct.

5.5.1. Detain. Detaining or detention is a term used for dealing with civilians or other personnel not subject to Article 2 of the UCMJ.

5.5.2. Apprehend. Apprehension is the equivalent of “arrest” in civilian terminology. It means taking a person into custody. The same rules apply to detentions and apprehensions. For example, if a person on base wearing civilian clothes violates the UCMJ, and/or federal and state laws, detain and verify their status. If the detainee is a military member, and it is appropriate, apprehend.

5.5.3. Report. Security Forces members’ responsibility to report includes a requirement to prepare or present an official detailed account of violations of the UCMJ to the proper authorities.

5.5.4. Correct. Security Forces have the authority to correct, caution or warn offenders for minor infractions of laws and regulations. However, Security Forces have no authority to punish an offender, so they must use caution that their action does not constitute an admonition or reprimand.

5.5.5. Federal Law. Security Forces also have the authority to enforce other aspects of federal law and U.S.C. not covered by the UCMJ. Examples which outline the installation commander’s responsibility for protecting personnel and property under their jurisdiction include:

5.5.5.1. The Internal Security Act of 1950.

5.5.5.2. Title 10 and Title 18, United States Code, Section 1382.

5.5.6. Assimilative Crimes Act. Makes criminal and adopts state criminal laws for areas of exclusive or concurrent federal jurisdiction, provided federal criminal law, including the UCMJ, has not defined an applicable offense for the misconduct committed.

**5.6. Probable Cause/Reasonable Grounds.** Apprehend any suspect, subject to the UCMJ, for whom there is probable cause to believe has committed a violation of the UCMJ. Base all apprehensions and detentions on probable cause. Probable cause to apprehend exists when there are reasonable grounds to believe that an offense has been or is being committed and that person to be apprehended committed or is committing it.” Reasonable grounds mean that there is reliable information that a reasonable, prudent person would rely on which makes it more likely than not that something is true. Reasonable grounds are also a logical and rational evaluation of the circumstances of an offense and of the suspect’s connection with the offense Security Forces members can establish reasonable grounds through one of the following:

5.6.1. The Security Forces member actually sees the person commit the crime.

5.6.2. The Security Forces member gets the description of a person or vehicle from another Security Forces member. For example, if the Security Forces controller directs that a particular person be apprehended or detained for assault on another person, the Security Forces member now has reasonable grounds.

5.6.3. The Security Forces member receives a statement by a reliable person. It is very hard to determine a person’s reliability. Security Forces members must use their judgment and/or past experience to determine the validity of this information. Be sure of sources before action is taken.

5.6.4. A superior in the Security Forces member’s chain of command orders an apprehension. Remember, all NCOs, petty officers and commissioned officers have the authority to apprehend anyone violating any section of the UCMJ.

5.6.5. Complainant or victim identifies the alleged perpetrator.

5.6.6. There exists a preponderance of evidence/circumstances to indicate a crime has been committed and/or certain individual(s) were responsible or involved.

**5.7. Posse Comitatus Act.** The Congress of the United States enacted this law in 1878 to restrict the use of the military to enforce civil law, Title 18, U.S.C., Section 1385. See also Title 10 U.S.C., Section 375.

5.7.1. This act prevents military personnel from executing the laws of the states or the laws of the United States except when acting under the authority of the US Constitution, an Act of Congress, and under the direction of the President of the United States. Posse Comitatus governs the use of military personnel only within the Continental United States (CONUS). The Act does not apply to National Guard personnel performing in Title 32 status under the command of a State governor.

5.7.2. This act does not prevent:

5.7.2.1. Military authorities from taking action on incidents involving civilians when such action involves a specific military purpose.

5.7.2.2. A military member acting in an unofficial capacity to make a citizen's arrest or to take other action to preserve the public peace.

5.7.2.3. Security Forces from using force to stop a fleeing felon or suspected felon for the purpose of aiding civilian law enforcement.

5.7.2.4. Actions in the performance of duties employed "off-duty" as a security guard or police officer (i.e. SF members with second jobs).

**5.8. Deputization of Air Force Law Enforcement Personnel by State and Local Governments.** The Secretary of the Air Force is the approval authority for the deputization by state and local governments of uniformed law enforcement personnel under the authority of the Air Force, including Security Forces, civilian police, and/or security guards.

5.8.1. If state or local deputization is needed, the senior installation law enforcement official will prepare the request. The request will be based on the justification guidelines established in DoDI 5525.13, *Limitation of Authority to Deputize DoD Uniformed Law Enforcement Personnel by State and Local Governments*, and will include:

5.8.1.1. The number of uniformed law enforcement personnel to be granted the authority and a certification that they have received the requisite training to affect the type of deputization.

5.8.1.2. The time frame envisioned for the authority to be exercised. Blanket time authorizations will not be considered.

5.8.1.3. The policies and procedures to prevent misuse of the authority to be employed by the requesting installation law enforcement official.

5.8.1.4. A copy of the proposed memorandum of understanding with the state or local jurisdiction that will carry out the deputization, to include the signature of the appropriate official representing that state or local jurisdiction.

5.8.2. Requests for approval will follow the appropriate chain of command to the Secretary of the Air Force for approval. As a minimum, requests will be coordinated through the following:

- 5.8.2.1. Installation Commander
- 5.8.2.2. MAJCOM A7S Director
- 5.8.2.3. HQ Air Force Security Forces Center
- 5.8.2.4. HAF/A7S Director of Security Forces
- 5.8.2.5. HAF/JA
- 5.8.2.6. SAF/GC
- 5.8.2.7. SAF/IG

5.8.3. The Secretary of the Air Force will consider the request and return a decision through appropriate channels.

**5.9. Off-duty employment as civilian police officers.** Off-duty Security Forces enlisted members may serve as members of a civilian police agency, either as a regular or reserve duty police officer provided such service is in their personal capabilities, does not require the exercise of military authority, and does not interfere with their military duties. Subject to the same restrictions, commissioned officers may engage in similar off-duty employment, provided they do not violate the “civil office” restriction found in 10 U.S.C § 973. The restriction provides that regular commissioned officers, and Guard, Reserve, or retired officers called to active duty for more than 270 days, may not accept off-duty employment as a federal, state, or local civilian law enforcement official in any position which qualifies as a “civil office”. Guidance on what constitutes a civil office within the meaning of 10 U.S.C § 973 is contained in AFI 51-902, *Political Activities by Members of the U.S. Air Force*. All off-duty employment of Security Forces personnel (officer and enlisted) is subject to approval of their commander and must be coordinated with the servicing legal office.

**5.10. Support to the US Secret Service (USSS) and US Department of State (DOS).** Refer requests for assistance from other federal agencies to AFOSI. When appropriately tasked to assist, Security Forces support the USSS in the protection of the President and Vice President of the United States, major political candidates, and visiting foreign heads of state. When assigned to such duty, Security Forces are subject to the overall supervision of the Director, USSS, or Director of Diplomatic Security, as appropriate. If working under the support of AFOSI for protective services, Security Forces work under the supervision of the AFOSI Protective Detail Leader.

**5.11. Personal Liability.** Military and civilian courts may review acts performed by military personnel for damages or in criminal proceedings.

**5.12. Vehicle Operation.** Each Chief of Security Forces must ensure Security Forces personnel understand and follow vehicle operation guidelines in this section and in the USAF Model Vehicle Operation Policy shown in Attachment 2. Chiefs of Security Forces may modify this policy to reflect local laws or conditions. The primary concern in emergency driving situations is the protection and safety of all citizens. Do not endanger the public. Nuclear and chemical resource recovery operations are exempt from the provisions of this section.

**5.12. (ACC)Vehicle Operation.** Document training in the individual's local training record for defensive driving, emergency (non-pursuit) driving and emergency pursuit driving.

## Chapter 6

### APPREHENSION, DETENTION, AND CUSTODY

**6.1. Apprehension on Military Installations.** As described in Chapter 5, Security Forces may apprehend any person subject to the UCMJ if probable cause to believe that an offense has been or is being committed and that person to be apprehended committed or is committing it.

6.1.1. Installation Chiefs of Security Forces, with the advice of the installation Staff Judge Advocate, will establish local procedures for handling civilian offenders.

6.1.2. For minor offenses, release civilian offenders to their military sponsor. If they do not have a military sponsor, release them to a relative, friend or on their own recognizance.

6.1.3. The installation commander or appointed magistrate authorizes apprehensions in private dwellings on or off base. Use AF Form 3226, *Authority to Apprehend in a Private Dwelling*, to document this authority.

6.1.4. Release military personnel to their First Sergeant, commander, and/or the designated person acting on behalf of the First Sergeant or commander. The individual will be released to an individual who is an E-7/MSgt or above and is at least one grade higher than the individual being received for. Exception: Individuals of any enlisted rank may be released to a First Sergeant.

**6.2. Off Installation Patrols.** Security Forces performing patrol duties off the installation have the authority to apprehend military personnel.

6.2.1. Develop policies and procedures for patrol activity conducted off installation in consultation with local civilian law enforcement officials and Staff Judge Advocate.

6.2.2. Overseas. The installation commander may authorize off installation patrols. Coordinate with the MAJCOM Staff Judge Advocate before authorizing off installation patrols. Security Forces maintain the authority to apprehend military personnel on or off the installation in an overseas environment in accordance with SOFA or host nation agreements. The authority to detain civilians on a US military installation varies in each host nation. Bilateral agreements and directives must specify such limitations.

**6.3. Custody.** Custody is the restraint of free movement. An apprehension occurs when a Security Forces member clearly notifies a suspect they are under apprehension. This notice should be given orally or in writing, but it may be implied by the circumstances. Once apprehended and in custody, the apprehending officer must control the movements of the offender. Protect the health and welfare of all apprehended suspects.

**6.4. Searches.** Immediately upon apprehending a suspect and for officer safety, conduct a search of the suspect for weapons or items of evidentiary value. This ensures the safety of the Security Forces member and the apprehended individual. The apprehending Security Forces person makes the decision to frisk (without handcuffs) or to search (handcuffed). Base this decision on the situation at hand. The situation may also warrant a search of the area under the suspect's control. (See Chapter 8 for detailed guidance on searches)

**6.5. Rights Advisement.** Advise suspects of their right against self-incrimination according to the UCMJ, Article 31, for active duty military personnel, or the US Constitution, Fifth

Amendment, for civilian personnel. Use the AFVA 31-231, *Advisement of Rights*, for verbal advisement (usually on-scene), or the AF Form 1168, *Statement of Suspect/Witness/Complainant*, for written proof of rights advisement (usually prior to taking a written statement).

6.5.1. Suspects on verified active orders (i.e. active ANG personnel while on active status, and AFR personnel while serving in an active Individual Mobilization Augmentee position) will be advised of their rights according to the UCMJ, Article 31. **NOTE:** Contact local SJA when duty status is in question.

**6.6. Use of Force.** Comply with AFI 31-207, *Arming and Use of Force by Air Force Personnel*, during apprehension and detention of suspects. Always use the minimum force necessary when placing a suspect under apprehension. Use handcuffs, as an intermediate use of force, and firearms only when specifically trained in their use. In addition, Security Forces must strictly adhere to USAF standardized employment procedures.

6.6.1. Handcuffs. The courts consider handcuffing a use of force; therefore, Security Forces must carefully analyze each situation to ensure they use the minimum level of force to protect themselves and others from injury. During an apprehension, Security Forces may apply handcuffs to ensure control of the apprehended individual during detention and search, at the apprehension site, and during transport. When applying handcuffs, Security Forces use a reasonable level of force to achieve control of a resisting detainee. Inform non-resisting detainees of the handcuffing procedure and give them the opportunity to cooperate. Use handcuffs as a precaution against an apprehended person who may become uncooperative or violent, to prevent escape, or to ensure personal safety.

6.6.2. Non-Lethal Weapons. Non-lethal weapons are weapons or techniques that are designed and primarily employed to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment. Non-lethal weapons provide a range of options to obtain subject compliance and achieve objectives short of employing deadly force. Unit Standard Operating Procedures (SOPs) and Tactics, Techniques and Procedures (TTPs) may require adjustment to enable employment of non-lethal weapons and new equipment for the success of specific missions.

6.6.2.1. The installation Chief of Security Forces will ensure that Security Forces members armed with the handgun, as a primary duty weapon will also carry at least one non-lethal weapon, consisting of the collapsible baton, OC pepper spray, electronic control device and/or any combination of these.

6.6.2.1.1. Refer to AFMAN 31-222, *Air Force Use of Force Manual*, for approved non-lethal weapon types and required training for each.

6.6.2.1.2. While overseas or deployed, comply with local SOFA and ROE mandated by the Installation commander.

6.6.2.2. Police Baton and Riot Baton. The installation Chief of Security Forces, with consent of the installation commander, determines the need to carry the police baton and riot baton. Use of the PR-24 police baton is not authorized.

6.6.3. Firearms. Security Forces routinely bear firearms in the performance of duties. AFI 31-207 contains specific criteria for their authorization and use. When responding to an actual incident where a member can reasonably expect to meet an armed adversary, respond

with firearms ready. Security Forces members must base any decision to chamber a round of ammunition in a firearm that's not normally carried with a round chambered, or draw a pistol from the holster, on the circumstances being faced and the threat present. Use realistic and safe exercises to develop the sound judgment required in situations that may involve the use of deadly force. Supervisors and exercise participants must follow the safety considerations outlined in AFI 31-207.

**6.7. Transporting Apprehended or Detained Persons.** Search all persons in custody for weapons before placing them in a Security Forces vehicle and transporting them.

6.7.1. Vehicles must be searched prior to and following transport of persons in custody. Always use seatbelts.

6.7.2. When transporting a suspect, notify the control center of the departure time and destination arrival time (along with odometer readings) for inclusion in the desk blotter.

## Chapter 7

### SEARCH, SEIZURE, AND EVIDENCE

**7.1. Search.** A search is an examination of a person, property, or premise to uncover evidence of a crime or criminal intent (e.g., stolen goods, burglary tools, weapons, etc). Security Forces conduct searches of persons, property, or areas within jurisdictional limitations. Evidence obtained in an illegal search is inadmissible at a court-martial or other legal proceedings.

**7.2. Probable Cause Search.** Probable cause or reasonable belief for a search are circumstances that would lead a reasonable person to believe the person, property or evidence sought is located in the place or on the person to be searched.

7.2.1. The special court-martial convening authority at each installation may appoint a military magistrate to authorize probable-cause searches. Have the installation commander sign the appointment, and specify the installation over which the magistrate has authority. Security Forces will obtain the installation commander's (or appointed military magistrate's) permission to conduct a probable-cause search. Use AF Form 1176, *Authority to Search and Seize*, to document this action.

7.2.2. Most searches require probable cause (reasonable belief) or consent to be valid. There are unique situations where Security Forces do not need probable cause such as when entering certain controlled or restricted areas.

7.2.3. When justified, the manner and extent of the search are commensurate with the reason for the search.

7.2.4. Normally, Security Forces do not conduct a probable cause search based solely on the statement of one individual. However, if there are reasons why that individual is particularly trustworthy or reliable, the search authority may authorize a search. A search authorization request for such searches must detail why they are considering the person trustworthy or reliable.

**7.3. Search Incident to Apprehension.** A search incident to an apprehension can be conducted without obtaining search authority and may include the immediate area over which the apprehended person exercises control. When conducting a search incident to an apprehension, it should be conducted immediately.

**7.4. Search with Consent.** Security Forces may conduct a search based on consent of the individual to search. If a person consents to a search of his or her property or person, Security Forces do not need separate search authority. When obtaining consent to search, the individual giving consent must give it freely and voluntarily. The law does not require the advisement of Article 31 or Fifth Amendment rights to persons who voluntarily give permission for a search.

7.4.1. Consent may be obtained orally or in writing. Use AF Form 1364, *Consent for Search and Seizure*, to obtain written consent to search.

7.4.2. The law may require rights advisement before, during, or after requesting or receiving consent to a search, depending upon if and when the individual becomes a "suspect" and the particular investigative circumstances.

**7.5. Search of and by the Opposite Sex.** When searching members of the opposite sex or premises occupied by members of the opposite sex is sensitive, take certain precautions and carefully consider actions and use common sense.

7.5.1. A search may be conducted of outer garments (e.g., jackets, coats, etc.) and hand carried items of a member of the opposite sex.

7.5.2. Regardless of the sex of the person being searched, conduct frisks in the same manner. Security Forces or other military persons of the same sex conduct the frisk unless an urgent safety or security need exists. Two Security Forces must be present to witness a frisk conducted by the opposite sex.

7.5.3. A search may be conducted of premises exclusively occupied by members of the opposite sex. However, Security Forces or military personnel of the same sex as the occupants of the premises should be present during the search.

7.5.4. Do not conduct body searches of personnel of the opposite sex. If such searches are necessary, Security Forces or other military persons of the same sex as the person searched will conduct the search.

**7.6. Personnel Searches.** There are four types of personnel searches used within the Air Force. In each case, the situation determines the type of search.

7.6.1. Standing. Use the standing search primarily for suspects who do not appear dangerous or violent.

7.6.2. Kneeling. Use the kneeling search when the suspect is a potential physical threat; when a standing search would not be effective because the suspect is significantly larger than the SF member; or if a suspect appears impaired and a standing search could jeopardize their safety.

7.6.3. Prone. Use the prone search when a suspect is aggressive or so physically or mentally impaired that the standing or kneeling search could cause injury to the suspect. This search is ideal for multiple apprehensions and is the primary search used during "high risk" operations.

7.6.4. Complete. Use the complete search, also known as the "strip search," only when placing a person into confinement or when ordered by appropriate authority. Health care providers should supervise complete searches.

**7.7. Off-Installation Searches.** Comply with local, state, and federal law if an off-installation search of a person subject to the UCMJ or their property is necessary.

7.7.1. The installation commander approves any requests for such searches.

7.7.2. Seek the advice of the installation Staff Judge Advocate.

**7.8. Searches Outside the United States, US Commonwealths, and US Territories.** Authority for conducting search and seizure operations outside US federal jurisdiction varies according to geographic locations and US and host nation agreements. Consult with the local Staff Judge Advocate.

**7.9. Searches Conducted by Foreign Nationals.** Command may not delegate the general authority to order or to conduct searches to a foreign national. When making a lawful

apprehension, host-nation contract Security Forces may search the suspect's person, clothing worn, and the property in the suspect's immediate possession. Host nation contract Security Forces may also search a motor vehicle that a suspect was operating or riding in as a passenger. Host-nation law or US and host-nation agreements govern other restrictions or authorizations.

**7.10. Entry Point Inspections and Searches.** Installation commanders may order Security Forces to inspect all or a percentage of motor vehicles entering or leaving their installation (per AFI 31-204, *Air Force Motor Vehicle Traffic Supervision*). They may also authorize searches of specific motor vehicles in the same manner as premise searches.

**7.11. Preserving Evidence.** Preserve all evidence found on a person or at the scene of an offense for use at future judicial proceedings. Maintain the chain of custody.

7.11.1. Record all circumstances surrounding the discovery of evidence (e.g., location of the discovery, date and time, witnesses present, etc). These notes provide facts for an incident report. Additionally, Security Forces may use these notes to testify in court. As a minimum, file a copy of the notes with the incident report. Retain original notes.

7.11.2. Place initials, date and time on all evidence for later identification. Use care not to destroy the evidentiary value of the item through the careless marking of the item. Use envelopes, boxes, plastic bags, etc., to collect evidence. Exercise sound judgment to avoid damaging a valuable stolen item, which may eventually be returned to its owner.

7.11.3. Security Forces units must maintain the capability to store evidence. See AFI 31-206 for evidence storage guidelines.

7.11.4. Maintain a complete "chain of custody" accounting of all personnel who handle evidence. Use AF Form 52, *Evidence Tag*, to preserve the chain of custody. In addition to the discovery location, mark the date, time, and initials of the Security Forces person who discovered the evidence. Make sure this form contains a complete description of the evidence and the signature of each person handling the evidence. Annotate the presence of any witnesses.

7.11.5. Return all evidence items to their rightful owners upon final disposition of a case. Coordinate all releases of evidence with the Staff Judge Advocate.

## Chapter 8

### NATIONAL LAW ENFORCEMENT TERMINAL SYSTEM (NLETS) AND NATIONAL CRIME INFORMATION CENTER (NCIC)

**8.1. Program Definition.** National Law Enforcement Terminal System (NLETS) and National Crime Information Center (NCIC) are access systems to computerized civilian law enforcement data. They allow the prompt exchange of law enforcement information between Security Forces and other law enforcement officials.

**8.2. Program Responsibilities.** The following agencies and personnel are responsible for various aspects of the NLETS/NCIC program:

8.2.1. HQ AFOSI is the US Air Force executive agency for National Crime Information Center (NCIC) matters.

8.2.2. MAJCOMs ensure US Air Force installations in the same state share systems, if practical, and fund system acquisition, installation, and support.

8.2.3. The installation Chief of Security Forces establishes the need for an NLETS/NCIC terminal(s).

**8.3. Acquiring and Installing NLETS/NCIC.** Before acquiring and installing an NLETS/NCIC at a base, the installation Chief of Security Forces:

8.3.1. Contacts the host state system administrator and coordinates action required to become part of the state's system through a dedicated terminal.

8.3.2. Determines the initial cost, to include procurement of power conditioning and continuation interfacing equipment (PCCIE).

8.3.3. Determines recurring costs of terminal equipment.

8.3.4. Receives PCCIE guidance from the base civil engineer.

8.3.5. Coordinates local funding for servicing equipment with base agencies.

8.3.6. Coordinates with the base contracting officer to develop a service agreement.

8.3.7. Determines facility protection and environmental requirements to satisfy state requirements for terminal installation.

8.3.8. Coordinates with the base civil engineer with the necessary building repairs or modification requirements to accommodate NLETS/NCIC.

8.3.9. Coordinates with the base communications squadron to ensure necessary equipment and capabilities exist.

**8.4. Training.** The installation Chief of Security Forces:

8.4.1. Coordinates and establishes training requirements for local operators with the state terminal authorities.

8.4.2. Ensures the training meets state and Federal Bureau of Investigation (FBI) requirements.

- 8.4.3. Ensures training of selected persons in terminal operation.
- 8.4.4. Ensures only trained and qualified persons operate the terminal.
- 8.4.5. Ensures proper documentation of training records.

**8.5. Providing System Protection.** Restrict access to data to official use only. Users and serviced agencies follow the state and NCIC guidance on policies, procedures, formats, and codes required for entering records into the system. Users of the system can include but are not limited to SF members, AF Civilian Police/AF Security Guards, and/or Security Contract Guard personnel requiring an official need of the information.

**8.5. (ACC)Providing System Protection.** Access to information obtained from National Law Enforcement Terminal Systems (NLETS) terminals must be limited to criminal justice purposes only. You must destroy printed NLETS material by shredding once you determine NLETS material is no longer needed. The Department of Justice has determined that National Crime Information Center (NCIC) access to confirm the ability of civilians applying for residence in privatized housing on military installations falls within the scope of previous authorizations for using NCIC and the Interstate Identification Index (III). As a result, installations are now authorized to conduct name-only background checks (name check) on those applying for housing on a military installation and current residents on military installations who have not already been subject to a background check.

**8.6. Criminal History Data.** Computerized Criminal History (CCH) and the National Crime Information Center (NCIC) Interstate Identification Index (III) are federal systems of records and controlled under the Privacy Act of 1974. Grant access to this data for valid law enforcement purposes on a case-by-case basis.

8.6.1. The installation Chief of Security Forces may authorize access to CCH and III on a case-by-case basis. Other than AFOSI, requests from outside the SF unit must be in writing, include the reason for the request, and be approved by the installation Chief of Security Forces. Disclose data according to AFI 33-332, *Privacy Act Program*. Terminate operator access privileges for misuse of terminals.

8.6.1. (ACC) Do not forward or attach copies of computerized criminal history or III data to incident reports sent for command action.

8.6.1.1. It is recommended the installation Chief of Security Forces authorize NCIC III checks for all visitors entering the installation.

8.6.1.1.1. Although this is not a background check, it will provide feedback on whether the person is wanted by any federal agency, to include the national Terrorist Screening Center.

8.6.1.1.2. If NCIC III is not used to screen all visitors, the installation Chief of Security Forces should implement a policy so that the screening is done based on set, non-discriminatory criteria, similar to Installation Entry Point Checks.

8.6.2. Prohibit obtaining the CCH or NCIC III data from other sources except as authorized by the installation Chief of Security Forces.

8.6.3. Keep all requests for CCH or NCIC III check data from outside the SF unit on file for validation purposes. If validation records do not correspond with access-approval files, conduct an inquiry to resolve the difference.

8.6.4. A name/descriptor CCH or NCIC III may be used to screen contractors for work on an installation. Installation Chiefs of Security Forces must coordinate with their local state NCIC access providers for final permission to conduct such checks. When doing so, the following rules apply:

8.6.4.1. Accomplish a fingerprint card and submit to the Federal Bureau of Investigation.

8.6.4.2. Maintain documentation for two years at which time destruction of information is appropriate.

8.6.4.3. Costs of background checks are borne by the organization contracting the service.

**8.7. Validation System and Records Maintenance.** Validate all entries into NCIC III, or State Terminal System (STS). The FBI or STS sends records that require validation to the installation Chief of Security Forces. The installation Chief of Security Forces establishes a validation system that includes:

8.7.1. Security Forces Desk Blotter (AF Form 53) entry or an Incident Report (AF Form 3545A) that reflects a complaint and is prepared by the installation where the offense occurred, serving as source documents for entries.

8.7.2. Use a folder for NLETS or NCIC-directed validation documents from each agency receiving or using NLETS or NCIC service to maintain a list of all system entries.

8.7.3. The installation Chief of Security Forces must select a terminal agency coordinator (TAC) to supervise, train on, and control terminal operations. The TAC uses available documentation to validate entries into the system.

**8.8. Agencies Receiving NLETS/NCIC Service.** Agencies receiving NLETS/NCIC service follow the written requirements and responsibilities provided by the terminal-owning agency. Written requirements include training, physical protection, and validations.

## Chapter 9

### HIGH RISK SITUATIONS

**9.1. Air Force Philosophy.** Installation commanders have the authority and responsibility to maintain law and order on their installations. In some situations, such as an active shooter, Security Forces must take immediate action to neutralize the threat. In other situations, such as a barricaded suspect, the best means of preventing loss of life and property may be to use available resources to contain the situation until the situation can be resolved. As needed, develop memoranda of agreement with local, state, federal agencies, and, for overseas installations, host nation agencies, to be able to call for outside assistance when necessary.

**9.2. Duties and Responsibilities.** Resolution of high-risk incidents on federal property involves many agencies and personnel. Installation plans should identify the role of key base agencies. Plans must address the use of Security Forces to isolate, contain, and neutralize a terrorist, active shooter, or hostage incident, with or without assistance. Contingency plans should address the use of installation Security Forces, other military forces, and civilian and host nation resources. Installations on foreign soil should coordinate plans with host nation and the State Department (normally the Regional Security Officer of the US Embassy). In overseas situations, the status of forces or other agreements and understandings may determine the use of host nation resources instead of US forces.

9.2.1. Secretary of the Air Force Public Affairs. The SAF/PA provides public affairs guidance and authorizes local responses to news media inquiries for high-risk situations.

9.2.2. HAF. HAF/A7S and SAF/IGX develop policies and procedures for high-risk situations.

9.2.3. Installation Commanders:

9.2.3.1. Prepare contingency plans and provide for initial and immediate response to any incident occurring on the installation, including a capability to counter high-risk situations on their installations.

9.2.3.2. Organize, train, and equip base units to implement the plans.

9.2.3.3. Maintain responsibility for high-risk situations until appropriate authority directs otherwise.

9.2.3.4. Determine the need for hostage negotiators and emergency service teams (EST). If deciding to establish and train Security Forces to perform in these roles, commanders must seek specialized training from the FBI, local law enforcement agencies, or other Services. (See Chapter 11)

9.2.3.5. Determine the response time based on the local threat.

9.2.3.6. Take immediate action to prevent loss of life (i.e. active shooter situation), to protect property and personnel, and restore order, if necessary before the appropriate civilian response force arrives. If the civilian authorities decline jurisdiction, the Air Force will act to resolve the incident. Refer to AFMAN 31-201, Volume 4, *High-Risk Response*, for additional information.

9.2.4. The installation Chief of Security Forces is the primary advisor to the installation commander on hostage negotiations and EST employment.

9.2.5. AFOSI Detachment. AFOSI is the lead Air Force agency responsible for criminal investigations on Air Force installations. The servicing AFOSI detachment is the Air Force liaison with all federal agencies on criminal investigations and will maintain close coordination with civil authorities to exchange information that could indicate a threat to individuals or property on a military installation. AFOSI also provides investigative support within its capabilities when needed.

9.2.6. Local Law Enforcement. The role of state and local law enforcement agencies can be much more complicated. Each installation establishes unique alliances in the form of jurisdictional agreements. Commanders, Staff Judge Advocates, and Chiefs of Security Forces must become familiar with these local arrangements and comply with the negotiated policing protocols.

**9.3. Lead Agency Concept.** Public Law 93-366 and several National Security Directives outline the management of US Government response to high-risk incidents on federal property or terrorist incidents against US citizens, facilities, and/or interests. These publications identify a lead agency for coordinating US Government actions to resolve both terrorist and high-risk incidents. Specifically, lead agency designations include:

9.3.1. The Department of State (DOS). The Department of State is the lead agency for U.S. government efforts to combat terrorism through use of “soft power” (diplomacy/foreign aid-related) overseas.

9.3.2. The Department of Homeland Security (DHS). DHS is the principal Federal Department for domestic crisis management. Pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies.

9.3.3. The Department of Justice (DOJ) and Federal Bureau of Investigation (FBI). DOJ is the lead agency for threats or acts of terrorism overseas and domestically. The Department of Justice assigns lead responsibility for operational response to the FBI.

9.3.3.1. Within the operational response role, the FBI operates as the on-scene manager for the Federal Government. It is FBI policy that crisis management will involve only those Federal agencies requested by the FBI to provide expert guidance and/or assistance, as described in PDD-39, Domestic Deployment Guidelines (classified), and the FBI Weapon of Mass Destruction Incident Contingency Plan.

9.3.3.2. The FBI is the lead US Government agency for investigating criminal acts committed against US Government offices and employees on US Government reservations, including military installations, or against US Government property. In addition, the FBI is the lead agency for investigation and prosecution of individuals alleged to have violated the Omnibus Diplomatic Security and Antiterrorism Act of 1986 by committing prohibited acts against Americans abroad. Thus, it is the FBI's responsibility to investigate incidents the installation commander declares "terrorist" in nature. AFOSI remains the Air Force liaison with the FBI and should be notified any time assistance from the FBI may be required.

9.3.4. The Federal Emergency Management Agency (FEMA). FEMA is the lead agency for consequence management within U.S. territory. FEMA retains authority and responsibility to act as the lead agency for consequence management throughout the Federal response. It is FEMA policy to use Federal Response Plan structures to coordinate all Federal assistance to state and local governments for consequence management.

9.3.5. The Transportation Security Administration (TSA). The TSA is the lead agency for international terrorist incidents involving aircraft in flight. The TSA has exclusive responsibility for the direction of law enforcement activity during a hijacking involving in-flight aircraft within the US. The FBI has jurisdiction when the aircraft is not in flight. In this case, "flight" begins when support personnel close and secure the aircraft door, and the aircraft is no longer dependent on ground service. TSA has the lead for aircraft piracy within all the airspace in the United States and its territories. If the hijacking occurs overseas, the host nation, in conjunction with the DOS and DoD, manages intervention.

**9.4. Off-Installation Incidents.** The FBI is the lead federal agency for terrorist incidents occurring off the military installation in the US. AFOSI maintains liaison with the FBI on terrorist incidents occurring off military installations that may impact Air Force operations. DoD Directive 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials*, greatly restricts the use of military forces to enforce civil laws within the territory of the US.

9.4.1. National Defense Area (NDA). The installation commander is ultimately responsible for the protection of military equipment, property, information, or personnel in the US and its territories. If they are at risk, off an installation, the installation commander may declare a National Defense Area to contain and secure the federal government resources.

9.4.2. The Air Force may need to establish an NDA in such situations as when:

9.4.2.1. Aircraft divert to civilian airports.

9.4.2.2. An aircraft carrying nuclear weapons makes an emergency landing.

9.4.2.3. It is necessary to temporarily stop the movement of an off-base nuclear weapons convoy.

9.4.2.4. An aircraft crashes.

9.4.2.5. Any other unplanned emergency occurs pertaining to military personnel or assets.

## Chapter 10

### EMERGENCY SERVICE TEAMS (EST)

**10.1. Requirements for EST.** The formation of emergency service teams is an optional program established at the discretion of the installation commander. The basic unit is a four-person Security Forces team acting as a single tactical team or in conjunction with other teams during high-risk operations. These include, but are not limited to, anti-sniper actions, barricaded suspect neutralization, hostage rescue/negotiations, counterterrorist tactics, and special event operations. The basic premise for the use of EST is that of a tactical team of highly motivated and well-conditioned Security Forces. Specially trained and equipped to function as a team, EST is more effectively and safely employed than a larger group of Security Forces members. The USAF's primary objective in dealing with high-risk situations is to prevent or minimize the loss of life or property by response, containment, negotiation, and yielding to the expertise and unique training of civilian authorities like the FBI and TSA when possible.

**10.2. Goals.** Generally, the goals of any high-risk situation requiring EST employment should include the release of hostages unharmed, protection of bystanders, prevention of injury to responding forces, apprehension of suspects unharmed, and restoration of normal operations. Tasks associated with initial response include crisis point and location identification, site isolation, evacuation of nonessential personnel, establishment of an inner perimeter, and conducting a reconnaissance and intelligence gathering mission.

**10.3. Capability.** Each installation should have the ability to contain potential hostage, sniper, barricaded suspect situations, and acts of terrorism, and to provide a standby force to support special events. If an installation commander desires a pre-selected and highly trained team, assignment to these teams should be voluntary as units receive no additional manpower for this activity. The volunteer nature of their members often determines the effectiveness and success of specialized teams. While designed as stand-alone teams, ESTs must remain capable of teaming up with other teams and elements as situations warrant. Team positions include:

10.3.1. Team Leader. Responsible for primary direction of the operations and team control during deployment.

10.3.2. Marksman. Provides selected firepower at an individual or location. For obvious reasons, this member should possess the sharpest shooting skills and highest level of concentration.

10.3.3. Point Member. Guides the team's movement during search and clear operations. Acts as the reconnaissance component within the search element. Select a quick thinking individual who can maintain composure under stressful conditions.

10.3.4. Defense Member. Provides close protection for the team during movement and deployment.

**10.4. Assignment.** Units with an EST should ensure that team training is a top priority. Lessons learned from high-risk situations such as campus and workplace shootings and hostage situations show that serious threats can strike without warning. If feasible, CSFs should consider consolidating EST members on a similar daily working element, to promote teamwork and

camaraderie. The more time members spend together, the more effective they will become as an EST.

**10.5. Emergency Medical Skills.** Planning for a high-risk or tactical mission should include medical care. Units establishing an EST should also establish a tactical emergency medical support program.

**10.6. Intelligence.** Tactical operations and intelligence are interdependent. Develop and nurture the capacity to gather tactical intelligence. Seek assistance and planning support from the local AFOSI.

**10.7. Interagency Cooperation.** Meet regularly with counterparts from other federal agencies. Conduct meetings at least annually with federal special operations leaders and command personnel (BATF, FBI, US Marshals Service, and US Customs) to discuss tactical analysis and contemporary procedures. Emphasize the necessity for interagency cooperation and training. Periodically include guest speakers from civilian law enforcement teams so attendees can share their experience and expertise.

**10.8. Employment.** Employ the EST as required to resolve situations where loss of life appears imminent. Other considerations include:

10.8.1. The installation maintains functional control of emergency service teams. The installation commander or designated representative directs the decision to assault.

10.8.2. Don't use specialized teams in conjunction with civil disturbances and protest demonstrations, unless intelligence indicates the potential for violence.

10.8.3. Consider using the EST during open house functions. Keep the EST out of sight until actually deployed.

**10.9. Uniforms and Equipment.** Procure the basic equipment authorized for EST through supply channels. For standardization, the battle dress uniform (BDU) or Airman's Battle Uniform (ABU) is the accepted uniform. Use approved equipment listed in TA 538.

**10.10. Crisis Negotiation Team (CNT).** The principal method to resolve crisis situations is through negotiation by the CNT. Hostage negotiation is not necessarily a Security Forces-unique responsibility, but the CNT may include trained Security Forces. Seek local training for negotiators.

10.10.1. EST Relationship with the CNT. EST members do not participate in or influence negotiations. They may, however, pass information to the CNT regarding the hostage taker. When an EST is deployed, the CNT may assist by creating a diversion.

10.10.2. Nonnegotiable Demands. Nonnegotiable demands include:

10.10.2.1. Access or continued access to a nuclear weapon.

10.10.2.2. Release of inmates.

10.10.2.3. Weapons, ammunition, or explosives.

10.10.2.4. Absolute promises of amnesty.

10.10.2.5. Security Forces or AFOSI radios.

10.10.2.6. Tactically significant information.

10.10.2.7. The exchange of Security Forces, AFOSI, other law enforcement persons, or high-ranking officials for hostages. Because of the dangers involved, avoid the exchange of any hostages.

10.10.2.8. Alcohol, narcotics, or other drugs are nonnegotiable unless the demand is reasonable or for the health of an injured or sick hostage.

**10.11. Planning Considerations.** Preplanning and coordination with other base agencies are important to successful resolutions to situations. Preplanning actions include:

10.11.1. Acquisition of base maps and high-risk structure floor plans.

10.11.2. Coordination with AFOSI for technical surveillance and other services.

10.11.3. Coordination with local FBI and law enforcement for special services.

10.11.4. Coordination with base communications personnel for equipment.

10.11.5. Coordination with the base civil engineer and civilian utility companies for control of utilities.

**10.12. Initial EST Training.** Installation commanders choosing to establish an EST must seek initial training and certification for all team members. The Army's Special Reaction Team Course, described below, is an excellent source for initial EST training either in residence or through a Mobile Training Team (MTT). Installation commanders may also seek this type of specialized training from the FBI or from local law enforcement.

10.12.1. US Army Course. The Army's two-week Special Reaction Team (SRT) Course, 7H-F17/830-F12 (Education & Training Course Announcement (ETCA) # L5AZA3P071 0S2A), is offered numerous times annually at Ft Leonard Wood, Missouri. This course provides excellent training for teams designed to handle high-risk situations. Topics range from building entry and tactics to firearms training, trauma aid, operational planning, and physical conditioning. If units decide to use this course to train their emergency service teams, they must comply with Army fitness standards and provide funding for attendance by team members. The Army also teaches this course through the use of a MTT that travels to installations requesting such services. This may be the best option as these MTTs emphasize training designed specifically for the host installation. The installation provides all funding.

10.12.2. Sustainment. The sophistication and perishable nature of EST skills require intense sustainment training. ETCA offers an SRT follow up course identified previously. This course ETCA #L5AZA3P071 0S4A, instructs SRT tactics and special threat operations to include combating terrorism, hostage situation management, instinctive firearms training, surveillance and intelligence reporting, incident preplanning and independent select weapon firing. In summation, following a basic training and certification program, each EST should train regularly to remain proficient. Suggested training topics include:

10.12.2.1. Integration of hostage negotiations and EMS.

10.12.2.2. Forward observer training--observation and recording skills; establishment of a command and control mechanism for forward observer/marksman; marksmanship skills.

10.12.2.3. Intelligence operations to include management, analysis, and intelligence support of tactical operations.

10.12.2.4. Performance-oriented team leader/member skills.

10.12.2.5. Physical fitness.

10.12.2.6. Individual and small group training activities, to include periodic exercises to hone and evaluate preparedness.

**10.13. Military Working Dog (MWD) Team Use.** MWD teams are best employed inside the inner perimeter providing overwatch to avenues of escape. If a suspect attempts to flee, the dog should be used as minimum force to affect apprehension. Only use MWDs with an EST entry team if they have practiced beforehand and the dog is familiar with and tolerable of all team members. Dog teams can interfere with EST tactics, creating hazards. Evaluate the risks associated with use of MWDs on an assault when there are hostages or multiple subjects. If risks are greater than the benefit, do not use MWD teams. If an MWD team is used with the entry team, the entry team will enter first and secure the immediate area prior to MWD team entry. In this situation, the MWD handler should be EST trained and must remain to the rear of the entry team.

**10.14. Reporting Requirements.** Initially report all incidents through OPREP-3 reporting channels (See AFI 10-601). After the incident, the installation Chief of Security Forces provides a Security Forces Lessons Learned report, IAW Chapter 13, on any actual employment of EST.

## Chapter 11

### CRIME PREVENTION

**11.1. Definition.** Crime prevention is a pattern of attitudes and behaviors directed both at reducing the threat of crime and enhancing the sense of safety and security to improve the quality of life in our society and help develop environments where crime cannot flourish.

11.1.1. **The Air Force Vision.** The goal of the Air Force crime prevention program is to eliminate or minimize the opportunity and desire to engage in criminal activities. Prevention and elimination of crime are quality of life issues.

11.1.2. Crime prevention is more than a single focus, law enforcement effort. Effective crime prevention requires interaction among commanders, staff, officers, NCOs, Airmen, civilian employees, and dependents.

**11.2. Objectives.** To have an effective program, clearly describe and widely publicize crime prevention objectives, which include:

11.2.1. Upgrade the protection of personnel and property by educating people to recognize and avoid situations in which they are likely to end up the victim of an assault or robbery. Encourage the installation to invest in better locks; stress the need for consistent use of existing locks and safeguards.

11.2.2. Increase surveillance by encouraging residents and workers to challenge unidentified individuals in dormitory, housing, and work areas; establish neighborhood watch programs; encourage permanent marking of property.

11.2.3. Achieve maximum involvement of the Air Force community and Security Forces in crime prevention activities.

11.2.4. Crime prevention is everyone's responsibility. All members of the base community must be convinced of the need to protect themselves, their neighborhoods, and work areas by supporting crime prevention goals.

**11.3. Connection to Integrated Defense.** The Air Force Crime Prevention Program, by design, complements and works with AFI 31-101, *Integrated Base Defense*. Achieve the goals of both programs through active participation of the total Air Force community.

**11.4. Role of Security Forces.** The role of Security Forces, though pivotal to crime prevention, is that of an educational, technical, and supportive resource--an "enabler or catalyst" rather than a "doer." The primary role of Security Forces law enforcement is that of installation entry control, preventive patrol, armed response, detection, and investigative services. Security Forces also provide equally important technical services such as physical security and resources protection. Security Forces must achieve and maintain proficiency in prevention and resource protection programs.

11.4.1. **Program Manager.** The Crime Prevention Program is a function of Police Services in the S5 branch. The installation Chief of Security Forces selects an individual to manage resource protection and crime prevention functions. Installation Chief of Security Forces focuses resources based on the installation's requirements. The NCOIC, Police Services

Branch, should attend course WCIP07A- *Resource Protection/Crime Prevention Theory, Practice and Management*, PDS Code 1F2.

11.4.2. Considerations. Personnel selected for these positions should have top oral and written communication skills, have the flexibility to work with both young and mature groups, and be willing to work varied hours. Crime prevention specialists keep direct communication with law enforcement shifts, investigations, and reports and analysis, and should have access to operations and command leadership.

11.4.3. Program Responsibilities. The following is a list of the types of crime prevention services the crime prevention program manager may choose to provide for the installation:

11.4.3.1. Establish installation-wide crime prevention programs. This would include assessing needs, identifying problems, establishing objectives, coordinating training, and managing program implementation. It further includes providing continuing analysis, program revision, and community-wide crime prevention consultation services.

11.4.3.2. Use crime statistics to examine crime patterns. Use analyzed data to determine strategies for employment of crime-risk management, as well short- and long-term crime prevention to fight local crime problems.

11.4.3.3. Provide crime trend data to unit commanders, law enforcement, and other interested base agencies. Security Forces use this information to determine selective enforcement techniques and element-level crime prevention techniques.

11.4.3.3. (ACC) SF Management Information System reports will be used to provide short-term (quarterly) and long-term (three years or longer) statistical analysis to the operations flight or Chief of Security Forces (CSF) to formulate directed runs, selective enforcement, etc. The data generated may be provided to the base civil engineers and safety program management offices to assist them with traffic management functions. Refer to AFI 31-101, for guidance on the frequency of ACC reporting requirements. Refer to the Air Force records disposition schedule for retention and disposition of these reports. As a reminder, statistical information may not be released without the approval of the Air Force Network Operations Commander approval. This does not prevent installation commanders or the CSF from using their own statistics to obtain criminal patterns or brief personnel on criminal activity in the local area of their installation. Statistics will not be released for unit, other installation, numbered AF, regional, or major command comparisons.

11.4.3.4. Develop and implement a media campaign to publicize the base crime prevention program, prevailing crime problems, and effective measures to counter these problems.

11.4.3.5. Conduct speaking engagements to promote crime prevention goals. Use Commander's Calls, First Sergeant briefs, social activities, youth gatherings, spouses' club meetings, school visitations, etc.

11.4.3.6. Participate in community projects that foster joint police and community efforts; for example, Operation Identification, neighborhood watch, crime stop, and crime hazard reporting. Determine the effectiveness of each program.

11.4.3.7. Conduct citizen awareness programs that educate the military community on the crime risks they face. Emphasize specific problems and precautions to protect themselves and their property.

11.4.3.8. Provide crime prevention statistics, rates and trend analysis to members of the Installation Defense Council (IDC). Implement programs identified by the IDC.

11.4.3.9. Assist in formulating youth activity programs and selecting volunteers to act as youth leaders and advisors in youth programs.

11.4.3.10. Conduct on-base residential, dormitory, and work area crime prevention surveys for occupants and organizations.

11.4.3.11. Request and distribute crime prevention literature and forms to promote crime prevention programs.

11.4.3.12. Maintain close liaison with civilian organizations and authorities on crime prevention programs. Where possible, set up joint programs to promote military and civilian community involvement and combat mutual crime problems. Participate in local, state, and federal crime prevention activities that benefit the military community.

11.4.3.13. Encourage unit commanders to establish crime prevention programs within their unit and suggest they designate a focal point to coordinate program activities within the unit.

**11.5. Basic Crime Prevention Programs.** As a primary source of information on crime patterns, Security Forces should provide guidance to the community on prevailing kinds of crime and the specific mode of operation used by criminals. Each base has its own unique community environment and crime prevention needs. Some successful programs help prevent the most prevalent types of crime occurring on Air Force bases, including:

11.5.1. Operation Crime Stop. An essential element of crime prevention is the prompt and accurate reporting of imminent crime situations or criminal acts. Some people will report their observations to police only when they know they can remain anonymous. Operation Crime Stop helps overcome reluctance to become involved with Security Forces by providing a single telephone line for crime reporting while allowing witnesses to remain anonymous. Crime Stop provides a safe way to report suspected or actual crimes anonymously. Anonymous crime reports can include school crimes, such as persistent bullying, domestic violence, suspicious activity, threatening acts or behavior, possession of weapons and or the use or sale of illegal drugs

11.5.1.1. Units may install a dedicated Crime Stop telephone at the law enforcement desk, capable of receiving calls from both on and off base, with a single number dedicated to Crime Stop reporting. Advertise the purpose of the dedicated line and the ability to remain anonymous. Distribute Crime Stop reporting materials to other unit personnel and encourage their support of the program. Bases having access to either 911 or Enhanced 911 (E911 provides automatic caller ID) Emergency Reporting Systems may elect to use that system instead.

11.5.1.2. Log each Crime Stop call on an AF Form 53, *Security Forces Desk Blotter*. Begin each entry with "Crime Stop" to aid in statistical retrieval.

11.5.2. Operation Identification. The Operation Identification program, referred to by the logo "OPID", is a crime resistance technique which individuals use to deter burglaries and larcenies. It also provides investigative leads that increase the chances of solving crimes.

11.5.2.1. OPID encourages owners of high value or pilferable property to permanently mark their property with an identifying number. This gives a way to identify the property and to establish ownership. Use the Service prefix "AF-" followed by the owner's last name, plus last 4 digits of his/her social security number. Photograph property not easily marked like rings, watches, silverware, etc.

11.5.2.2. Mark the property by engraving, etching, or by using fluorescent marking devices. Security Forces should maintain one or more electric engravers or other marking devices at the law enforcement desk for checkout by interested personnel.

11.5.3. Crime Hazard Identification Program. One goal of crime prevention is to identify, report, and eliminate as many crime hazards as possible, and thus reduce the opportunity for crime.

11.5.3.1. Security Forces and base-level crime prevention program managers may solicit and issue Crime Hazard Reports to commanders and agency chiefs for corrective actions.

11.5.3.2. Crime Hazard Reminder. Security Forces should leave crime hazard reminders when they discover insecure vehicles, office areas, equipment, or unattended property.

11.5.4. Citizen Awareness Program. The thrust of this program is to educate the base community on crime prevention. Base newspapers and other media are good ways to get the word out on typical crimes, victims, and offenders. Additionally, the installation crime prevention program manager may brief all newly assigned personnel on the local crime program, with an emphasis on precautions to avoid becoming victims of crime.

11.5.5. Military Working Dogs. MWDs are great deterrents to crime. Articles in the local news media announcing their presence and capabilities serve to increase public awareness and acceptance. Use caution when publishing precise details to avoid revealing law enforcement tactics or placing a handler and dog at risk for retaliation.

11.5.6. Selective Enforcement. Selective enforcement focuses Security Forces manpower on local crime and incident problems. It is based on accurate analysis of the time, place, type, and frequency of incidents or violations. The crime prevention program manager tabulates information from complaints, and reports of offenses and vehicle accidents.

11.5.6.1. A good analysis of this information will show the underlying conditions or behaviors that need to be corrected. In many instances, selective assignment of Security Forces may be an effective solution. Crime prevention program managers provide their analysis to the operations flight leadership for patrol activity consideration.

11.5.6.2. Before applying selective enforcement to correct a traffic problem, the analysis should consider whether other solutions would be more effective. For example, analysis may show that the best way to cut accidents at a particular intersection is to trim shrubbery, install a larger stop sign, or repaint the pavement markings. Repeated reports of speeding may require speed enforcement, along with the deterrence of a marked Security Forces vehicle.

11.5.7. Physical Protection Surveys. Security Forces units may establish a program to offer physical protection surveys to residents of base housing, dormitories, and to supervisors of activities not normally inspected or surveyed under the resource protection program. These surveys educate personnel about how to protect themselves and their property. The survey is a critical analysis of the physical protection of the facility. Coordinate surveys with AFOSI when done as part of the antiterrorism or Force Protection program. When feasible, the crime prevention program manager should consider using help from law enforcement specialists who normally patrol the area.

**11.6. Situational Crime Prevention.** Other sources of crime prevention information include:

11.6.1. The Crime Prevention Coalition of America (CPCA). The CPCA is a nonpartisan group of national, state, and federal organizations united to promote citizen action to prevent crime. The USAF is one of the original members of this broad-based, interdisciplinary group whose members represent youth development organizations, municipalities, health care providers, law enforcement, and federal and state organizations, to name a few.

11.6.2. National Crime Prevention Council (NCPC). The NCPC is a nonprofit organization that acts as an advocate for crime prevention policies and programs throughout the nation. Its mission is to enable people to prevent crime and build safer communities. The National Citizens' Crime Prevention Campaign is symbolized by the crime dog, McGruff, and the "Take a Bite Out of Crime" slogan. NCPC manages the day-to-day activities of the public service advertising campaign by providing the following services to coalition members:

11.6.2.1. Develops materials, including posters, brochures, and books that help teach crime prevention skills to citizens of all ages.

11.6.2.2. Provides information, referral services, and technical assistance to people trying to enhance a crime prevention effort.

11.6.2.3. Conducts training in crime prevention skills and techniques.

11.6.2.4. Establishes demonstration programs and practical research to find the most effective ways to prevent crime.

11.6.3. NCPC granted authorization to the USAF to reproduce NCPC-copyrighted material. Security Forces may adopt elements of the national program to meet local needs. For further information, contact the National Crime Prevention Council, 2345 Crystal Drive, Suite 500, Arlington, VA, 22202, [www.ncpc.org](http://www.ncpc.org).

## Chapter 12

### SECURITY FORCES LESSONS LEARNED

**12.1. Purpose.** The Security Forces After Action Report is a living document striving to capture the experiences of significant events in the Security Forces career field. Its purpose is to educate and train our forces. Training and operations planners and leaders at every level can use the examples to focus and guide programs. Commanders and operations staffs can review them with an eye toward local procedural policy, both written and unwritten. Leaders can use them for motivation and training. Most importantly, Security Forces performing front line duty can look inward and reflect on their actions in situations they may potentially face.

**12.2. Types of Reports.** After Action Reports focus on the worker-level to allow quick application for exercises and operations.

12.2.1. Lesson Learned. The Lesson Learned is the most common type of report. It is how a technique, procedure, or practical work-around to overcome a deficiency or shortcoming, or create a better way to accomplish a task.

12.2.2. Issue Report. Issue Reports are similar to Lessons Learned in that they identify a shortcoming, deficiency, or problem, but they do not include a work-around or solution. Include the word "Issue" in the report title (example, "Issue - Spare Parts Kits for Deployed Assets Were Obsolete").

12.2.3. Observation Report. Observation Reports document a technique or circumstance that significantly impacted an operation or training event and should be shared with the Air Force and joint community. Include the word "Observation" in the report title (example, "Observation – Unit-Designed Scheduling Template Reduced Deployed Workload").

12.2.4. Summary Report. Summary Reports document operations and exercises including dates, locations, objectives, major participants, and limitations. A Summary Report may have several Lessons Learned/Issues/Observation reports within it. Submit reports within 30 days of the conclusion of an exercise or operation.

12.2.5. **(Added-ACC)** Miscellaneous. Forward lessons learned/after action reports on air shows/open houses to HQ ACC/A7SOP NLT 30 calendar days after the air show/open house.

**12.3. Types of Actions.** These are examples of actions that require an After Action Report submission. This list is not all inclusive:

**12.3. (ACC)Types of Actions.** Route all final lessons-learned products through HQ ACC/A7SOP for forwarding to the Air Force Security Forces Center (HQ AFSFC).

12.3.1. Shooting Incidents. Any peacetime government firearms discharge meeting the reporting requirements outlined in AFI 31-207, *Arming and Use of Force by Air Force Personnel*. Report all instances where Security Forces used deadly force in the performance of their duties.

12.3.2. Security Incidents. This category includes serious security incidents, unlawful entry to aircraft, sabotage or attempted sabotage to AF aircraft, a breach of aircraft security, acts of vandalism directed at AF priority resources, hijacking or attempts, unauthorized entry into a

launch facility, significant security incidents at AF-sponsored air shows, and damage to aircraft.

12.3.3. Deployments (Actual/Exercise). Examples of Lessons Learned from previous deployments includes: Operations ENDURING FREEDOM and IRAQI FREEDOM.

12.3.4. Law Enforcement Incidents. Actual employment of EST, regardless of the outcome. Robberies or attempts, especially if they involve weapons, munitions, or large sums of money.

12.3.5. Military Corrections Incidents. Inmate escapes and inmate disturbances or riots, and inmates that experience serious injury while in custody.

12.3.6. Information/Industrial Security Incidents. Summaries of major espionage cases, independent research on insider threats, and substantiated cases of industrial espionage/sabotage.

12.3.7. Terrorist Acts. Terrorist attacks at an Air Force base or its resources, bombings/rocket attacks, and significant threats from known terrorist groups.

12.3.8. Civil Disturbances. Protest activities or demonstrations at AF installations, military operations other than war (MOOTW), like peacekeeping operations that lead to civil unrest, migrant camp operations and disaster relief missions involving mass crowd violence or disorder.

12.3.9. Military Working Dog (MWD) Incidents. All training aid losses, incidents in which MWDs are commanded to bite suspects, unprovoked or non-commanded bites on persons other than the MWD handler and any other lessons of value to other MWD handlers.

12.3.10. CATM. Unusual training incidents like a M-240B "cook-off" or explosion of blank rounds, unexpected ricochets, and accidental/negligent weapons discharges.

12.3.11. Miscellaneous. This category provides an avenue for installation Chief of Security Forces to analyze and report any incident that may be of educational value for the Security Forces career field. Examples of the types of incidents previously reported in this section include domestic disturbance response; loss of a Security Forces weapon; base defense training accident; death of a Security Forces member; injury to a Security Forces member while making an apprehension; Security Forces response to a potential suicide; and use of electronic control devices.

12.3.12. Incidents Resulting in Significant Loss of Security Forces manpower. Report all incidents such as, vehicle accidents, arrests, etc...where five or more Security Forces personnel are involved.

12.3.13. **(Added-ACC)** Reports on the loss/theft/misplace of weapons or ammunition will be sent through HQ ACC/A7SOP for forwarding to HQ AFSFC NLT 24 hours after the incident occurs.

**12.4. Reporting Requirements.** Security Forces commanders analyze and report significant incidents that occur during Security Forces operations to include, but not limited to, exercises, special events, deployments and daily operations and will provide After Action Reports on incidents listed in paragraph 13.3. above, using the Security Forces After Action Report Format in Attachment 5 of this AFI.

12.4.1. Provide the final report within 30 days of the conclusion of an exercise or operation or within 15 days after an incident via Joint Lessons Learned Information System (JLLIS).

12.4.1.1. When a report is submitted to JLLIS it is electronically sent to the appropriate MAJCOM, DRU, or FOA for validation and simultaneously HQ AFSFC/SFOP receives a courtesy copy of the report.

12.4.1.2. Once the MAJCOM, DRU, or FOA validates the report it is available to view via the JLLIS website.

12.4.2. For Lessons Learned, Issues, and Observations that identify a problem requiring action at HQ USAF, MAJCOMs, FOAs, DRUs, and Air Staff agencies, AFSFC/SFOP will forward a Lessons Learned report to USAF/A9L not later than (NLT) 30 days following an exercise or operation.

12.4.3. The MAJCOM/A7S will return validated reports to AFSFC/SFOP within 30 days of receipt for publication or recommended dissemination.

**12.5. Reporting Procedures.** The method for submitting Lessons Learned, Issues, Observations, and Summary Reports is the JLLIS web sites at <https://www.jllis.mil/USAF> for the NIPRNET or <http://www.jllis.smil.mil/USAF> for the SECRET Internet Protocol Router Network (SIPRNET) site.

12.5.1. An alternate method, which should only be used as a last resort, of reporting for Air Force-only events is a Word document file that contains the same information. An electronic Word document template for these reports may be downloaded from the JLLIS web sites.

12.5.2. If unable to open, send, or upload to the JLLIS website, send a Word report using the Security Forces After Action Report Format in Attachment 5, via NIPRNET: [sflessonslearned@lackland.af.mil](mailto:sflessonslearned@lackland.af.mil) and SIPRNET: [sflessonslearned@afsfclackland.af.smil.mil](mailto:sflessonslearned@afsfclackland.af.smil.mil).

## Chapter 13

### SECURITY FORCES FORMS

**13.1. AF Form 52, Evidence Tag.** Use this two-part form to record evidence and maintain a chain of custody.

**13.2. AF Form 53, Security Forces Desk Blotter.** Use this form to record a chronology of Security Forces activities during a shift. Security Forces blotters often contain sensitive investigative or Privacy Act information and must be controlled. Restrict distribution of this form (paper and electronic) to the direct chain of command and key agencies such as AFOSI and Staff Judge Advocate. Wing commanders may allow others to receive the blotters.

**13.2. (ACC)Blotter** distribution is controlled by SF. Distribution is determined by the CSF and approved by the installation commander due to the sensitive nature of information contained in the SF blotter. Referral agencies are not authorized daily distribution of the blotter. However, deviations to this policy are authorized if approved by the installation commander. Send blotters to an individual by name and not to an office symbol or group address, when distributing blotters by electronic means. Electronically transmitted blotters must be password protected or common access card (CAC) encrypted and include a warning prohibiting forwarding or further distribution. Emailed blotters will be digitally signed prior to being electronically transmitted. Warnings should include the following statement: "This document contains For Official Use Only information and is subject to the Privacy Act of 1974."

**13.3. AF Form 75, Visitor Pass.** Pass issued to visitors of installations. Form is generally computer generated in SFMIS.

**13.4. AF Form 1109, Visitor Register Log.** Provides a log of visitors/and or personnel entering areas which the entry and/or exit is controlled

**13.5. AF Form 1168, Statement of Suspect/Witness/Complainant.** Use this form to take a written statement from a suspect or accused person, witness, or complainant. Also used to advise an individual of their Article 31/Fifth Amendment rights.

**13.6. AF Form 1176, Authority to Search and Seize.** Use this form to obtain authorization to search and seize per Chapter 8.

**13.7. AF Form 1313, Driver Record.** Use this form as a cumulative traffic record (driving history) for drivers who are principals in motor vehicle traffic accidents or moving traffic violations IAW AFI 31-204, *Air Force Traffic Supervision Program*.

**13.8. AF Form 1315, Accident Report.** Use this form to record investigations of major traffic accidents (refer to AFI 31-204).

**13.9. AF Form 1361, Pick Up/Restriction Order.** Use this form to record facts and provide Security Forces with information about pick-up orders or to place a restriction order on a military member.

**13.10. AF Form 1364, Consent for Search and Seizure.** Use this form to document when an individual consents freely and voluntarily to a search of his or her person or property.

**13.11. AF Form 3226, Authority to Apprehend in Private Dwelling.** Use this form when requiring authority to make an apprehension in a private on-base dwelling.

**13.12. AF Form 3907, Security Forces Field Interview Data.**

**13.13. DD Form 460, Provisional Pass.** Use this form to assist military members in returning to their unit.

**13.14. DD Forms 2708 and 2708 PA, Receipt for Prisoner or Detained Person.** Use this form to transfer prisoners between confinement facilities or to release a detained person to his or her unit commander or representative.

**13.15. AF Form 3545A, Incident Report.** The use of the AF Form 3545A is mandatory for all incidents which are reportable under the Defense Incident Based Reporting System (DIBRS). For additional information refer to AFI 31-203, *Security Forces Management Information System (SFMIS)*. Use this form to record facts about an incident or complaint for the proper military authority. Include in the report all available facts, names of personnel involved and a summary of the initial on-scene investigation.

**13.15. (ACC)AF Form 3545A, Incident Report.** Send AF Forms 3545A to an individual by name and not to an office symbol or group address, when distributing reports by electronic means. Distribution is determined by the CSF and approved by the installation commander due to the sensitive nature of information contained in these reports. Electronically transmitted AF Forms 3545A must be password protected or CAC encrypted and include a warning prohibiting forwarding or further distribution. Warnings should include the following statement: "This document contains For Official Use Only information and is subject to the Privacy Act of 1974."

**13.16. Prescribed and Adopted Forms.**

13.16.1. **Forms Prescribed.** AF Form 52, *Evidence Tag*

AF Form 53, *Security Forces Desk Blotter*

AF Form 75, *Visitor Pass*

AF Form 1109, *Visitor Register Log*

AF Form 1168, *Statement of Suspect/Witness/Complainant*

AF Form 1176, *Authority to Search and Seize*

AF Form 1315, *Accident Report*

AF Form 1361, *Pick Up/Restriction Order*

AF Form 1364, *Consent for Search and Seizure*

13.16.2. **Forms Adopted.** AF Form 1313, *Driver Record*

AF Form 3226, *Authority to Apprehend in a Private Dwelling*

AF Form 3545A, *Incident Report* (SMFIS generated)

AF Form 3907, *Security Forces Field Interview Data*

DD Form 460, *Provisional Pass*

DD Form 2708 and 2708 PA, *Receipt for Prisoner or Detained Person*

LOREN M. RENO, Lt General, USAF  
DCS/Logistics, Installations and Mission Support

**(ACC)**

DAVE C. HOWE, Brigadier General, USAF  
Director, Installations and Mission Support

## Attachment 1

### GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

#### *References*

(**Added-ACC**) AFI 31-201, *Security Forces Standards and Procedures*, 30 March 2009

AFPD 31-2, *Air Provost Operations*

AFI 36-2903, *Dress and Personal Appearance of Air Force Personnel*. 2 Aug 2006

AFI 31-207, *Arming and Use of Force by Air Force Personnel*, 29 Jan 2009

AFI 31-206, *Security Forces Investigations Program*, 1 Aug 2001

AFI 36-2626, *Airman Retraining Program*, 1 Jul 1999

AFI 31-101, *Integrated Base Defense* for further information), 01 Mar 2003

AFVA 31-231, *Advisement of Rights*, 01 Jan 1999

AFI 33-332, *Privacy Act Program*, 29 Jan 2004

AFI 31-204, *Air Force Motor Vehicle Traffic Supervision*), 14 Jul 2000

AFMAN 31-201, Volume 4, *High-Risk Response*, 20 Mar 2002

DoD Directive 5525.5, *DoD Cooperation with Civilian Law Enforcement Officials*, 15 January 1986

DoD Directive 7730.47, *Defense Incident-Based Reporting System (Dibrs)* 15 Oct 1996

DoDI 5525.13, *Limitation of Authority to Deputize DoD Uniformed Law Enforcement Personnel by State and Local Governments*, 28 Sep 2007

Uniform Code of Military Justice (UCMJ)

The Internal Security Act of 1950

Title 10 United States Code, Section 1382

Title 10 U United States Code., Section 375

Title 10 United States Code, Section 8013

Title 18, United States Code, Section 1382

Title 18, United States Code., Section 1385

Homeland Security Act of 2002

Public Law 93-366

#### *Abbreviations and Acronyms*

**ABU**—Airman Battle Uniform

(**Added-ACC**) **ACC**—Air Combat Command

**AFLETS**—Air Force Law Enforcement Terminal System

**AFOSI**—Air Force Office of Special Investigations

**AFSC**—Air Force Specialty Code

**AFSFC**—Air Force Security Forces Center

**ANG**—Air National Guard

**BDU**—Battle Dress Uniform

**(Added-ACC) CAC**—Common Access Card

**CATM**—Combat Arms Training and Maintenance

**CCH**—Computerized Criminal History

**CLEA**—Civilian Law Enforcement Agencies

**COMSEC**—Communications Security

**CONUS**—Continental US

**CPR**—Cardio-Pulmonary Resuscitation

**CSF**—Chief of Security Forces

**DCF**—Defense Force Commander

**DHS**—Department of Homeland Security

**DOS**—Department of State

**EST**—Emergency Service Team

**FBI**—Federal Bureau of Investigation

**FCC**—Federal Communications Commission

**FEMA**—Federal Emergency Management Agency

**HNT**—Hostage Negotiation Team

**(Added-ACC) HQ ACC/A7SO**—ACC Security Operations

**(Added-ACC) HQ ACC/A7SOP**—ACC Law Enforcement/Provost Marshall Office

**(Added-ACC) HQ AFSFC**—Air Force Security Forces Center

**III**—Interstate Identification Index

**LMR**—Land Mobile Radio

**MAJCOM**—Major Command

**(Added-ACC) MPH**—Miles per hour

**MWD**—Military Working Dog

**NCIC**—National Crime Information Center

**NLETS**—National Law Enforcement Terminal System

**OSHA**—Occupational Safety and Health Agency

**PCCIE**—Power Conditioning and Continuation Interfacing Equipment

**RCM**—Rules for Court-Martial

**(Added-ACC) RDS**—Records Disposition Schedule

**SECAF/SAF**—Secretary of the Air Force

**SF**—Security Forces

**SJA**—Staff Judge Advocate

**SSN**—Social Security Number

**STS**—State Terminal System

**TA**—Table of Allowance

**TO**—Technical Orders

**UCMJ**—Uniform Code of Military Justice

**USAFR**—US Air Force Reserve

**USSS**—US Secret Service

### *Terms*

**Apprehension**—The taking of a person into custody.

**Desk Blotter**—A 24 hour, chronological record of significant events during a Security Forces tour of duty.

**Duress**—The result of person being threatened with harm by another person if his/her wishes are not carried out.

**Evidence**—Something admissible in a legal proceeding which may bear on or establish a point in question.

**Jurisdiction**—The power, right, or authority to interpret and apply the law. Refer to para 6.1. for further description of military jurisdiction.

**Search**—An examination of a person, property, or premises to uncover evidence of a crime or criminal intent.

**Subject**—A person, about which credible information exists that would cause a reasonable person to suspect the person may have committed a criminal offense, or otherwise make a person the object of a criminal investigation.

## Attachment 2

### USAF SECURITY FORCES MODEL VEHICLE OPERATION POLICY

#### **A2.1. Non-Emergency Operation of Security Forces Vehicle.** Security Forces personnel will:

A2.1.1. Comply with all installation and state laws when operating USAF-owned or leased vehicles.

A2.1.2. Use seat belts when operating any vehicle.

A2.1.3. Ensure their vehicles have sufficient gas and oil for their and relieving shift and proper inflation of tires.

A2.1.4. Inspect their assigned vehicles prior to their shift for any damage or missing equipment, and inspect the rear seat area for contraband or evidence. Inspect the rear seat area before and after transporting any person.

A2.1.5. Report all vehicle damage or missing equipment to a supervisor prior to placing the vehicle in service.

A2.1.6. Keep vehicles clean and free of trash.

#### **A2.2. Emergency Driving -- General (Non-Pursuit Situations).** The primary concern in emergency driving situations is protection of lives and the safety of all citizens and Security Forces personnel. During emergency driving situations, Security Forces will operate their vehicles with extreme caution. Driving under emergency conditions does not relieve the vehicle operator from the duty to drive with due regard for safety of all persons, nor will these provisions protect the driver from consequences of their disregard for safety of others.

A2.2.1. Emergency Driving Defined. Emergency driving is operation of an authorized emergency vehicle (emergency lights and siren in operation) by Security Forces personnel in response to a life threatening situation or a violent crime in progress, using due regard for safety. *Note: Drivers should not use their emergency flashers during emergency driving as it will make turn signals inoperative.*

A2.2.2. Emergency Driving Conditions. The decision to drive under emergency conditions rests with each individual, subject to supervisory oversight, based on the following conditions:

A2.2.2.1. Consider factors such as driving abilities, traffic volume, time of day, and potential hazard or liability to themselves and the public.

A2.2.2.2. Make emergency responses only when the call involves a life threatening situation or a violent crime in progress.

A2.2.2.3. Have sufficient information to justify emergency driving.

A2.2.2.4. Even when responding to a "patrolman needs assistance" type call, Security Forces must bear in mind that, while a rapid response is important, they must arrive at the scene safely.

A2.2.3. Deciding to Make an Emergency Response. All personnel making an emergency response will immediately notify the desk sergeant of that action by using the term "Code Three." This indicates use of emergency lights and siren. The ranking individual on duty

will override the vehicle operator's decision to make an emergency (Code Three) response if, in his/her judgment, it is not warranted or safe. Additionally:

A2.2.3.1. Security Forces personnel will not operate a vehicle in emergency (Code Three) status if it is occupied by any passengers other than Security Forces. Exception: If Security Forces are transporting injured personnel to a medical facility, use sound judgment when determining to use an emergency (Code 3) response.

A2.2.3.2. Security Forces vehicles without emergency lights and siren will not make emergency (Code Three) responses.

**A2.3. Pursuit Driving.** Pursuit driving is inherently dangerous and should be avoided except in extreme situations. Examples of extreme situations include: Pursuing a vehicle with material that is extremely dangerous to others, such as nuclear, biological, or chemical munitions or components; and pursuing a vehicle whose occupant(s) are suspects in an incident in which deadly force would be authorized. In situations where deadly force would not be authorized, consider an alternative course of action, such as vehicle intercept, where Security Forces strategically move their vehicles into a position to block or disable the suspect vehicle – by the use of barrier systems or “Stop Sticks” for example, without the use of high speed.

A2.3.1. Safety. At no time will pursuit driving endanger the public, Security Forces involved in the pursuit, or Air Force resources. When engaged in a vehicle pursuit, Security Forces must weigh the need to immediately apprehend a suspect against the danger created by the pursuit. Extreme caution must be exercised to ensure public safety.

A2.3.2. Responsibility. Responsibility for the decision to pursue an offender rests with each vehicle operator; however, on-duty Security Forces supervisors can, at anytime, order termination of any vehicle pursuit. Carefully evaluate each situation and consider the following factors:

A2.3.2.1. Mission impact

A2.3.2.2. Local policy.

A2.3.2.3. The danger to the public.

A2.3.2.4. The danger to self and fellow patrols.

A2.3.2.5. Experience and training.

A2.3.2.6. Weather and road conditions.

A2.3.2.7. Time of day (e.g. is it rush hour? Has school just let out? Is it the middle of the night with deserted streets?).

A2.3.2.8. Facilities located along the route (e.g., schools, hospital, shopping centers, etc.).

A2.3.2.9. Type of violation--Even if use of use of deadly force prerequisites are met, this does not mean Security Forces may disregard the safety of the public, other Security Forces personnel, or self. Security Forces may be held responsible for injuries or deaths if they act with reckless disregard for the safety of others.

A2.3.2.10. Vehicle characteristics--use of emergency equipment is essential, so ensure vehicle operators turn on the siren and emergency lights. Use both throughout the pursuit. If vehicle is not equipped with emergency lights and siren, do not pursue.

A2.3.2.11. The warning effect of the siren will decrease rapidly as pursuit speed increases.

A2.3.2.12. Use no more than two marked emergency vehicles in the immediate pursuit. Other Security Forces vehicles will support the pursuit units without actively joining the pursuit. Security Forces should also be positioned to block a suspect vehicle from threatening priority resources.

A2.3.2.13. Close installation gates to contain the suspect vehicle on base.

A2.3.3. Radio and Driving Techniques. Use the radio sparingly and keep the frequency open for the desk sergeant and other units to assist. Where possible, use both hands on the steering wheel to maintain control. In the case of a two-person patrol, the rider conducts the radio communications. If two separate units are involved in the pursuit, the lead patrol concentrates on the suspect vehicle while the second patrol makes all radio transmissions concerning the pursuit. When transmitting, remain calm and speak clearly and coherently. Do not shout. When a pursuit begins, call the desk sergeant immediately and relay the following information:

A2.3.3.1. Direction of travel.

A2.3.3.2. Vehicle description and license number.

A2.3.3.3. Number of occupants.

A2.3.3.4. Exact reason for pursuit.

A2.3.3.5. Traffic conditions and other details that will assist other patrols in the area.

A2.3.4. Terminating a Pursuit. Security Forces must use good judgment throughout a pursuit and continuously evaluate whether to terminate the pursuit. End a pursuit when the risks to bystanders, other traffic, or the pursuing patrolman are unjustified. Supervisors are also responsible for monitoring the pursuit and must order its termination when the risk is not justifiable.

### Attachment 3

#### SECURITY FORCES RESPONSE AND BREVITY CODES

**A3.1. Code 1 (Routine).** When a call is not given a priority code, assume it is routine.

A3.1.1. Respond by observing all traffic laws.

A3.1.2. Never use emergency lights or siren for any routine call.

A3.1.3. If circumstances are unknown to the dispatching agency, the response may be upgraded to Code 2 or Code 3, when reasonably justifiable.

**A3.2. Code 2 (Urgent).**

A3.2.1. A call requiring an immediate response to a non-life-threatening emergency is normally assigned an "urgent" priority.

A3.2.1.1. Respond by observing all traffic laws.

A3.2.1.2. Use emergency lights for all urgent calls.

A3.2.1.3. Sirens are not authorized.

A3.2.1.4. The urgent call is also known as the "silent response." Use this type of response when answering non-life-threatening, crime-in-progress calls.

A3.2.2. Check local, state, territorial, or host nation traffic codes for limitations on use of lights and siren (some traffic codes do not support Code 2 responses).

**A3.3. Code 3 (Emergency).** A call requiring an immediate response to a life-threatening emergency or emergency involving Air Force priority resources is normally assigned an "emergency" priority.

A3.3.1. The use of emergency lights and siren is mandatory; however, use common sense when approaching the scene of the emergency.

A3.3.2. If the emergency lights and siren put Security Forces, victims, or bystanders in peril, turn them off a safe distance from the scene.

**A3.4. Code 4 (Request Wants and Warrants).** Use this code to obtain a check for outstanding wants and warrants on a person or vehicle. Immediately follow this transmission by listing:

A3.4.1. Information about the person to be checked, or

A3.4.2. Description and license plate number of the vehicle to be checked.

## Attachment 4

### BLOODBORNE PATHOGENS EXPOSURE CONTROL PLAN

**A4.1. Blood-borne Pathogens Exposure Control Plan.** Each Security Forces unit will develop a blood-borne pathogen exposure control plan and make it readily available to all unit members. Ensure the plan contains, as a minimum:

A4.1.1. The exposure determination of personnel (those reasonably anticipated, as a result of performing their day-to-day duties, to have potential skin, eye, or mucous membrane contact with blood or other potentially infectious fluids or materials). This determination includes:

A4.1.1.1. A list of all duty positions in which personnel in those positions are likely to be exposed to contaminated material.

A4.1.1.2. A list of all tasks and procedures, or groups of closely-related tasks and procedures, in which exposure may occur, and performed by personnel who handle contaminated material.

A4.1.2. The methods available to prevent contact with blood and other potentially infectious fluids or materials.

A4.1.3. Procedures for those who reasonably believe they have contacted a potentially infectious fluid or material.

A4.1.4. Procedures for placing warning labels on containers or plastic bags containing blood or other potentially infectious material. Labels must comply with Occupational Safety and Health Agency (OSHA) Standard 1910.1030.

A4.1.5. Procedures for keeping records of all incidents and occupational exposures per OSHA Standard 1910.1030.

A4.1.6. Procedures for evaluating circumstances surrounding exposure incidents.

**A4.2. Plan Review and Updates.** Review the exposure control plan at least annually. Update the plan as necessary to reflect new or modified exposure determinations. Coordinate with local medical liaison to ensure relevancy and accuracy.

**A4.3. Training.** Train Security Forces identified in the exposure determination in the use of protective equipment and disposition of possibly contaminated materials. Qualified Security Forces or hospital personnel may conduct this training.

**Attachment 5****SECURITY FORCES LESSONS LEARNED REPORT FORMAT**

- A5.1. Submitted by:** Usually the installation Chief of Security Forces or squadron commander.
- A5.2. Operation/Event Name:** The formal name of the military operation or a brief description of the event, such as: "OPERATION ENDURING FREEDOM at Bagram AB, Afghanistan, from 5 August to 8 December 2007," or "Use of Deadly Force, Sample AFB, MD, 1 April 2008."
- A5.3. Keywords:** Critical terms specific enough to support an automated search for the subject. Example: "law enforcement, use of deadly force."
- A5.4. Title:** Name of the incident. Example: Murder of a Security Forces/robbery.
- A5.5. Observation:** A precise, factual description of the entire incident in narrative format. This section should include background information on the subject.
- A5.6. Discussion:** A critical review of the procedures used and actions accomplished during the incident. The intent is to highlight potential problem areas so readers can prevent similar mistakes or to prompt a review of policy or procedures.
- A5.7. Lessons Learned:** A synopsis of a "better way" or a "best business practice" to handle similar future events.
- A5.8. Recommended Action:** Use this section to outline suggested review actions by higher headquarters.
- A5.9. OPR Comments:** This is an open area designed for the OPR to add any additional comments.