

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

AIR FORCE MANUAL 31-201, VOLUME 4

17 NOVEMBER 2011

Security

HIGH-RISK RESPONSE



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no release restrictions on this publication.

OPR: AFSFC/SFOP

Certified by: AF/A7S
(John A. Fedrigo, SES)

Supersedes: AFMAN 31-201V4, 20 Mar 2002;
AFMAN 31-201V6, 17 May 2002

Pages: 79

This manual implements AFPD 31-2, *Air Provost Operations*. This Manual sets forth guidance regarding Security Forces (SF) standards and procedures of Air Force civilian and military personnel, including the Air Force Reserve and Air National Guard serving in SF roles. It applies to military, civilian and contract personnel as well as military personnel from other US military branches assigned or attached to Air Force units. This includes Air Force Reserve and Air National Guard units. Violations may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. This manual includes material developed by the Critical Incident Response Group, Federal Bureau of Investigations National Academy, Quantico, Virginia and is used with their permission.

Records Disposition: Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 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/afrims/afrims/afrims/rims.cfm>. Refer recommended changes and conflicts between this and other publications to HQ AFSFC/SFOP, 1517 Billy Mitchell Blvd, Bldg 954, Lackland AFB, TX, 78236, on the AF Form 847, *Recommendation for Change of Publication*. Field activities are not required to send implementing publications to the higher headquarters functional OPR for review and coordination before publishing. The use of any manufacturer name, trademark, commercial product, commodity, or service within this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. Information from the previous AFMAN 31-201, Volume 6, *Civil Disturbance*, 17 May 2002, has been incorporated into this document. This document integrates Public Law 93-366, Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, and enables the National Response Framework in the United States Air Force. Countering Threats (Chapter 2) has been included and incorporates Active Shooter, Workplace Violence, and School Violence response; Crisis Negotiation has been added (Chapter 5); Civil Disturbance has been added (Chapter 8); Attachments 2, 3, 5 and 6 have been added.

Chapter 1—SECURITY FORCES ROLE IN EMERGENCY MANAGEMENT RESPONSE	5
1.1. Planning.	5
1.2. Responsibilities.	7
1.3. Phases of Incident Management.	10
1.4. Security Forces Response.	10
1.5. Special Considerations for Response to HAZMAT or CBRNE incidents.	12
1.6. Special Considerations for Criminal or Terrorist Use of CBRNE.	13
1.7. Exercises.	14
1.8. Legal Considerations.	14
Chapter 2—COUNTERING THREATS	15
2.1. Definitions.	15
2.2. Prevention.	15
2.3. Reporting.	16
2.4. Workplace Violence.	16
2.5. School Violence.	17
2.6. Active Shooter.	19
Chapter 3—BARRICADED SUBJECTS	24
3.1. Initial Response.	24
3.2. Containment of the Scene.	24
3.3. Establishing Jurisdiction and Command and Control.	25
3.4. Negotiations.	25
Chapter 4—DOMESTIC VIOLENCE AND ABUSE RESPONSE	26
4.1. Domestic Violence.	26
4.2. Security Forces Role in Domestic Violence.	26

4.3.	Unit Commander’s Role in Domestic Violence.	27
4.4.	Family Advocacy Officer’s Role in Domestic Violence.	27
4.5.	BDOC/ECC Controller’s Role in Domestic Violence.	27
4.6.	Patrol Response.	27
4.7.	Differentiating Types of Disputes.	30
4.8.	Conducting the Interview.	31
4.9.	Security Forces Actions.	31
Chapter 5—CRISIS NEGOTIATION		33
5.1.	Overview.	33
5.2.	Types of Behavior.	33
5.3.	Types of Hostage Takers.	33
5.4.	Reasoning Behind the Taking of Hostages.	33
5.5.	Types of Situations.	34
5.6.	High Risk Indicators.	34
5.7.	Philosophy of Crisis Negotiation.	34
5.8.	Response.	35
5.9.	Operations Section Chief.	36
5.10.	Use of Tactical Teams.	36
5.11.	Negotiation Teams.	36
5.12.	Selecting Team Members.	37
5.13.	Training Negotiation Teams.	38
5.14.	Resiliency.	39
5.15.	First Responder Negotiations.	39
5.16.	Guidelines.	40
5.17.	Suicide Intervention.	41
5.18.	Training.	43
Chapter 6—EMERGENCY SERVICES TEAM (EST)		44
6.1.	Concept.	44
6.2.	Objective.	45
6.3.	Capability.	45
6.4.	Organization.	45
6.5.	Employment.	46
6.6.	Weapons.	46

6.7.	EST Training and Team Certification.	47
6.8.	EST Relationship with CNT.	48
6.9.	MWD Team Use.	49
6.10.	Emergency Medical Readiness.	49
6.11.	Information.	49
6.12.	Interagency Cooperation.	49
6.13.	Exercises.	49
6.14.	Reporting Requirements.	49
Chapter 7—CIVIL DISTURBANCES		50
7.1.	Introduction.	50
7.2.	Definition.	50
7.3.	Federal Intervention and Aid.	50
7.4.	Roles of the States.	51
7.5.	Presidential Powers.	51
7.6.	Causes.	51
7.7.	Locations.	52
7.8.	Role of Military Forces.	52
7.9.	Levels of Disturbances.	53
7.10.	The Participants	54
7.11.	Control Force Social Factors.	55
7.12.	Crowd Tactics.	55
7.13.	Civil Disturbance Training.	57
7.14.	Information Needs.	59
7.15.	Threat Analysis.	59
7.16.	Operations	60
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		64
Attachment 2—CATEGORIES OF SUSPICIOUS ACTIVITY		70
Attachment 3—BEHAVIORAL THREAT INDICATORS		72
Attachment 4—SAMPLE MOA		77
Attachment 5—POSSIBLE SITUATIONS REGARDING ENFORCEMENT OF ORDER WITHIN OR NEAR AIR FORCE INSTALLATIONS		79

Chapter 1

SECURITY FORCES ROLE IN EMERGENCY MANAGEMENT RESPONSE

1.1. Planning. Security Forces cannot afford to wait until disaster strikes before taking action to protect resources and personnel. Security Forces personnel must be able to initially respond and cope with any situation that might occur. The Comprehensive Emergency Management Plan (CEMP) 10-2, *Major Accidents, Natural Disasters, Enemy CBRNE Attacks & Terrorist use of CBRNE*, outlines the necessary actions to cope with on and off base emergencies and disasters. Because of the probability that Security Forces will be the first on scene, it is important that Security Forces personnel become familiar with the terms, duties and responsibilities associated with the Air Force Incident Management System (AFIMS).

1.1.1. AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*, and the CEMP 10-2 contain specific guidance on the categories of EM planning. Security Forces must coordinate with the Defense Force Commander (DFC), EM office, and installation Antiterrorism Officer (ATO) to ensure that the various installation plans are mutually supportive and are consolidated to the greatest degree possible.

1.1.2. Plans must be coordinated through all tasked agencies and should be coordinated with all units/agencies on the installation to eliminate redundancies in planning and operational response capability. Special attention must be given to any memoranda of agreement or mutual aid agreements with civil authorities to ensure roles are clearly defined.

1.1.3. Personnel and equipment accountability during an incident response is critical and must be addressed in the planning stages. Security Forces will be responsible for personnel accountability at the Entry Control Point (ECP) of an incident site and procedures must be clearly defined in plans. Some additional Security Forces specific planning factors to consider are:

1.1.3.1. Post changes and how they will be conducted to ensure a smooth transition during prolonged incidents.

1.1.3.2. Possible Force Protection Condition (FPCON) manning increases.

1.1.3.3. Protection Level (PL) security mission impacts.

1.1.3.4. Identify Personal Protective Equipment (PPE) available and required to continue the mission. Determine if Individual Protective Equipment (IPE) is available on the installation and will it be effective based on the CBRNE/HAZMAT involved.

1.1.3.5. Determine how many Security Forces personnel may be involved and what their equipment requirements are to conduct the mission.

1.1.3.6. Determine what Security Forces vehicles may be involved and if there will be shortages within the unit or installation. Determine if the Logistics Readiness Squadron (LRS) is able to support any additional vehicle requirements. Consider vehicle marking and emergency equipment requirements, if feasible.

1.1.4. Military Working Dog (MWD) planning factors:

1.1.4.1. In some CBRNE/HAZMAT incidents, the MWD may succumb to the materials or agents involved.

1.1.4.2. Before a MWD team processes through a Decontamination Corridor, pre-planning and training must take place. Competent authority will follow guidelines set forth in AFI 31-202, *Military Working Dog Program* and AFMAN 31-219, *The USAF Military Working Dog Program*.

1.1.4.3. The MWD Kennel Master and trainer will schedule familiarization training with the Fire and Emergency Service (FES) HAZMAT and/or Contamination Control Area (CCA) decontamination teams for their MWD teams. This training will familiarize the MWD with the sights, sounds and smells of the decontamination equipment, and learn that FES and CCA personnel, dressed in fire bunker suits, PPE or IPE with full face masks and air tanks do not present a threat to them.

1.1.4.4. Progressive training should include the handler decontaminating the MWD by local decontamination processes including the MWD being soaped down, as if being shampooed and rinsed off.

1.1.4.5. The Kennel Master must discuss with the installation FES HAZMAT Branch Officer any possible MWD issues, i.e., decontamination equipment for MWD, control poles or spare set of control equipment stored in HAZMAT vehicle or trailer.

1.1.4.6. In CBRNE High Threat Areas (HTA) and Medium Threat Areas (MTA), the Kennel Master must plan for MWD safety when collective protective kennels are not available.

1.1.4.7. MWD Team Decontamination: MWD Team decontamination procedures are covered in FM 4-02.18.

1.1.5. Resiliency. To reinforce the Airman Resiliency program we must include the philosophy throughout all phases of planning, response, and recovery operations. Effective planning must include mentally preparing the base populace for the anticipated physical and mental reactions during high risk and stressful situations. These skills will arm personnel with solid coping techniques, which will assist them throughout the incident. Finally, by building and implementing resiliency into the program from start to finish we will decrease the impact these situations can have on our Airmen and reduce the overall recovery time. At a minimum, training must be incorporated into all exercises where exposure to traumatic stress, mass casualties, or high risk to first responders and emergency responders is anticipated.

1.1.5.1. Instilling resiliency building opportunities in our training is critical to ensuring our first responders have the mental toughness to anticipate, react, respond, and recover from high stress situations.

1.1.5.2. Reinforcement and assessment of skills in reality based scenarios/exercises is critical to building resiliency in our first responders.

1.1.5.2.1. When planning training, make your scenarios as realistic as safely possible. Inclusion of trauma and chaos such as realistic simulated injuries and sound effects effectively conditions our brains to deal with real-life situations.

1.1.5.2.2. Consider vigorous physical training for all first responders immediately prior to the training scenario to simulate elevated heart rate and other physiological impacts.

1.1.5.2.3. The Trauma Stress Response (TSR) team can be activated by the Wing Commander IAW AFI 44-153, *Traumatic Stress Response*. The TSR team will provide TSR services to enhance resilience to potentially traumatic events. Exercising the resiliency component of high-risk incidents is a critical part of assessing readiness.

1.2. Responsibilities.

1.2.1. General EM responsibilities are outlined in AFI 10-2501 and AFI 31-201 and further defined in installation-level plans.

1.2.2. The Initial Response Base (IRB) is the nearest military installation having a disaster response capability, regardless of size, to a major accident involving DOD resources. The Air Force IRB responds unless directed otherwise by the MAJCOM, theater, or Air Force Service Watch Cell (AFSWC). Specific actions are included in AFI 10-2501 and AFMAN 10-2504, *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*.

1.2.3. Nuclear Weapons Incident. Installations must provide initial response to incidents involving nuclear weapons and must control the scene until relieved by higher authority. For Security Forces specific responsibilities for response to incidents involving nuclear weapons, refer to DoD 3150.8-M, *Nuclear Weapon Accident Response Procedures (NARP)* and DOD S-5210.41-M_AFMAN 31-108V1, (S) *The Air Force Nuclear Weapons Security Manual* (U).

1.2.4. Emergency Operations Center (EOC). As the AFI 10-2501 designated Office of Primary Responsibility (OPR) for Public Safety and Security, Security Forces play a critical role in the Emergency Operations Center. The Security Forces EOC representative for on-base accidents/incidents will:

1.2.4.1. Report as directed to the EOC and immediately conduct communications checks with the Base Defense Operations Center (BDOC)/Emergency Communications Center (ECC).

1.2.4.2. Obtain the plotted location of the cordon, ECP and staging area as directed by the Incident Commander (IC).

1.2.4.3. Obtain the incident grid location from the BDOC/ECC.

1.2.4.4. Report possible hazards and required Personal Protective Equipment (PPE) to responding Security Forces and inform BDOC/ECC via any communication means.

1.2.4.5. Monitor evacuation of affected buildings inside the cordon and report status to the EOC Director.

1.2.5. The Security Forces EOC representative for off-base accidents/incidents will:

1.2.5.1. Identify the initial IC and inform initial security response unit(s) to report to the IC, if not already accomplished.

1.2.5.2. Request assistance from civilian law enforcement agencies via locally developed procedures.

1.2.5.3. Obtain the ECP grid coordinates and notify EOC to provide the information.

1.2.5.4. Coordinate required Security Forces follow-on units and monitor the following actions:

1.2.5.4.1. Security Forces units report to convoy assembly area and check in as described in the installation's CEMP 10-2.

1.2.5.4.2. The Posting NCO checks security elements for equipment, maps, and clothing.

1.2.5.4.3. The Posting NCO briefs all convoy drivers on road conditions and any identified or potential threats.

1.2.5.4.4. The senior ranking Security Forces member designates a specific Security Forces vehicle to lead the convoy.

1.2.5.4.5. Follow-on units make contact with the Security Forces units at the scene.

1.2.5.4.6. Follow-on units have materials to erect cordon perimeter.

1.2.5.4.7. Follow-on units have National Defense Area (NDA) signs as described in AFI 31-101, *Integrated Defense*.

1.2.5.4.8. Participate in the preparation of the recovery plan.

1.2.5.4.9. Facilitate relocation of the ECP, if required by the IC.

1.2.6. BDOC/ECC Actions:

1.2.6.1. Plot incident site on map or installation common operating picture.

1.2.6.2. Dispatch first responders and emergency responders.

1.2.6.3. Maintain contact with the IC, first responders and emergency responders.

1.2.6.4. Accomplish appropriate checklist(s).

1.2.6.5. Keep Security Forces EOC representative up to date on incident site resource requests.

1.2.6.6. Keep BDOC staff informed of the incident status.

1.2.7. Establishing Cordon and ECP Locations. Each incident site must be cordoned and an ECP established. Some incidents will require an evacuation. The type of incident, amount/type of materials involved, and weather conditions are some factors that will influence the size of the cordon. The cordon size is determined by the IC and will be based on the area affected by the incident and any requirement for additional resources within the cordon area.

1.2.7.1. Cordon. A cordon surrounds the accident area where controls are established to keep emergency responders safe and preclude unauthorized entry. Cordon sizes vary and will be decided by the IC or be predetermined by local guidance. Cordons typically consist of military personnel and/or physical barriers that keep personnel out of the area affected by the incident. The goal of the cordon is prevent contamination and/or injury to

both the personnel manning the cordon and the personnel they are keeping from the scene.

1.2.7.2. The ECP location is established by the IC and initially located upwind or crosswind if upwind is not available, on the perimeter of the cordon, within a 90-degree arc on either side of the current surface wind.

1.2.7.2.1. The ECP must be clearly marked for easy recognition by responding forces. At night, vehicle, flood or similar lights should illuminate the ECP.

1.2.7.2.2. The ECP may be relocated to enhance entry and exit control procedures.

1.2.7.2.3. When conditions (i.e. inclement weather) arise and relocation is not feasible, personnel manning ECPs and cordon/traffic control points should shelter in place or seek the closest cover/protection available.

1.2.8. Evacuation. If required, all nonessential personnel must be directed to evacuate the accident scene in an upwind or crosswind direction towards a point designated by the IC.

1.2.8.1. Removal of aircraft, missiles and other equipment requiring specialized actions is the responsibility of maintenance forces.

1.2.8.2. Personnel evacuating the area should remove equipment, vehicles and material from the danger area.

1.2.8.3. Priorities for evacuation are:

1.2.8.3.1. Injured personnel.

1.2.8.3.2. Endangered personnel.

1.2.8.3.3. PL resources.

1.2.8.3.4. Equipment carrying hazardous material.

1.2.8.3.5. High-value or mission essential equipment.

1.2.8.3.6. Fatalities.

1.2.9. Release of Information. This term applies to public affairs material, of any means/medium for mass communications that is prepared for distribution, to disseminate facts or news to the public. It is also the act of disseminating information to the public. Release of information also includes release of records through the Freedom of Information Act (FOIA) as required by Title 5 United States Code, Section 552, and outlined in AF Supplement to DoD 5400.7-R, *DoD Freedom of Information Act Program*. At an accident scene or situation, Security Forces refer all questions to the Public Affairs Office.

1.2.9.1. Air Force Policy. Air Force policy is to keep the public informed, on a timely basis, of unclassified information concerning Air Force activities, whether favorable or unfavorable.

1.2.9.2. The Installation Public Affairs (PA) Officer will promptly release unclassified information about Air Force accidents or mission aircraft. This must be released promptly to news media representatives and recognized news gathering agencies. Written FOIA requests must be processed through the installation FOIA manager as outlined in AF Supplement to DoD Regulation 5400.7-R_AFMAN 33-302. Public

affairs will coordinate releases of information with the installation Staff Judge Advocate (SJA).

1.2.10. Control of Photography. Refer to AFI 35-101, *Public Affairs Policy and Procedures*.

1.2.11. Responsibilities in Foreign Areas.

1.2.11.1. The Department of State, in cooperation with the Agency for International Development, is responsible for determining US participation in conducting disaster relief operations in overseas locations.

1.2.11.2. The Joint Chiefs of Staff have provided instructions regarding the use of military resources in such operations to the commanders of unified commands for foreign areas.

1.2.11.3. Air Force installation commanders in these areas must include guidance and procedures necessary to ensure prompt and effective response to the requirements of the unified command commander in their CEMP 10-2.

1.2.12. Civil Defense Warning and Notification System. Refer to AFMAN 10-2504, *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*, for further information on this subject.

1.2.13. Important Considerations after an Incident.

1.2.13.1. Rescuing the injured.

1.2.13.2. Preventing further injury and loss of life.

1.2.13.3. Protecting property and investigative data of evidentiary value from loss or damage.

1.2.13.4. Safeguarding any classified information within the vicinity.

1.2.13.5. Meeting the needs of informing the public. Meeting this requirement under the chaotic conditions at an accident site calls for close cooperation and mutual understanding between Security Forces, Public Affairs and the news media representatives.

1.3. Phases of Incident Management. The Air Force Incident Management System (AFIMS) incorporates the five phases of incident management: prevention, preparedness, response, recovery, and mitigation. AFIMS provides the framework with which the installation Disaster Response Force (DRF) responds to all EM incidents. DRF members will respond to an incident per the installation's CEMP 10-2. Refer to AFI 10-2501 and AFMAN 10-2502, *Air Force Incident Management System (AFIMS) Standards and Procedures*, for definitions and tasks assigned during each phase. The Federal Emergency Management Agency's (FEMA's) web site at <http://www.fema.gov/> has information on the National Incident Management System (NIMS). FEMA also offers emergency management training on-line at <http://training.fema.gov/EMI/>.

1.4. Security Forces Response. IAW AFI 10-2501, The Air Force will establish a single integrated EM program to mitigate the effects of major accidents; natural disasters; conventional attacks (including those using high-yield explosives); and terrorist use of CBRN materials on Air

Force personnel, resources, and operations. Reference AFI 10-2501, AFMAN 10-2502 and AFMAN 10-2504 for further guidance and term definitions.

1.4.1. Major Accidents, Including Hazardous Materials (HAZMAT).

1.4.1.1. A major accident is an accident of such a magnitude as to warrant response by the installation DRF. It differs from day-to-day emergencies and incidents that are routinely handled by base agencies without the DRF.

1.4.1.2. Security Forces (SF) are Emergency Responders for HAZMAT events and provide support to First Responders. SF personnel do not fill the traditional roles and responsibilities of civilian law enforcement agencies during HAZMAT events and will not investigate or operate in suspected warm or hot zones. SF will take no further action beyond the following:

1.4.1.2.1. Initiating the alarm sequence by making the appropriate notifications.

1.4.1.2.2. Providing entry control point management.

1.4.1.2.3. Performing cordon security to support the IC.

1.4.1.2.4. Providing counter-attack to protect mission critical resources. SF commanders must weigh the risk to forces by understanding the protective capabilities of SF IPE and the environment the force will be expected to operate in before committing an assault force. See AFTTP(I) 3-2.46, *Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection*, for information on assessment of NBC filter performance as they relate to protection against selected Toxic Industrial Chemicals.

1.4.2. Natural Disasters.

1.4.2.1. Natural disasters can create emergency conditions that vary widely in scope, urgency and degree of damage and destruction. When planning for natural disasters that could occur on or near the installation plan for the worst-case scenario. Specific natural disasters will differ in scope and effects. Therefore, response, recovery and mitigation actions will vary. A national-level response will be required to help Air Force installations recover from extensive natural disasters.

1.4.2.2. Natural disasters include earthquakes, extreme heat or cold, floods and flash floods, hurricanes or typhoons, landslides and mudflows, thunderstorms and lightning, tornadoes, straight-line winds, cyclones, tsunamis, volcanoes, wild land fires, avalanches, winter storms, and natural outbreaks of disease.

1.4.2.3. Installations use the ICC and EOC for C2 of resources when responding to and recovering from natural disasters. When requested, MAJCOMs may choose to deploy all or part of their DRF to support installations affected by a natural disaster.

1.4.2.4. Commanders must be able to maintain the primary installation mission, save lives, mitigate damage and restore mission-essential resources and infrastructure after a natural disaster.

1.4.2.5. Base the level of response and actions on the magnitude of the disaster and degree of damage.

1.4.3. Conventional attacks (including those using high-yield explosives); and terrorist use of CBRN materials.

1.4.3.1. Recognize attack initiation and protect personnel, weapon systems, and material from weapon effects.

1.4.3.2. Maintain airbase security and physical integrity.

1.5. Special Considerations for Response to HAZMAT or CBRNE incidents. When responding to an emergency situation, Security Forces may accidentally come into contact with a peacetime mishap involving a HAZMAT spill or a terrorist use of Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive (CBRNE) weapons, materials or agents. If responding to a known HAZMAT or CBRNE incident, Security Forces personnel must proceed cautiously to avoid becoming a victim of the incident and follow the directions of trained HAZMAT responders.

1.5.1. Response to Contaminated Incident Site. An initial task within the emergency responder missions is that the IC must establish control of the site to protect first responders and keep out unauthorized personnel. The strategy is to establish three distinct zones: the exclusion zone (Hot Zone), the contamination reduction zone (Warm Zone), and the support zone (Cold Zone). Security Forces primary responsibility during initial response is to establish, in concert with the IC, a cordon, Incident Command Post (ICP), ECP, and Decontamination Corridor (DC). The BDOC/ECC will contact all affected posts and patrols and FES and advise them to proceed to the Cold Zone ICP staging area.

1.5.2. If an incident occurs in a Protection Level (PL) 1-3 resource restricted area, evacuation processes will have to be coordinated through the BDOC/ECC. Prior to evacuating Restricted Areas, ICs must consider the totality of the incident to include threat to life, availability of personal protective equipment and threat to PL 1-3 resources. This decision will be made before evacuating or relieving contaminated Security Forces personnel from their duty positions.

1.5.3. If decontamination is required follow the instructions of the IC and/or FES personnel. The base Fire Chief (FC) will develop local decontamination procedures. The Defense Force Commander (DFC) will work with the base FC to conduct cross functional training and exercise process to determine the best solution for their installation.

1.5.4. Decontamination processes and equipment available will vary dependent on the situation and hazard involved.

1.5.4.1. Security Forces performing day-to-day duties are armed with a variety of weapons ranging from the handgun to heavy machineguns. These items are accountable and require special handling, storage and/or destruction per AFI 31-101, *Integrated Defense*. For more information on weapon decontamination processes, refer to AFMAN 31-229, *USAF Weapons Handling Manual*. **NOTE:** Equipment items that cannot be decontaminated will be destroyed. This includes weapons and ammunition. MAJCOM/A7S will establish procedures for the immediate replacement of contaminated weapons and ammunition once it's determined that they cannot be reissued based on the type of contaminate. See AFMAN 23-220, *Reports of Survey for Air Force Property*, for procedures for accountability of items being destroyed.

1.5.4.2. In a high risk response, Security Forces must work with the FBI and the HAZMAT team to coordinate the collection of evidence. Only those SF members properly trained and equipped to collect contaminated evidence will participate in the handling of any contaminated evidence or material.

1.5.4.2.1. The lead investigative agency may request that evidence is not decontaminated before being bagged. See AFI 31-206, *Security Investigations Program*, for evidence collection.

1.5.4.2.2. The chain of custody of evidence collected at HAZMAT or CBRNE incidents must be part of the preplanning and execution.

1.5.4.3. Security Forces personnel will be medically examined and depending on the situation or symptoms, transported to a Medical Treatment Facility (MTF).

1.6. Special Considerations for Criminal or Terrorist Use of CBRNE. As previously noted, during all response actions, first responders must continually assess the situation and be alert for indicators of terrorist or criminal intent or that the disaster may have been human-caused. If a CBRNE incident is believed to have been human-caused, the following procedures apply.

1.6.1. Security Forces members may likely become victims based on their location at the initiation of the incident or initial response to the incident scene. The decontamination process will be the same as other HAZMAT incidents.

1.6.2. If evidence is found on someone that provides a reasonable belief that they were responsible for the CBRNE incident, immediately apprehend and notify the BDOC/ECC and IC. Example: While going through decontamination a person is found with a bag containing a white powdery substance. Based on the person's nervous behavior and the suspicious powder in the bag the person should be apprehended and the bag set aside as evidence. Decontamination of all personnel should occur prior to leaving the hazard zone.

1.6.2.1. Consideration must be taken on how to transport the suspect to the Decontamination Corridor. The contaminated Security Forces unit will be responsible for the suspect until released to AFOSI or FBI agents to limit further contamination exposure to other Security Forces.

1.6.2.2. When the contaminated Security Forces members are moving or transporting the suspect to the Decontamination Line, Security Forces flight leadership must plan to transfer the suspect, after decontamination, over to a two-person decontaminated Security Forces unit. Continual communication during decontamination and transfer is critical and must be adequately planned for and exercised.

1.6.3. Suspect decontamination and handling procedures.

1.6.3.1. During the decontamination of a suspect, the safety of the first responder at the Decontamination Line must be paramount. Officer safety and emergency responder safety must be foremost in the minds of the Security Forces members. The agency responsible for decontamination must be informed that a possible hostile suspect is being processed.

1.6.3.2. The receiving "clean" unit will handcuff and search the decontaminated suspect as he/she leaves the decontamination area. Handcuffing and searching of the suspect will take place before the suspect is taken to the next stage.

1.6.3.3. Security Forces must coordinate with the lead Federal Investigative Agency (e.g. AFOSI or FBI) as soon as possible; however, the transportation of a suspect who requires medical attention to the nearest medical treatment facility takes priority.

1.6.3.3.1. If no coordination with the lead Federal Investigative Agency can be made, Security Forces will be responsible for maintaining the custody and guarding any suspect transported to medical treatment facilities until properly relieved.

1.6.3.4. The transfer of the suspect to AFOSI or FBI will be properly documented IAW established procedures.

1.7. Exercises. Installations must conduct exercises as outlined in the Integrated Defense Plan (IDP), AT Plan (ATP) and CEMP 10-2. These plans must include functional exercises that allow for coordinated responses between Fire Emergency Services personnel and Security Forces. This will ensure first responders know how to work collaboratively during response to real world and exercise scenarios. To the greatest extent possible, exercise scenarios should be combined to meet the objectives of the installation IDP, ATP, and CEMP 10-2 while avoiding redundancies.

1.8. Legal Considerations.

1.8.1. The provisions of this AFMAN direct Air Force personnel in their responses to high risk incidents. The provisions apply largely to US-based installations. Any operations conducted at an installation overseas may be subject to additional regulations and restrictions depending on the Status of Forces Agreement or other bi-lateral agreements with the host nation.

1.8.2. Any guidance in this AFMAN relating to riot control agents or other less than lethal means do not provide authority to use such non-lethal measures in any area where US forces are engaged in hostilities or contingency operation. Such use of non-lethal munitions is authorized only as directed in the Rules of Engagement for the particular operation or contingency.

1.8.3. Air Force operations in the US must comply with the Posse Commitatus Act, which generally prohibits federal military personnel from conducting law enforcement activities off of a military installation. During some civil disturbance scenarios, and other limited circumstances, federal military forces may be permitted to conduct law enforcement activities. The installation SJA must be consulted before Air Force personnel are employed off of the installation to ensure the manner in which they are being used complies with federal law and regulation.

Chapter 2

COUNTERING THREATS

2.1. Definitions. The following definitions are provided for the purpose of clear communication and to standardize titles and descriptions for operational planning and response purposes.

2.1.1. Insider Threat. The DoD defines an Insider Threat as “A disaffected individual(s) within the force motivated to do violence against the force and the nation.”

2.1.2. Active Shooter. The DHS defines an Active Shooter as “An individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims.”

2.1.3. Suspicious Activity. The DoD defines Suspicious Activity as “Observed behavior that may be indicative of intelligence gathering or other preoperational planning related to a terrorist or other security threat to DoD interests worldwide.” There are thirteen categories of suspicious activity. These categories are clearly defined and can be found in Attachment 2.

2.1.4. Radicalization. The DHS defines Radicalization as “The process of adopting an extremist belief system; including the willingness to use, support, or facilitate violence as a method to effect societal change.”

2.1.5. Workplace Violence. The Occupational Safety and Health Association (OSHA) defines Workplace Violence as “Any physical assault, threatening behavior, or verbal abuse occurring in the work setting.”

2.1.6. School Violence. The Center for Disease Control (CDC) defines School violence “as a subset of youth violence, which refers to harmful behaviors that may start early and continue into young adulthood... It includes bullying, slapping, punching, weapon use, and rape. The young person can be a victim, an offender, or a witness to the violence-or a combination of these”.

2.2. Prevention. Prevention starts with the ability to detect potential threats. Numerous documented case studies exist that indicated trends of behavior demonstrated prior to violent actions taken by an Active Shooter or other insider threats. Attachment 3 standardizes these indicators and facilitates training, detection, and reporting. These indicators are specific actions, behaviors, or activities that correlate to the thirteen categories of suspicious activity and may indicate an individual’s propensity for violence. Additionally, this list of indicators incorporates indicators of workplace violence. It is imperative that the DFC, ATO or S2 educate the base populace on these indicators through awareness briefings and effective community policing, crime prevention and workplace violence prevention programs.

2.2.1. All reporting and response actions will be based on specific observed behaviors and other indicators of possible threats (not because of someone’s race, ethnicity or religion).

2.2.2. The people most likely to recognize potential threat indicators are friends, coworkers, and supervisors. The DFC, ATO, and S2 are charged with educating the base populace and enabling airmen to report individuals exhibiting behavioral indicators that are possibly

indicative of violence, terrorist, or criminal activity. Educating our personnel to refer these individuals for additional law enforcement intervention or assistance enhances the overall integrated defense posture of an installation.

2.3. Reporting. Prevention through education and detection is critical, but proper reporting of observed behaviors that may be indicative of violence, terrorist, or criminal activity enables law enforcement officials to properly investigate and take appropriate action. As part of base populace awareness training, the DFC, ATO, or S2 must educate the base populace on how to properly report suspicious activity or behavior through appropriate law enforcement reporting channels.

2.3.1. eGuardian. eGuardian has been designated as the system of record for all DoD law enforcement agencies/activities. Security Forces shall coordinate with their local AFOSI detachment to use the eGuardian system for reporting, storing, and sharing unclassified Suspicious Activity Reports (SAR) dealing with information regarding a potential threat or suspicious activity related to DoD personnel, facilities, or forces in transit.

2.3.1.1. No entry may be made in eGuardian based on a person's ethnicity, race, religion, or lawful exercise of rights or privileges guaranteed by the law, unless reasonable suspicion exists of a direct relationship between such information and a specific criminal act or behavior that may pose a threat to DoD personnel, facilities, and forces in transit.

2.3.1.2. The following specific categories of information are not permitted to be entered into eGuardian: classified information; information that divulges sensitive methods and techniques; information derived in accordance with chapter 36 of title 50, U.S.C., also known as "The Foreign Intelligence Surveillance Act" (Reference (t)); grand jury information; Federal taxpayer information; sealed indictments; sealed court proceedings; confidential human source and witness information; and any other information of which the dissemination is prohibited by law.

2.3.1.3. The collection and retention of information on US citizens by non-intelligence units within the Department of Defense is regulated and must comply with Department of Defense Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*.

2.4. Workplace Violence. At each installation, the key to identifying and preventing workplace violence is to place emphasis on engaging the individual's leadership and/or contacting Security Forces or AFOSI regarding any concerns involving potential criminal conduct. Security Forces is a key player in the Workplace Violence Program and the DFC must coordinate on any installation plans concerning this program.

2.4.1. Planning. Successful workplace violence prevention programs are based on a strong policy against violent behavior combined with effective training on understanding indicators of violence and properly reporting concerns to the appropriate agency. AFI 44-154, *Suicide and Violence Prevention, Education, and Training*, establishes policy and mandatory training requirements for USAF personnel on detecting/reporting indicators of workplace violence.

2.4.1.1. Per AFI 44-154 unit commanders will ensure all personnel complete a mandatory suicide prevention and violence awareness education program.

2.4.1.2. Completion of the suicide prevention and violence awareness education program training will be documented, and a tracking mechanism developed to ensure training is accomplished.

2.4.1.3. When an individual demonstrates indicators, unit leadership must be made aware to facilitate the appropriate response and support for the individual and the potential target to prevent further escalation of the situation.

2.4.1.4. If Security Forces is contacted about personnel demonstrating indicators of potential workplace violence, Mental Health professionals and the individual's unit leadership must be notified.

2.4.2. Response. If prevention fails, Security Forces must develop procedures for responding to and resolving incidents of violence. A plan specific to workplace violence should be included in the IDP as an attachment. Additional information concerning workplace violence is available from the Office of Personnel Management at the following website: http://www.opm.gov/employment_and_benefits/worklife/officialdocuments/handbooksguides/WorkplaceViolence/index.asp.

2.4.3. Resiliency. The TSR team will provide TSR services to enhance resilience to potentially traumatic events.

2.4.4. Exercises. Installations should conduct an exercise that addresses response to an incident of workplace violence annually. Tabletop exercises are sufficient for exercising the partnership with local first responder agencies, but should not be used more than two years in a row to meet participation needs. Exercising the resiliency component of high-risk incidents is a critical part of assessing readiness. Exercises may be conducted in conjunction with other annual exercise requirements. Lesson Learned from these exercises should be thoroughly documented and reviewed and uploaded to the Air Force – Joint Lessons Learned Information System (AF-JLLIS) at <https://www.jllis.mil/USAF>.

2.5. School Violence. In recent years, there have been several incidents of violence in schools throughout the United States. Although incidents of this nature are rare, many Air Force installations have either DoD or locally sponsored schools on the installation. As a result, installation commanders must ensure proper planning and exercises are conducted. Close coordination between base and school officials is essential to successfully concluding any school-related incidents.

2.5.1. Planning. Security Forces must coordinate with school officials and become familiar with school policies concerning incidents on school grounds at their installation. Each school district has different policies and actions required based on incidents. If an installation school has no policies in force, base officials, including Security Forces, should assist them in establishing security and lock down procedures. Security Forces should inform school officials on their response capabilities and procedures as well, so all parties involved are comfortable with processes involved in response to school violence. MOAs must be maintained to address procedures; all procedures will be codified in the IDP.

2.5.1.1. Jurisdiction. Local SJAs provide advice on the implications of installation jurisdictional requirements for schools located on Air Force installations. Jurisdictional requirements will necessitate different and varying responses by Security Forces and could require support from local Law Enforcement Agencies (LEA).

2.5.1.2. Diagrams and Maps. Security Forces will have maps of school facilities and grounds immediately available to assist in responses to violence.

2.5.1.3. Cordons. Security Forces and Fire Emergency Services will predetermine cordons for response to eliminate confusion that may occur upon notification of an incident at an installation school. Upon actual response to an incident, the cordon may be adjusted to accommodate specific threats.

2.5.1.4. Encourage the use of Security Forces personnel that are already assigned duties as instructors at the schools [e.g. Drug Abuse Resistance and Education (DARE) instructors] to coordinate and exercise plans. These personnel already have a rapport with the children and they are familiar with the layout of the school.

2.5.1.5. Coordinate with school officials (school liaison officer) for periodic walkthroughs with an MWD to familiarize the canine and handlers with school facilities. This also acquaints the faculty and students with this process.

2.5.1.6. Security Forces will coordinate with school officials prior to utilizing school facilities for training. Active school facilities are best used during periods when school is not in session (weekends, spring breaks, holidays, etc.). School officials have the final say as to how their facilities are utilized.

2.5.2. Reporting and Response. School officials should immediately lock down the school and notify Security Forces for immediate response to school incidents. The lock down process is necessary to ensure the safety of their students and accountability of students and personnel. School officials should report school violence incidents using the installation's emergency response telephone numbers or alarms, when available. Upon arrival, Security Forces must immediately contain the situation and enclose the scene. Attempt to obtain information on the subject's location and accountability of all students and faculty.

2.5.3. Media. Media interest at scenes of school violence will be high. Ensure PA is immediately involved in establishing a media reception plan and media center to assist with information flow.

2.5.4. Parents. As mentioned earlier, parental requirements at the scene will be challenging. The EOC Director and IC should select and establish an area for parents to respond to and receive information. PA is responsible for all information flow; however, Airman and Family Readiness Center, chaplains and medical personnel can assist with this. Give parents appropriate information for the situation.

2.5.5. Resiliency. The TSR team will provide TSR services to enhance resilience to potentially traumatic events.

2.5.6. Exercises. Installations that have on base schools, will conduct an exercise at least annually to bring all tasked agencies together to practice responding to a violent incident in a base school. It is recommended that an exercise occur during the school year so teachers and students can get involved as well. Exercising the resiliency component of high-risk incidents is a critical part of assessing readiness. Exercises may be conducted in conjunction with other annual exercise requirements. Lesson Learned from these exercises should be thoroughly documented and reviewed and uploaded to the Air Force – Joint Lessons Learned Information System (AF-JLLIS) at <https://www.jllis.mil/USAF>.

2.6. Active Shooter. Active shooter incidents are incredibly dangerous and difficult because there is no criminal objective (robbery, hostage taking) involved other than violence. Often, the shooter has no regard for their life, and may be planning to die. These factors leave Security Forces no other recourse but to locate and stop the shooter as quickly as possible. As a result, installation commanders must ensure proper planning and exercises are conducted. Close coordination between all tasked agencies and the base populace is essential to mitigate the threat and minimize the loss of life in an Active Shooter incident.

2.6.1. Planning. These types of incidents require preplanning and preparation in order to conclude the incident as quickly and as safely as possible. There are many tasks that can be considered but the following actions, at a minimum, must occur or be planned for immediately:

2.6.1.1. Base Populace Education. In addition to awareness training on behavioral indicators as described in paragraph 2.2 and Attachment 3, the DFC, ATO, and S2 must ensure the base populace knows what actions to take upon notification that an Active Shooter incident is occurring at their location or elsewhere on base. This awareness training should be developed locally and contain a brief historical review of past incidents, but primarily focus on what actions airmen and civilians should take to protect themselves and assist responding forces. Special care should be taken to not divulge specific tactics, techniques, or procedures of responding forces.

2.6.1.2. Each installation must develop and maintain an operational plan for response to active shooter incidents. This installation plan may be an element within an existing plan, such as the IDP, AT Plan or the CEMP 10-2, or a separate plan, as directed by the installation commander. These plans must incorporate all first responder agencies, to include off-base support, and be as detailed as possible to reduce the amount of time necessary to react, as response time is very crucial in this type of incident.

2.6.1.3. Large Venues/Gathering Areas. Security Forces units must coordinate closely with owner/operators of large occupancy venues on the installation to become familiarized with those locations, both internally and externally.

2.6.1.4. Arming Considerations. Security Forces goal is to always maintain superior fire power during response to high-risk incidents. If possible, every patrolman entering the building should possess an additional weapon, such as a rifle, carbine, or shotgun, to provide additional range capability to engage an Active Shooter. Do not delay response waiting for additional weapons; the primary focus remains on locating and stopping the Active Shooter as quickly as possible.

2.6.1.5. Law Enforcement Training. To ensure standardization of Active Shooter training, unit-level trainers will utilize the Active Shooter curriculum located in the Electronic Tactics, Techniques, & Procedures Guides (eTTPGs) Library located on the Air Force Security Forces Center website. The library is at <https://afsmil.lackland.af.mil>, on the left column, click 'eTTPGs'.

2.6.1.6. Equipment Considerations. Equipment availability must be considered and include:

2.6.1.6.1. Concealable body armor. Concealable body armor should be a matter of routine use by all law enforcement and security patrols, as indicated by AFI 31-101,

Integrated Defense. In an active shooter event, heavier armor such as an Improved Outer Tactical Vest (IOTV) with ceramic plates carried in the patrol vehicle could provide a tactical advantage to the entry team. The responding patrol is required to stop the threat immediately and donning additional armor shall not take more than a 1 to 2 minutes

2.6.1.6.2. Flashlights. Electrical power could be disrupted, possibly intentionally by either the suspect or the responders, during the incident. Security Forces units are highly recommended to incorporate into training the use/handling of a flashlight and a weapon simultaneously.

2.6.1.6.3. Breaching equipment. This kind of equipment may be needed to force entry to a secure building. These tools include a ballistic shield, single-person door ram, Halligan tool, and bolt cutters. These tools should be contained in a man-portable backpack so they can be carried by any of the responding teams. Each Security Forces member should undergo thorough familiarization training on the employment of these tools.

2.6.1.6.4. In addition to Security Forces standardized duty gear, consideration should be given to add individual first aid kits (IFAK), felt tip markers, portable litters, and Meals-Ready-to-Eat (MRE) or energy bars to Security Forces A-bags.

2.6.2. Response. The primary goal of Security Forces in response to an Active Shooter incident is to eliminate the threat and minimize the loss of life. Each Security Forces member must realize that the speed of their response will minimize casualties, but will likely not prevent all loss of life. Unless otherwise directed by Base Defense Operations Center (BDOC) or the Flight Sergeant, the Security Forces member must take immediate action to eliminate any active threat to human life.

2.6.2.1. Security Forces need to have an accurate understanding of the tactical situation, and a working plan to confront it. Because there is little time to develop an extensive plan at the scene, patrolmen should mentally prepare and build an action plan in advance. All actions should be in accordance with AFI 31-207, *Arming and Use of Force by Air Force Personnel*.

2.6.2.1.1. Notify BDOC immediately of what teams are entering, what avenues of approach are used, and their associated armament and equipment.

2.6.2.1.2. Upon arriving, if there is an active shooting in progress, do not verbalize your intent to use force if it endangers yourself or others. Use lethal force IAW AFI 31-207.

2.6.2.1.3. If the suspect manages to barricade himself/herself in a manner that limits physical/visual contact and is no longer an active threat, initiate EST or civilian Special Reaction Team (SRT) response. Refer to Chapter 3 for specific guidance in handling a barricaded subject.

2.6.2.2. The scene will be loud and chaotic. Terrified victims may be able to direct you to the shooter and the sound of shooting may also assist in locating the shooter. The shooter will be highly focused on violence.

2.6.2.3. A Security Forces member can use the chaos and the shooter's diverted focus as cover to move quietly to a position of advantage.

2.6.2.4. Incident Command. The initial incident command will come from the senior Security Forces member on-scene until transferred to a certified/trained IC and the AFIMS Incident Command System is established. At that time, the senior Security Forces member on scene will assume the role of Operations Section Chief (OpsSC), as outlined in AFMAN 10-2502, until properly relieved by higher Security Forces authority. The IC will retain overall management of the entire incident and supporting functions.

2.6.2.4.1. The IC must establish a safe staging area for follow-on forces to include FES, Emergency Medical Technicians (EMTs), and other on and off-base tasked agencies.

2.6.2.4.2. The IC should have a pre-established code word that all responding units will use if they locate an improvised explosive device (IED) or other deliberately placed hazard at the incident scene. This code word must be incorporated into pre-planning and exercises.

2.6.2.5. OpsSC Responsibilities. The OpsSC is responsible for the tactical operations at the incident, to include knowing the number of responding patrols at the scene, team compositions, roles and armament, team locations in facility/building, and up-to-date suspect actions to brief follow-on forces and the IC. The senior on-scene Security Forces representative will request assistance through the IC such as additional personnel, obtaining affected facility schematics to properly track and coordinate the various teams entering the building, or any other resources needed to mitigate the incident. This information, plus other critical data, must be transmitted to and documented by BDOC, ECC and/or EOC accordingly.

2.6.2.5.1. The OpsSC will coordinate through the IC a methodical and efficient plan to clear the building or scene after any immediate threat is terminated. This is necessary to ensure there are no IED or additional subjects prior to allowing emergency responders in to tend to casualties.

2.6.2.5.2. Consider tracking evacuated personnel by their original location at the incident scene. While not the primary focus, this will enable crime scene reconstruction and assist investigators.

2.6.2.6. Team Composition/Additional Support. If the threat cannot be stopped by the initial responding patrol(s), try to isolate and contain it, and await backup. Backup/support should come in the form of specialized teams that have been specifically trained (see para 4.6.1.5.) in the role of Entry Team, Contact Team, and Search/Rescue Team. These teams should deploy in a manner that gets them to the shooter quickly, and offers a tactical advantage. The following is a brief synopsis of each team's capability and role:

2.6.2.6.1. Entry Team. The primary role of the Entry Team is to immediately locate and eliminate the threat and minimize the loss of life. All Security Forces personnel should be trained to perform the role of Entry Team.

2.6.2.6.2. Contact Team. The Contact Team's role is to limit the shooters movement, prevent escape, communicate status to the OpsSC and/or IC, provide preliminary assessment (dynamic intelligence), give victim locations and medical needs if time permits, report explosives types and locations, offer descriptions and locations of suspects, describe the shooter(s) weapons, and apprehend the suspect(s) if capable.

2.6.2.6.3. Search/Rescue Team. The Search/Rescue Team's role is to recover casualties by entering or approaching danger areas to locate victims, extract victims to a safe area and relay medical information to the OpsSC, who will relay to the IC and medical personnel. Prior to entry, the team must know where to direct the uninjured and ambulatory (who can walk or run) in order to send them to a safe area. In the case of multiple victims, the search/rescue team(s) may need to be expanded or multiplied. Methodical control of the area around them must be emphasized by the search/rescue team and a system of identifying and accounting for victims must be put in place.

2.6.2.7. Crime Scene Preservation. Once the incident site is secured, it and the surrounding area becomes a crime scene. All first responders, including Fire and/or Medical personnel, and all other individuals will have to be cleared by the IC before entry into the secured incident site. Legal jurisdiction and any agreements with outside law enforcement agencies will determine who has the responsibility to collect and store evidence and which agency will take the lead investigative role. Contact the base SJA for guidance. An active shooter incident will most likely include the formation of a Law Enforcement Joint Operations Center (JOC) to integrate/house the multiple law enforcement agencies involved in the investigation. The Air Force Office of Special Investigations (AFOSI) SAIC (Special Agent in Charge) or the DFC will most likely be the primary liaison within the JOC. At the scene, Security Forces will play an important role in maintaining the installation mission of protecting Air Force property, resources, and personnel.

2.6.3. Jurisdiction. Local SJAs provide advice on evidence collection and the implications of jurisdictional requirements for facilities and open areas located on Air Force installations. Jurisdictional requirements will necessitate different and varied responses by Security Forces and other assisting law enforcement agencies.

2.6.4. Media. Media interest at scenes of an active shooter incident will be high. The IC, through PA, is responsible for all public information flow. The Installation Commander or IC must ensure the PA Officer is a key player in exercises and training, and in the event of an actual incident, is immediately involved in establishing a media reception plan and media center to assist with information flow.

2.6.5. Families. The EOC Director, through the Airman and Family Readiness Center (A&FRC) should establish an area for families to gather at to receive information and consult with Chaplains and other family support personnel. Like other agencies, the A&FRC must be included in all installation planning efforts to ensure their rapid and efficient response to an actual event. NOTE: This is a traumatic event for all involved. Lessons Learned have demonstrated the need to cordon the affected area to prevent emotional family members and friends from attempting to enter the incident scene.

2.6.6. Resiliency. Following an Active Shooter incident, it is essential that all Security Forces members and Emergency Responders have access to a TSR Team. The installation TSR Team should have Security Forces personnel assigned to it to provide responding Security Forces incident personnel with peer support.

2.6.7. Exercises. Installations must conduct Active Shooter exercises annually IAW AFI 10-2501. Exercising the resiliency component of high-risk incidents is a critical part of assessing readiness. Exercises may be conducted in conjunction with other annual exercise requirements. Lesson Learned from these exercises should be thoroughly documented and reviewed and uploaded to the Air Force – Joint Lessons Learned Information System (AF-JLLIS) at <https://www.jllis.mil/USAF>.

Chapter 3

BARRICADED SUBJECTS

3.1. Initial Response. In high-risk situations that do not involve an Active Shooter, it is important that Security Forces immediately contain or enclose the scene. On-duty Security Forces personnel are likely to be the initial response element on scene. The first arriving unit will establish command and control and assume the role of initial IC and initiate the Incident Command System. The IC will maintain control of the situation until properly relieved of command by a senior official/competent authority, based on parameters of the incident. Some barricaded suspect cases involve hostage taking. Information regarding hostage situations is described in further detail in [Chapter 5](#).

3.1.1. Responding units must keep the BDOC/ECC informed of the following:

3.1.1.1. Arrival on scene.

3.1.1.2. Position.

3.1.1.3. Safe avenues of approach for other responding units.

3.1.1.4. Status of the situation.

3.1.2. To reduce risk, the patrolmen should take a covered position where they can best see what is happening while preventing the suspect from escaping. Immediately evacuate all nonessential personnel far enough away so they are in no danger of being taken hostage or hit by a suspect's fire. Do not allow volunteers or family members to start or become involved in any negotiations.

3.2. Containment of the Scene.

3.2.1. Establish a cordon. The initial IC will direct the establishment of a 360-degree cordon at the scene of a barricaded subject. This cordon will be established and maintained by Security Forces, or designated augmentation forces, until the IC determines there is no longer a need. The senior Security Forces member on scene does this by assigning Security Forces personnel to establish inner and outer perimeters. How far these perimeters are established from the scene depends on the scope, complexity, and location of the incident.

3.2.1.1. Outer perimeter. The outer perimeter is established to prevent people from interfering with recovery operations and to keep innocent bystanders and onlookers from being hurt. This perimeter should be established outside the maximum effective range of any weapons the barricaded subject has, if Security Forces members can establish the type/caliber of the weapon(s) involved. Direct all vehicles and pedestrians not involved in response and recovery operations away from the threat area. Set up an ECP along the outer perimeter in an area that is easily accessible to responding units. Send all personnel who need to enter the area to the ECP.

3.2.1.2. Inner perimeter. Security Forces personnel normally establish the inner perimeter to contain the immediate scene. The Emergency Services Team (EST), if available, may replace on-duty Security Forces personnel posted on the inner perimeter if deemed appropriate for use by the OpsSC and IC. Guidance governing establishing, training, and utilizing EST can be found in Chapter 6. Security Forces can adjust the

inner perimeter as needed. Due to the dangers involved, strict control of the area must be maintained. Only key personnel, such as EST, negotiation teams, and the senior representatives from Security Forces, Fire Emergency Services, and Emergency Medical Services, are allowed within the inner perimeter and only at the direction of the IC. Security Forces, or EST if available, is responsible for searching and clearing the inner perimeter. At this point, the installation commander could choose to have the lead agency assume control of the situation.

3.3. Establishing Jurisdiction and Command and Control.

3.3.1. Role of Local Civilian Law Enforcement. The specific roles of state and local LEAs must be part of pre-incident planning. The type of jurisdiction (exclusive, partial, concurrent or proprietary) will dictate civil and military roles. Coordinate with the installation staff judge advocate prior to employment of off base law enforcement.

3.3.1.1. Exclusive or Partial jurisdiction. For installations or portions of installations under exclusive federal jurisdiction, the state and local LEAs have no jurisdiction or authority, though they may seek or be asked to assist with security precautions and other duties consistent with their respective interests (e.g., off-installation traffic control, sealing the area).

3.3.1.2. Concurrent or proprietary jurisdiction. If an incident occurs in an area of concurrent or proprietary jurisdiction, the status of the state and local LEAs is clearer, but roles in responding to the incident remain uncertain and must be clearly defined in plans. The installation commander exercises broad and ultimate authority to maintain law and order on the installation, notwithstanding concurrent state jurisdiction. The installation commander may also deny entry to or remove from the installation anyone who poses a threat to good order and discipline. It is recommended that the installation commander pursue memorandums of agreement (MOA) with local civilian law enforcement agencies to define response strategies and division of responsibilities (Attachment 4). These agreements must be exercised to validate their effectiveness and ensure the safety of the installation's personnel and resources.

3.4. Negotiations. The principle method for peacefully resolving a high-risk situation is through the use of a negotiator. Each installation must have the services of a trained negotiator available. Negotiators may be drawn from trained Security Forces, AFOSI, FBI, local civilian LEAs, or even medical professionals. The source for the negotiator is determined by the resources available in any given area and may be influenced by the incident itself. The source for the negotiator capability must be determined in advance and available 24 hours a day for immediate recall. A combination of sources may be used, i.e., AFOSI and Security Forces. For further information concerning crisis negotiation, refer to Chapter 5.

Chapter 4

DOMESTIC VIOLENCE AND ABUSE RESPONSE

4.1. Domestic Violence. Security Forces personnel must be prepared to encounter potentially hostile incidents of domestic violence. Security Forces need to know how to diffuse these incidents and regain control of the situation. Each year law enforcement personnel, including Security Forces, are injured or killed responding to family violence calls.

4.1.1. Studies have shown that family violence calls are often repeat calls. When the initial call is not effectively handled, it is likely the situation will reoccur and the patrolmen will be called again. By learning how to recognize child abuse/neglect and spouse abuse and by acquiring the skills necessary to act accordingly, Security Forces personnel can:

4.1.1.1. Reduce the likelihood of injury to the family member.

4.1.1.2. Provide protection to victims of family violence.

4.1.1.3. Avoid repeat calls.

4.1.2. Security Forces personnel have a critical role to play in restoring order and preventing future incidents of family violence. They are trained to respond in an emergency and have transportation and communication equipment immediately available. Security Forces also have the authority to intervene and, if necessary, to detain or apprehend.

4.2. Security Forces Role in Domestic Violence. One of the missions of Security Forces is to maintain law and order. To reestablish order and preserve the peace, Security Forces personnel are required to respond to situations of domestic violence. The primary role in these situations is to take immediate action to restore order and protect lives. In addition, the sponsor's unit commander, first sergeant and the base family advocacy officer must be advised of all incidents of family violence. AFOSI is responsible for investigating major offenses, including child abuse and spousal abuse involving aggravated assault. The local AFOSI detachment must be notified immediately of all child abuse or neglect allegations to assist in determining who the investigating authority is. Security Forces routinely investigate minor incidents of child abuse/neglect and spousal abuse. Incidents should be recorded on AF Form 3545, *Incident Report*, and AF IMT 53, *Security Forces Desk Blotter*. When peace has been restored and the appropriate authorities have been notified of the incident, the Security Forces member's role has ended, except where an offense has been committed and an apprehension will take place.

4.2.1. Attitude of Responding Security Forces. The attitude of the responding Security Forces personnel, in many cases, will determine the attitude and cooperation of the family members involved. Realize that people may be hostile or angry, frightened or abusive, ashamed or uncooperative and they may view Security Forces personnel as intruders and resent their presence. The Security Forces member's approach should be calm, controlled and concerned. Care should be taken to avoid sarcastic or critical remarks, an impolite tone of voice or threatening or aggressive body positions. Hostility, indifference or aggression may provoke further violence while a sensitive and tactful approach may restore order and calm the situation.

4.2.2. Best Approach. In responding to a call, keep in mind that each situation is different and must be treated individually. Meanings and attitudes might be read into words, facial

expression and body positions. The best approach is a calm and positive one. Responses involving ongoing violent action or other aggressive actions by a suspect may require a more proactive and forceful response.

4.3. Unit Commander's Role in Domestic Violence. Unit commanders are responsible for the actions of assigned personnel, both on and off duty. This responsibility includes the behavior of both military sponsors and their military dependents. Security Forces personnel should recognize this command responsibility and duty to inform the commander of incidents of family violence involving their assigned unit personnel and their family members.

4.4. Family Advocacy Officer's Role in Domestic Violence. The Family Advocacy Officer functions as the central coordinator for the base Family Advocacy Program. Under the direction of the director of base medical services or chief of hospital services, the Family Advocacy Officer performs a number of family violence prevention and intervention services. For more information on family advocacy see AFI 40-301, *Family Advocacy*.

4.5. BDOC/ECC Controller's Role in Domestic Violence. In answering family violence calls, controllers must have all available information on the families and situations. The controller has the responsibility for obtaining as much information as possible from the individual making the call while dispatching a patrol unit. When a call is received indicating the possibility that family violence has occurred or is occurring, the controller will:

4.5.1. Obtain as much data as possible from the caller by asking who the involved parties are, what has happened, if the altercation is not currently ongoing when did it occur, where did it happen, where are the involved parties now, how the incident occurred, whether weapons were involved or available, and if medical aid is required.

4.5.2. Asks the caller for the telephone number from which the call is being made. This enables the controller to call the number back to check the validity of the call and determine whether the situation has changed prior to the arrival of responding Security Forces patrols.

4.5.3. Relay information to Security Forces responding to the situation. If the controller is unable to obtain a clear description of the situation, the responding unit(s) must be informed.

4.5.4. Check AF Form 1314, *Firearms Registration*, roster or local firearms roster/database.

4.5.5. Ensure that an appropriate patrol response has taken place, the controller will also ensure follow-up actions and referrals to unit commanders through first sergeants, family advocacy officer, and/or AFOSI has occurred. In cases where the reported abuse is not currently ongoing, a patrol response may not be appropriate. In these instances, coordination between the controller and their supervisory chain of command, the unit commander of the military member involved, AFOSI and the family advocacy officer will determine the appropriate response. If the incident has already occurred and is not currently in progress, it may be more appropriate to dispatch a Security Forces Investigator or AFOSI to the incident to investigate in accordance with AFI 31-206.

4.5.6. Contact AFOSI immediately to meet the dispatched patrol when notified by the base hospital that a victim of a suspected child abuse incident is being treated.

4.6. Patrol Response.

4.6.1. Arriving Safely. The responding patrol(s) must drive to the scene as quickly and safely as possible. Patrols must comply with the standards set forth in AFI 31-201, Attachment 2, *USAF Security Forces Model Vehicle Operation Policy*.

4.6.1.1. The responding patrol should formulate a plan before arrival to include determining in advance who will be in charge, who will approach first, who will serve as backup, etc.

4.6.1.2. Use discretion when approaching a house where a domestic disturbance is occurring. Park Security Forces vehicles at least one (1) house away from the address of the incident. Parking directly in front of the house in question may escalate the situation or warn residents to conceal evidence of a crime. For the same reasons, flashing lights and sirens should be turned off at least one block before arrival and there should be no loud noises like slamming car doors or blaring radio communications.

4.6.2. Approaching the Scene. Security Forces personnel must use caution when approaching the house of a domestic violence complaint.

4.6.2.1. Before approaching the house, Security Forces personnel should stop and listen. Windows, doors, adjoining buildings or areas of possible concealment should be visually checked for unusual movements or objects.

4.6.2.2. Security Forces must exercise caution if they decide to approach from the side or back door instead of the front door, as they could be mistaken for prowlers and escalate a situation.

4.6.2.3. If the approach is made at night and flashlights are used, they should not be shined in windows. Avoid silhouetting other patrols; light discipline is essential.

4.6.3. Entry Procedures. Security Forces personnel should always be dispatched in pairs to domestic violence calls and should always stand to one side of the door, never in front of it. The second Security Forces member should be behind and to one side of the first, in position to maintain visual contact with the inside of the residence and provide cover.

4.6.3.1. Before knocking, pause and listen at the door. Security Forces personnel may be able to obtain information on the nature of the disturbance and whether or not it is violent before announcing their presence.

4.6.3.2. Check screen doors before knocking to see whether they are locked. Locked screen doors can create an unexpected barrier between the Security Forces member and residents if immediate action is required.

4.6.3.3. Knock on the door in a calm non-aggressive manner or use the doorbell, ringing only once each time. When knocking on the door, do not stand directly in front of the door. It creates the “fatal funnel” effect and may put the Security Forces member at a disadvantage.

4.6.3.4. Evaluate the risk of entry, even when invited to enter, and respond accordingly.

4.6.3.5. If there is no response at the door and the dwelling appears quiet, the address should be verified with the BDOC/ECC controller. If the address is correct, the sides and

rear of the quarters should be checked for indications of the presence of the occupants. Neighbors may also provide useful information.

4.6.4. Initial Contact with Residents. Depending on the situation Security Forces personnel should display a calm, positive and helpful manner. Initial impressions will set the tone for the interview.

4.6.4.1. When someone answers the door, Security Forces personnel should introduce and identify themselves and state the reason for their presence.

4.6.4.2. If not invited into the dwelling, Security Forces personnel should request to move the discussion inside. This will remove the situation from the view of the neighbors and enable observation of:

4.6.4.2.1. Any injuries requiring treatment;

4.6.4.2.2. Location and number of the disputants;

4.6.4.2.3. Visible weapons and threatening moves;

4.6.4.2.4. Living conditions;

4.6.4.2.5. Emotional stage of dispute and emotional condition of disputants;

4.6.4.2.6. Impairment;

4.6.4.2.7. Children at risk;

4.6.4.2.8. Physical damage to property.

4.6.4.3. Separate the disputants as necessary and maintain visual contact with the other Security Force members. If possible, keep disputants away from rooms and items that can be dangerous to themselves or Security Forces members.

4.6.4.4. After providing for any necessary medical assistance and calming the situation, obtain information on the family structure and background. Such information will give important background and allow a "cooling off" period. Questions asked may include:

4.6.4.4.1. Names and whereabouts of the sponsor and family members;

4.6.4.4.2. Sponsor's rank, (and any other military member's) social security number and unit;

4.6.4.4.3. Relationship and legal status of residents: i.e., nephew, uncle, boyfriend, girlfriend, valid marriage, for example;

4.6.4.4.4. Length of residence in quarters and period assigned to installation;

4.6.4.4.5. Ages and relationships of children;

4.6.4.4.6. Whether military or civilian police have been required to respond to previous incidents;

4.6.4.4.7. Whether the family has been to family advocacy office.

4.6.5. Visual Observation. Observing conditions inside the quarters while obtaining background information may give ideas of the cause contributing to the situation. The behavior of residents can provide important clues.

4.6.5.1. Signs of fear, hate, depression and embarrassment can be detected in facial expressions, eye movements and body positions.

4.6.5.2. Be alert for sudden movements and continual glances at closed doors, closets or bureaus. Such actions may be the first indication the individual has a weapon available or is attempting to conceal the presence of an injured family member or other evidence.

4.6.5.3. The condition of the home and appearance of the residents may provide clues to family functioning. If the living conditions are unusual, unsafe or unhealthy, Security Forces members may want to arrange for photographs of the scene and request response of the military member's first sergeant or commander.

4.7. Differentiating Types of Disputes.

4.7.1. Violent Disputes. When responding to a violent disturbance, Security Forces personnel must immediately separate the disputants. If personnel being interviewed are a suspect/subject ensure you read them their rights IAW Article 31, Uniform Code of Military Justice (UCMJ) or the 5th Amendment United States Constitution. If medical attention is required, it should be secured at once. AFOSI must be contacted if the assault resulted in serious injuries.

4.7.1.1. Security Forces personnel must be vigilant about their personal safety as well as that of disputants. In separating the persons involved, make a visual search for objects that could be used as weapons. The disputants should never be allowed to come between the Security Forces members. Disputants should never be left alone in another room and should not be moved to the kitchen because of the availability of potential weapons. If the disputants cannot be calmed, apprehension and removal to the BDOC may be necessary. CAUTION: The victim may become hostile or violent when a spouse or family member is apprehended, detained, or physically restrained.

4.7.1.2. Alcohol is involved to some extent in many situations of domestic violence. Intoxicated people tend to be violent in disputes making it difficult to reason with them or obtain factual information from them. The individual may have to be removed from the scene until sober enough to be effectively interviewed.

4.7.1.3. A potential danger exists in persons who are unusually quiet and controlled in highly emotional disputes. Such people may be near the breaking point and may become violent and upset by an innocent gesture or remark.

4.7.1.4. During violent disputes, it may be beneficial to separate the parties out of sight from each other. Only do this if it does not put Security Forces personnel or other innocent bystanders at increased risk. Once they are separated and order is restored, the parties may be interviewed.

4.7.2. Verbal Disputes. The difference between violent disputes and verbal disputes is that in a verbal dispute, a physical assault has not occurred. The parties involved may be easier to reason with and a prompt resolution to the dispute is more likely.

4.7.2.1. Remove the disputants to separate rooms if possible. Avoid leaving them alone or in the kitchen or other areas that may provide them access to weapons.

4.7.2.2. Separating normally causes a distraction to the disputants. If Security Forces personnel use a calm, firm and assured tone of voice, it may further distract the disputants

and better control the situation. Once they are separated and order is restored, the parties may be interviewed.

4.7.3. Disputes Involving Children. In disputes where one disputant is a child or young adult, there may be a feeling in the youth of resentment against authority figures. The youth may assume that Security Forces will automatically side with the parents. Therefore, when answering such a disturbance call, an attitude of concern and understanding for the child's version of the argument is important. The youth's feelings, problems and thoughts should be listened to and evaluated as carefully as those of the parents or other disputants. However, take care not to interfere with parental rights regarding the children. If other children are present, but not involved in the dispute, ask parents to remove them from the room.

4.8. Conducting the Interview.

4.8.1. The purpose of the interview is to:

- 4.8.1.1. Assess the immediate danger to family members and need for medical assistance or protective custody;
- 4.8.1.2. Determine whether suspected abuse or neglect is occurring or has occurred;
- 4.8.1.3. Determine the appropriate response to the situation;
- 4.8.1.4. Identify the perpetrator if possible;
- 4.8.1.5. Protect the legal rights of suspects;
- 4.8.1.6. Identify victims and give them proper assistance.

4.8.2. Gathering Information. Separate personnel and conduct interviews. Each person should be interviewed. If personnel being interviewed could be a suspect/subject, ensure you read them their rights IAW Article 31 of the UCMJ for military members or the 5th Amendment U.S. Constitution for civilians.

4.9. Security Forces Actions. Three actions may occur in domestic violence situations; referral, temporary separation or apprehension. After order has been restored, one or more of these actions is possible.

4.9.1. Referral. If the BDOC/ECC controller has not already done so, request notification of the unit commander or first sergeant, AFOSI, and the family advocacy officer of the situation, as appropriate.

4.9.2. Temporary Separation. Family members may be separated to ensure safety and protection. For example, the first sergeant may suggest that a spouse temporarily leave the quarters or a commander may order the separation by temporarily having the military member stay in a dormitory or military lodging facility. If a child's safety is threatened, take appropriate action under state law, including contacting child protective services. AFOSI has primary jurisdiction for serious child abuse or neglect involving infliction of serious bodily harm. The Security Forces role in this instance is to provide whatever support is requested by the hospital or commander.

4.9.3. Apprehension. Apprehension may be the most prudent course of action when:

- 4.9.3.1. There is a formal complaint;

4.9.3.2. Probable cause exists that a violation of the UCMJ or local law has occurred;

4.9.3.3. The family member refuses to cooperate with Security Forces, unit commander or first sergeant or family advocacy officials.

4.9.3.4. If it becomes necessary to control someone who is not subject to the Uniform Code of Military Justice they will be detained, rather than apprehended, until such time as they can be handed over to local authorities.

4.9.4. Victim and Witness Assistance Program. Security Forces personnel investigating crimes must ensure all victims and witnesses are provided a DD Form 2701, *Initial Information for Victims and Witnesses of Crime*, to ensure victims/witnesses are aware of their rights under the Victim and Witness Assistance Program. For more information, refer to AFI 51-201, *Administration of Military Justice* and Department of Defense Instruction (DoDI) 1030.02., *Victim and Witness Assistance Procedures*. NOTE: If suspected of committing an offense, a party will require rights advisement, pursuant to Article 31 of the UCMJ for military members or the 5th Amendment U.S. Constitution for civilians.

Chapter 5

CRISIS NEGOTIATION

5.1. Overview. A crisis overrides an individual's normal psychological and biological coping mechanisms. During crisis situations, people spontaneously turn to others for comfort, support, understanding, and protection. A crisis does have the potential to disconnect individuals from needed sources of support. The absence of support during a crisis represents the loss of the primary human coping resource and often results in a subject's illogical and highly emotional behavior. All of these factors make crisis situations difficult to control and negotiators must first have a fundamental understanding of crisis negotiation in order to reach successful resolution of situations.

5.2. Types of Behavior. When responding to a crisis involving a hostage taker or barricaded subject, negotiators normally experience one of two categories of behavior; instrumental or expressive. Although these two distinctly different categories of behavior represent opposite ends of a continuum, subjects may often exhibit elements of both types during an incident.

5.2.1. Instrumental Behavior. Instrumental behavior is characterized by substantive demands and clearly recognizable objectives that, if attained, will benefit the subject.

5.2.2. Expressive Behavior. Expressive behavior is designed to communicate the subject's frustration, outrage, passion, despair, anger, or other feelings.

5.3. Types of Hostage Takers. Hostage takers usually fall into one of four major types; mentally disturbed persons, criminals trapped during the commission of a crime, prisoners who are revolting, or political terrorists attempting to produce social change through threat of or use of violence.

5.3.1. Hostage taking, by the very nature of the act, forces the hostage taker into stereotyped responses. The hostage becomes a pawn, caught between the hostage taker and authorities. The hostage takers become violent, strive to control the situation and move the event toward completion of their objective.

5.3.2. The hostage, by conduct, can enhance or diminish their chance of survival. The more the hostage understands about their hostage taker, the better they will be able to predict the hostage takers behavior and feel some degree of control. This can assist by diminishing the hostages fear.

5.4. Reasoning Behind the Taking of Hostages. Hostage taking represents a unique bargain struck over the value of human life. Whatever the immediate motivation, the basic purpose remains the same. Hostage taking is a way of setting up a bargaining position to achieve an otherwise unattainable objective.

5.4.1. A victim may be chosen because the hostage taker believes they can receive a large ransom for the victim's return or because they're well-known, hold a significant job position, or simply because of their affiliation with a country, state, or organization. A victim may simply be hated by their captors and the captor may blame the victim directly for any personal grievances.

5.4.2. Most of the time, the hostage is just an innocent victim of circumstance who happened to be in the wrong place at the wrong time.

5.5. Types of Situations. All crisis situations, regardless of motive, mental health, or criminal history of the subject are either hostage or non-hostage situations. Understanding the difference between the two is paramount to successful resolution of the situation.

5.5.1. Hostage Situations. Subjects demonstrate goal-oriented and purposeful behavior. They hold another person or persons for the purpose of forcing fulfillment of substantive demands upon a third party, usually law enforcement. Substantive demands include things they cannot obtain for themselves, such as money, escape, and political or social change. They use hostages as leverage to fulfill their demands.

5.5.2. Non-Hostage Situations. Subjects often act in an emotional, senseless, and self-destructive manner and have no clear goals. Unable to control their emotions in response to life's many stressors, they are motivated by anger, rage, frustration, hurt, confusion, or depression, and often exhibit purposeless, self-defeating behavior. They have no substantive or escape demands or totally unrealistic demands that they have no reasonable expectation of fulfilling. Disgruntled employees, jilted lovers, rejected spouses, aggrieved individuals, idealistic fanatics, individuals with mental illness, and others with unfulfilled aspirations who feel they have been wronged by others or events fall into this broad category. Non-Hostage situations often result in Domestic Violence, Workplace Violence, or an Active Shooter scenario.

5.6. High Risk Indicators. Law enforcement authorities should be familiar with a number of high risk factors involving background characteristics and behavioral patterns of the subject so appropriate actions may be taken. Law enforcement authorities should be especially wary of a situation that involves a subject who has a history of similar incidents, or who has had previous problems with the hostage(s). Particular attention should be given to whether there have been previous restraining orders issued against the subject for incidents of child or spouse abuse.

5.6.1. Background Characteristics. Subjects with certain background characteristics have a greater potential for being involved in a volatile incident.

5.6.1.1. Multiple Stressors

5.6.1.2. Home Environment Stresses Male Dominance

5.6.1.3. Similar Incidents and Problems with Victims

5.6.1.4. Lacks Family or Social Support System

5.6.2. Behavioral Patterns. Behavioral patterns may also give insight into the type of subject involved in the situation. Types of behavior negotiators may encounter include:

5.6.2.1. Forcing Confrontation with Police

5.6.2.2. Threatening or Injuring Victim(s)

5.6.2.3. Verbalizing Intent to Commit Suicide

5.7. Philosophy of Crisis Negotiation. The philosophy of crisis negotiations includes self-control, approach, empathy, and process. These four separate but interrelated steps have a bearing on the outcome of successful negotiations.

5.7.1. Self-Control. The only aspect of a crisis situation we have absolute control of is our own emotions. When confronted with a difficult subject, the first step is not to control the subject's behavior, but to control your own behavior.

5.7.2. Approach. Don't confuse getting even with getting what you want. Work toward de-escalation of the situation in order to lower tensions. Focus on the process of satisfying each side's needs, rather than the outcome, victory. The subject may be frustrated, angry, afraid, confused, depressed, or demonstrating other emotions. Listening is most effective concession you can make when negotiating. Show respect for the subject regardless of the circumstances or situation.

5.7.3. Empathy. Empathy absorbs tension, and should be used to see through the eyes of the subject. A calm controlled demeanor is more effective than a brilliant argument. Being "right" is not the issue. The issue is making the attempt to correctly understand what the subject is saying.

5.7.4. Actively listen to the subject and acknowledge their point of view. This does not equate to agreeing with the subject. Attempt to find common ground and agree with the subject whenever you can without conceding. Don't argue with subjects. Attempt to create a positive atmosphere. Remember that people don't always say what they mean. Attempt to identify their true meaning, and be aware the true meaning is often an unsatisfied need. **NOTE:** Negotiators are not in the business of meeting demands, but rather they attempt to satisfy each side's needs.

5.8. Response. There are generally four choices for commanders at a hostage situation. The first traditional confrontational response is to amass patrolmen and massive firepower and assault. The second is to use selective sniper fire. The third is to use chemical agents. The fourth is to contain the area and negotiate with a specially trained negotiator. The first three will almost always result in injury.

5.8.1. If possible, progress from a lesser response option to increased force options as the situation unfolds. If the threat to the victims is believed low, then high-risk tactical actions are inadvisable and difficult to defend. If the threat to the victims is higher, then risk-effective tactical action is easier to defend and should at least be considered. Finally, if the threat to the victims is very high, then high-risk tactical action may be essential. It is extremely difficult to return to negotiating after an assault takes place.

5.8.2. The linear approach, parallel application, and law enforcement attitudes play a significant part in response options.

5.8.2.1. Linear Approach. The linear approach is a two-step approach. First, the negotiator tries to talk the subject out. Second, assault teams use force to take the subject out (if necessary). **NOTE:** Linear application of force almost always results in strong resistance from the subject(s), and should only be used as a last resort.

5.8.2.2. Parallel Application. Parallel application is the use of negotiations and tactics in synchronization. Tactics don't simply follow failed negotiations; rather the proper use of tactics encourages negotiations. Weigh the benefits of reaching agreement through negotiations with the risk of disagreement potentially leading to tactical intervention. An appropriate limited display of tactical power is not the same as an overtly threatening use of that power. The goal remains to bring subjects to the table, not to their knees.

5.8.2.3. Law Enforcement Attitudes. Law enforcement authorities should be aware of how their attitudes can affect the outcome of crisis situations.

5.8.2.3.1. Emotion. Keep your emotions under control regardless of what transpires during the situation.

5.8.2.3.2. Haste. Don't make snap decisions or attempt to push the subject to agree to resolution.

5.8.2.3.3. Rigidity. Refusing to listen and negotiate does not aid in peaceful resolution.

5.8.2.3.4. Creativity. Creativity is a strength. Use things subjects say to create opportunities to seek peaceful resolution.

5.8.2.3.5. Flexibility. Flexibility is a strength. Being flexible and negotiating with the subject establishes rapport and trust, and aids in peaceful resolution.

5.8.2.3.6. Patience. Do not develop preconceived ideas that you must do something to resolve the situation. Showing patience and having restraint is not a sign of weakness, and can contribute to peaceful resolution of situations.

5.9. Operations . The Operations Section Chief (OSC) must understand that the choices they make during any situation not only involve them, but also the Incident Commander (IC), and may be scrutinized both in a court of law and the court of public opinion. When making decisions, the OpsSC should use a three-part action criterion: 1) is the contemplated action necessary 2), is the contemplated action risk-effective, and 3) is the contemplated action acceptable in a particular situation? OpsSCs should be prepared to answer why they took action when they did and whether they fully explored and attempted to implement less risky alternatives first. OpsSCs should coordinate with SJA, as needed.

5.9.1. Tactical Intervention. Loss of life is most likely to occur during tactical intervention. Therefore, before initiating any tactical action, the OpsSC must carefully consider the current threat to hostages/victims and risks tactical officers face.

5.9.2. Unified Strategy. The OpsSC must bring all key component leaders together and ensure all parties understand the type of situation and its accompanying dynamics. All component leaders must understand and support the strategy once it is developed.

5.9.3. OpsSC or IC as Negotiators. OpsSCs and ICs must not act as negotiators during a situation. They do not have the time to dedicate to negotiations. Their focus must remain on the operation in its totality and must not be diverted.

5.10. Use of Tactical Teams. The use of deadly force is the last option. When dealing with "expressive" subjects, teams should keep a low profile to create a non-threatening environment to assist in returning the subject to a normal functioning level. When dealing with "instrumental" subjects, teams should make subjects aware of their presence in an effort to promote agreement.

5.11. Negotiation Teams. Crisis negotiation is one of law enforcement's most effective tools and constitutes a highly refined law enforcement discipline. The successful resolution of countless hostages, barricaded subjects, attempted suicides, and kidnapping cases throughout the world repeatedly has demonstrated the value of negotiating. These successful cases, as well as

those that resulted in the loss of fellow patrolmen and hostages, have shown the need for careful deliberation in the selection and training of crisis negotiation team members. From a safety and liability aspect, law enforcement authorities must understand how to select, organize, and train crisis negotiation teams.

5.12. Selecting Team Members. Certain skills and expertise make more successful negotiators and result in more peaceful resolutions in shorter time frames.

5.12.1. Negotiation Team Leaders. Negotiation team leaders must be experienced, knowledgeable, and articulate supervisors or senior personnel. They should be well trained in the most current procedures for establishing and maintaining negotiations. They must understand how to devise a flexible negotiation strategy based on the incident and be capable of effectively articulating this strategy to the OpsSC and IC. In addition to overseeing actual negotiations, team leaders are responsible for training team members and recruiting new team members. Team leaders serve as principal advisors to the OpsSC.

5.12.2. Negotiators. Negotiators should be volunteers and in excellent mental and physical health. The best criminal investigators tend to be the best crisis negotiators. They have had contact with a wide variety of people in diverse circumstances. Negotiators must have the time to participate in training and be available for call-outs regardless of other duties and responsibilities. Following are desirable personality traits for negotiators:

5.12.2.1. Possess emotional maturity.

5.12.2.2. Good listeners and possess excellent interviewing skills.

5.12.2.3. A person who can easily establish credibility with others.

5.12.2.4. Have the ability to use logical arguments to convince others that their viewpoint is rational and reasonable.

5.12.2.5. Able to communicate with persons from all socioeconomic classes.

5.12.2.6. Have practical intelligence, common sense, and are streetwise.

5.12.2.7. Have the ability to cope with uncertainty and be willing to accept responsibility with no authority.

5.12.2.8. Have total commitment to their job (negotiations).

5.12.2.9. Understand they will have to assist in planning an assault to rescue hostages if negotiations are not going well and lives are in imminent danger.

5.12.3. Negotiation Team Composition. A minimum of three negotiators is recommended for each incident. One team member acts as primary negotiator and engages the subject in dialogue. The second team member acts as a coach, or secondary negotiator, and assists the primary negotiator with choosing a specific dialogue and communication techniques. The third team member acts as team leader and assists in formulating the overall negotiation strategy, and interfaces with other response elements as they arrive. It is recommended that units have more than three negotiators available for incidents. If units are unable to source negotiators from within, it is recommended they establish an MOU/MOA with outside agencies.

5.12.4. Negotiation Team Duties. Experience has revealed that a properly staffed negotiation team can more thoroughly assess an incident and generate better strategies. Teams must efficiently perform vital functions such as coaching the primary negotiator talking with the subject, maintaining situation boards, keeping a log, and communicating with the on-scene commander, command post and tactical team. The following serves to identify recommended positions, locations, and duties of a negotiation team during a significant or protracted event. This is only a guide and may be tailored to meet the needs of a specific situation. **NOTE:** Only trained and certified negotiators should occupy the positions of team leader, primary negotiator, and coach. Other positions may be filled with investigators, other law enforcement personnel, or support personnel.

5.12.4.1. Negotiation Team Leader (Coordinator)

5.12.4.2. Assistant Negotiation Team Leader

5.12.4.3. Command Post Liaison

5.12.4.4. Primary Negotiator

5.12.4.5. Coach (Secondary Negotiator)

5.12.4.6. Recorder

5.12.4.7. Intelligence

5.12.4.8. Behavioral Profiler

5.12.4.9. Tactical Liaison

5.13. Training Negotiation Teams. Once a team is selected and assigned responsibilities, you must determine the type of training team members need. Training should consist of basic skills training, advanced and special skills training, team leader training, and regular team and individual skills maintenance training. **NOTE:** The FBI conducts courses at many locations throughout the United States at no cost to participating agencies. Training coordinators in FBI field offices arrange these courses by request. In addition, the Federal Law Enforcement Training Center in Glynco, Georgia, also offers training courses.

5.13.1. Basic Skills Training. All negotiators should attend a 40-hour basic crisis negotiation course. The basic course should include extensive training in crisis intervention, suicide assessment and intervention, and knowledge of how to work the various positions on the team, and how to interact with tactical teams.

5.13.2. Advanced and Special Skills Training. Experienced team members can use advanced and specialized training to build on basic crisis intervention techniques. This training should include handling manipulative subjects, reframing techniques to put a different spin on negative thoughts and perceptions of hostile subjects, and use of guided discovery-questioning techniques to augment basic problem solving techniques.

5.13.3. Team Leader Training. Team leader training should include further training and practice in risk assessment, legal considerations, procedures for handling protracted incidents, effects of alcohol and other drugs, kidnap/extortion negotiations, role of the media, and use of third-party intermediaries and mental health professionals.

5.13.4. Regular Team and Individual Skills Maintenance Training. Negotiation team members should periodically conduct in-house refresher training of the items covered in basic skills, advanced and special skills, and team leader training that they have been formally trained on.

5.14. Resiliency. The TSR team will provide TSR services to enhance resilience to potentially traumatic events. Following any negotiation, it is essential that all team members have access to a TSR Team.

5.15. First Responder Negotiations. The first 15 to 45 minutes are the most dangerous time in a crisis situation excluding a rescue attempt. Therefore, the most crucial moments of the situation are in the hands of the first Security Forces member on-scene. Although the first Security Forces member on-scene should not begin negotiations, it may be appropriate to initiate contact with the subject in order to gain intelligence. Further, subjects may initiate an on-going dialogue with the first Security Forces member on-scene on their own.

5.15.1. Stabilize and Contain the Situation. In the first few minutes of a crisis situation, the subject's anxiety may overpower rational thought processes. The subject is now more likely to act on impulse or out of desperation. Your first action should be to ensure your own safety and approach the area cautiously. Then you should attempt to isolate, contain, and evaluate the situation, provide an initial report, and request assistance.

5.15.1.1. Reduce Likelihood of Further Violence. Your next actions should be to reduce the likelihood of further violence. Begin to clear the area of innocent bystanders if you can do so safely without exposing yourself to other dangers. The best alternative is to evacuate the area along routes out of sight of the subject. This should be accomplished nonverbally with hand and arm signals if at all possible. If it is not possible to evacuate pedestrians out of sight of the subject, an alternative may be to tell the subject clearly what you want to do and get the subject to agree to allow the pedestrians to leave. Every effort should be made to evacuate pedestrians to a single location to assist in accounting for all pedestrians and have them available for witness interviews.

5.15.1.2. Calm the Subject. The first few statements between you and the subject may set the tone for the next few hours. Start with giving the subject your name and let them know that you are a law enforcement officer. Reassure the subject that things are under control outside and that you don't want anyone including the subject to be injured.

5.15.1.3. Avoid Eliciting Demands. Seemingly innocent questions may give the subject an opportunity to make demands on you. For example, a question such as, "What's going on in there?" may result in an answer like, "I have this clerk in here with a gun to her head and I'll shoot her if you're not gone in five minutes." If you become engaged in an ongoing conversation with subjects, you should make every effort to avoid bargaining and making concessions. Your best option is to continue to calm and reassure the subject that no one is going to attempt to harm him/her and that you don't want the subject or any hostages harmed. If the subject should make demands, let the subject know that you can't make that decision but that law enforcement authorities who can assist the subject are on their way to the scene. If the two of you establish some sort of rapport, the negotiation team may have you continue to act as the primary negotiator with their support and guidance.

5.15.1.4. Gather Information. Listening carefully to the subject may allow you to determine the sex, race, ethnic group, age range of the subject, or other pertinent information. Be prepared to pass any information to negotiators upon their arrival at the scene.

5.16. Guidelines. Once you have isolated and contained the situation as best you can, use the following guidelines when dealing with subjects pending the arrival of the hostage negotiation team.

5.16.1. Keep a Log. The negotiation and tactical teams will be looking to you for information upon their arrival at the scene. Accordingly, keep a log of everything that transpires even if you have little or no contact with the subject. Record all communications with the subject along with your initial observations and impressions. Note exact words of the subject and your exact response if possible.

5.16.2. Allow the Subject to Speak. Be a good listener and let the subject talk. Listening to the subject may provide some hint or indication of their willingness to surrender. Avoid dominating the conversation.

5.16.3. Avoid Giving Orders.

5.16.4. Play Down Past Events.

5.16.5. Don't Offer the Subject Anything.

5.16.6. Avoid Directing Attention to the Victims.

5.16.7. Be as Honest as Possible. The majority of situations are resolved through straightforward honest dialogue. The first task is to establish rapport and trust.

5.16.8. If Unsure What's Intended, Ask. Don't try to interpret an unclear statement. Simply ask what is meant if unsure.

5.16.9. Never Dismiss Any Request as Trivial.

5.16.10. Never Say "No."

5.16.11. Soften Demands.

5.16.12. Never Set Deadlines. Never set a deadline on yourself and try not to accept a deadline from a subject. Never tell a subject something will be done within a specific time. For example, "I'll have you some coffee in 10 minutes."

5.16.13. Don't Make Alternate Suggestions.

5.16.14. Don't Introduce Outsiders. Never allow a non-law enforcement person (wife, minister, friend, etc.) to enter into an ongoing hostage situation unless the OpsSC and IC approve it.

5.16.15. Don't Allow Exchanges. Do not allow any exchange of hostages, and especially don't exchange yourself for a hostage.

5.16.16. Ask About Suicide. Ask subjects directly if they are considering suicide if you sense they may be considering it based on their comments. If a subject isn't considering suicide, you won't push them over the edge or put the idea in their head. If a subject is considering suicide, they may realize you can understand how they feel. This could be the

first step in establishing rapport and trust eventually resulting in subjects abandoning weapons and surrendering.

5.16.17. Never Negotiate Face-to-Face. Negotiating face-to-face is unnecessarily risking your own life. Further, if a subject threatens your life, other law enforcement officers may have to expose themselves in order to assist you. Finally, if the subject is considering suicide, they may use an assault on you to provoke other patrolmen into taking their life (suicide by cop).

5.16.18. Plan Surrenders. The subject may decide to surrender prior to the arrival of the negotiation team and surrender plans are critical since you have an armed subject preparing to move from a barricaded position to your control. You must decide whether the hostages or the subject exit first and there are advantages and disadvantages to both. In any case, you should avoid taking a weapon directly from a subject. Instead, arrange for the subject to leave any weapons in a safe place prior to taking control of them.

5.17. Suicide Intervention. One of the most pressing considerations in dealing with a barricaded subject, whether hostages are present or not, is the possibility the subject might commit suicide. Unfortunately, many incidents conclude with the subject committing suicide even when a successful resolution seems near. Negotiators or first responders may be called on to attempt resolution of these situations, and suicide intervention can be more difficult than other situations.

5.17.1. Why Suicide. Subjects may choose suicide or exhibit suicidal behavior because of hostility toward others, traumatic life events, lack of social support, alcohol abuse, depression, or a feeling of hopelessness.

5.17.2. Crisis State. A subject who is suicidal is in a state of crisis. An event has occurred and the subject's normal coping mechanisms have failed to resolve the situation. The subject is behaving at an intense emotional level rather than a rational level in response to the situation.

5.17.3. Understanding Suicide. It is crucial that negotiators understand what suicide is, and are aware of myths and assumptions prior to attempting to resolve a suicidal situation. Negotiators should be familiar with AFI 44-154, *Suicide and Violence Prevention Education and Training*, and AFPAM 44-160, *The Air Force Suicide Prevention Program*.

5.17.4. Suicide Methods. Suicidal subjects often have a detailed plan as to how they intend to commit suicide. Determining the subject's intended method may enable negotiators to disrupt the plan and prevent the suicide. Negotiators must remain alert to any indications of the subject's preferred method of suicide. In this regard, negotiators need to determine whether the subject possesses the means of suicide such as firearms, explosive devices, medications, or cutting instruments, or if they intend to be killed by engaging law enforcement with lethal force, forcing the patrolmen to use deadly force against them to kill them (suicide by cop).

5.17.4.1. Negotiators and responding patrols should be aware that suicidal individuals may seek to destroy themselves because of depression, desperation, or a need to punish society for the wrongs they feel it has committed against them.

5.17.4.2. Subjects may not view death at their own hands as a socially acceptable method of death because of their individual social standards. Therefore, they may confront law enforcement authorities in a manner they know will require the use of deadly force. They believe this will allow society to perceive them as a victim of others instead of a victim of themselves.

5.17.4.3. Although the following information is not all inclusive, the presence of one or more of these indicators may help identify a subject who is considering suicide by cop. Where a combination of these indicators are present, law enforcement authorities should consider them as evidence of a possible suicide by cop scenario especially if the subject confronts them in a manner that could bring about his own death.

5.17.4.3.1. Subject has initiated a hostage or barricade situation and they refuse to negotiate with law enforcement authorities.

5.17.4.3.2. Subject has just killed a significant other in their life, especially if the victim was a child or the subject's mother.

5.17.4.3.3. Subject demands that law enforcement authorities kill them.

5.17.4.3.4. Subject sets a deadline for law enforcement authorities to kill them.

5.17.4.3.5. Subject has recently learned they have a life threatening illness or disease.

5.17.4.3.6. Subject indicates an elaborate plan for their death, one that has taken both thought and preparation.

5.17.4.3.7. Subject says they will only surrender in person to the officer in charge, e.g., the police chief or an officer with substantial rank and influence.

5.17.4.3.8. Subject indicates they want to go out "in a big way."

5.17.4.3.9. Subject presents no demands that include escape or freedom.

5.17.4.3.10. Subject provides law enforcement authorities with a verbal will.

5.17.4.3.11. Subject appears to be looking for a manly or macho way to die.

5.17.4.3.12. Subject has recently given away money or personal possessions.

5.17.4.3.13. Subject has a criminal record indicating past assaults.

5.17.4.3.14. Subject has recently experienced one or more traumatic events in their life that affects their family or career.

5.17.4.3.15. Subject expresses feelings of hopelessness and helplessness.

5.17.5. Negotiation Strategy. The purpose of intervention is to defuse intense emotions and return the subject to a normal functioning level. To accomplish this, negotiators must ask about suicide, buy time, establish rapport, communicate empathy, and gain information. Ultimately, your goal is to influence the subjects thinking in an attempt to return the subject to a normal functioning level where they will decide not to commit suicide. Negotiators should offer helpful suggestions and try to point out possible solutions to the subject's problems. However, negotiators should refrain from offering guaranteed solutions because these solutions have the potential to fail. Always try to help subjects face reality through discussions of the possible impact on the subject's family and friends.

5.17.6. Impact on Negotiators. The impact on negotiators of losing a suicidal subject can be severe. Negotiators consider the death of a hostage as being the direct responsibility of the subject, whereas, the loss of a suicidal subject may cause the negotiator to blame themselves. Negotiators often ask themselves what they did wrong or what else they could have said or done to prevent the subject from committing suicide. Supervisors should assess the negotiator to see if they need to seek attention from Mental Health.

5.18. Training. Units must incorporate first responder training as described in the Air Force Emergency Response Operation Command and Control course into their annual training plans. Units and flights need to coordinate training with the designated Incident Commander on the installation, usually the Fire Department. In most crisis situations, subjects either verbalize or otherwise demonstrate their concerns regarding possible armed intervention. First responder training should concentrate on improving patrolmen's verbal and communication skills. The way a first responder verbally conducts themselves has a significant bearing on their ability to deal effectively and successfully with a wide variety of situations to include crisis situations.

Chapter 6

EMERGENCY SERVICES TEAM (EST)

6.1. Concept. The basic premise of an EST is to have a tactical team of highly motivated and well conditioned SF members that are specially trained and equipped to function in a high-risk environment as a more effective and safer employment option than a larger group of SF without the specialized training. The formation/establishment of an EST is optional; however, each AF installation must have some type of emergency tactical response capability.

6.1.1. MOA for Tactical Support. Installation Commanders may utilize civilian law enforcement support in lieu of establishing an EST, with supporting Crisis Negotiations Team (CNT), on their installation. This will be done through an MOA. A sample MOA can be found in [Attachment 4](#) of this instruction. All MOAs will include the following information as conditions that must be agreed upon by both parties:

6.1.1.1. Command and Control. The Installation Commander or DFC, if delegated, has tactical control (TACON) of the civilian agency team members when employed on the installation. The civilian agencies' leadership will maintain operational control (OPCON) of their team members and act as the liaison officer to the IC regarding tactical employment of his/her personnel. The Installation Commander will have final authority for any changes in tactical employment throughout the operation as well as when/if the EST/tactical team executes high risk operations.

6.1.1.2. Authority/Jurisdiction. Prior to establishing an MOA with local law enforcement agencies, consultation with the installation SJA is necessary to determine if the civilian agency can operate on the installation. Consultation is also required with the SJA when the installation is located outside of the US to determine, among other matters, if the agreement is considered an international agreement within the meaning of AFI 51-701, *Negotiating, Concluding, Reporting, and Maintaining International Agreements.* Additionally, the MOA must be routed through the appropriate channels (e.g. Wing Plans, Integrated Defense Council, Installation Antiterrorism Working Group, etc. as determined by the Installation Commander) before entering into the agreement.

6.1.1.3. Certification. The local law enforcement agency must ensure their SRT or equivalent designated tactical team meets state certification and training standards prior to the DFC allowing employment on USAF installations. If there is no official state certification, the agency must meet the standards established by the National Tactical Officers Association (NTOA) in *SWAT Standards for Law Enforcement Agencies, Sep 2008*, posted on their website: <https://www.ntoa.org/massemail/swatstandards.pdf>. There are separate standards for permanent tactical teams and part-time tactical teams. **NOTE:** NTOA standards are not a certification, rather a training standard the agency must meet.

6.1.1.4. Training. MOAs with local law enforcement agencies must include guidance on their participation with mandatory recurring combined training on the installation. Training will take place with the local law enforcement agencies, the assigned SF unit, applicable FES personnel, and any certified ICs. At a minimum this training must occur semi-annually, not to exceed 180 days, with or without the participation of the local law

enforcement agencies. Additionally, a combined exercise must be conducted annually IAW AFI-10-2501, and will not exceed 365 days. This exercise will include, SF personnel, FES personnel, certified IC personnel, and if possible the local law enforcement agencies with whom MOA's have been signed. Exercises will be evaluated by the Wing Exercise Evaluation Team (EET). A senior representative from the local law enforcement agency will be invited to be part of the evaluation team. Documentation of all training and exercises will be maintained by SFMQ and the EST Officer-in-Charge (OIC) or Noncommissioned Officer-in-charge (NCOIC). **NOTE:** If the Wing EET does not possess a SF expert, SFMQ personnel should augment in the evaluation of the exercise.

6.1.2. The DFC is responsible for organizing, training and equipping the EST to meet mission objectives. A trained and certified IC will assume the role as the IC and the DFC or senior SF representative will assume the role of Operations Section Chief for EST employment operations.

6.2. Objective. The AF's primary objective in dealing with high-risk incidents is to prevent or minimize the loss of life and resources by containment, negotiation and yielding to other federal lead agencies. Consistent with the lead agency concept, during high-risk situation the USAF can yield to the FBI or FAA, as required. When a designated lead agency assumes control of a high-risk situation on an Air Force installation, the Installation Commander must be prepared to provide EST support if requested, either by organic resources or through an MOA with another civilian police agency.

6.2.1. EST provides the Installation Commander with a viable option to restore good order and discipline during high-risk incidents. Effective employment of EST can result in achieving the desired incident outcome and mitigate potential losses due to hostile forces or other criminal adversaries. EST's primary goal is the preservation of life and keeping USAF assets and resources out of the control of criminal and terrorist "elements".

6.3. Capability. Each installation must plan and exercise capabilities to respond to and resolve a variety of high-risk incidents including, but not limited to: hostage incidents, sniper attacks, DV protection support, aircraft hijacking, drug investigation/"buy-bust" apprehension support, acts of terrorism and barricaded suspect incidents. The EST concept is designed to provide support via pre-selected and highly trained personnel ready to respond as an effective team to these high-risk incidents in the most effective way possible. Installation ESTs will alleviate command and control problems that may be encountered when using local law enforcement agencies as the high-risk incident response force. Establishing organic assets or an MOA ensures USAF installations will not be unprepared to resolve high-risk incidents by relying on the assumption the FBI or FAA will respond in a timely manner or be available to respond to a given high-risk incident. EST concept success is predicated on the voluntary participation of highly motivated, well trained and properly equipped personnel.

6.4. Organization. The number of personnel assigned to an EST is determined by: geographic location of the installation, host wing mission, size of the SF unit, local criminal and terrorist threat, wing FPCON requirements and other localized antiterrorism and force protection requirements. Assigned primary and alternate personnel should equal the number necessary to ensure 24-hour recall/response capability and will be determined by the DFC.

6.4.1. Team composition should entail the following critical positions: OIC/NCOIC, Trainer, Entry Team, Apprehension/Extraction Team and Marksman/Observer Team. The minimum team requirement for building entry is eleven (11) personnel: six (6) to enter, four (4) to secure the inner perimeter and an OIC/NCOIC working with the Operations Section Chief to provide tactical advice. The DFC can augment minimum personnel requirements or establish additional requirements based on the installation's local criminal and terrorist threat environment.

6.4.2. The EST is a police services activity that reports directly to the DFC. The DFC is responsible for team training, coordination and advising the IC on EST employment. The EST OIC/NCOIC is responsible for staffing, rehearsals/training and general leadership of the EST. Additionally, he/she is responsible for maintenance of recall rosters, equipment inventories, applicable quick reaction checklists and other documentation that may be beneficial during response operations.

6.5. Employment. Employ the EST as required to resolve high-risk or potentially violent incidents. The DFC or designated representative should consider the following:

6.5.1. Negotiations should be the first option for peaceful resolution of high-risk incidents. The IC or Operations Section Chief will direct employment of the EST to secure the incident in lieu of other alternatives (i.e. continued negotiation when it has proven ineffective), but the DFC is ultimately responsible for executing the operation and must maintain functional control of the EST.

6.5.2. EST should not be staged in open areas in conjunction with non-violent civil disturbances, protest demonstrations and/or special events such as air shows and open house events. Crowd control should be conducted by other SF members. The EST should be staged well out of sight in a designated area during these events to respond if high-risk incidents evolve.

6.6. Weapons. If using a military EST team, their authorized EST weapons include the carbine/rifle, handgun/pistol, grenade launcher and the shotgun. Unapproved modifications are not authorized. Reference AFMAN 31-222, *Use of Force Manual*, for authorized nonlethal weapons/munitions.

6.6.1. EST members will carry a primary and secondary weapon. The pistol will normally be the secondary weapon, but is not limited to this role.

6.6.1.1. The entry element should carry the carbine or rifle and be configured to accommodate employment of nonlethal munitions.

6.6.2. EST designated marksman (DM)/observer teams should be armed with the rifle (currently authorized SF carbine or rifle, e.g. M-4 or M16A2) equipped with an Advanced Combat Optic Gunsight (ACOG) or an approved variable power scope. Individuals who have completed the Advanced Designated Marksman (ADM) AFQC or the Sharpshooter AFQC and whose qualification is current, may perform EST DM duties utilizing the currently authorized AF Sharpshooter or ADM rifle if available. Units will not be authorized these rifles for EST use alone. **NOTE:** Specific Sharpshooter, ADM and EST DM qualification training is required to employ personnel in these roles. Refer to AFI 36-2226, *Combat Arms Program*, for qualification training requirements. The EST DM will not

normally be employed at target distances beyond 200 meters, with the optimal range in urban environments being 100 meters.

6.7. EST Training and Team Certification. National training standards required for SWAT/EST personnel are published by the National Tactical Officer Association (NTOA). These minimum standards must be completed successfully and documented on a localized AF Form 1098, *Special Task Certification and Recurring Training* prior to the individual being certified as an EST member. Regular sustainment training IAW NTOA guidelines as a Fulltime or Collateral team member must be successfully completed to maintain certification. Failure to sustain training will result in decertification. Remedial training must be conducted before the member may be employed in a tactical environment. Formal EST training must be obtained through either the United States Army SRT Phase I course or another training course that meets the national training standards IAW NTOA guidelines. Qualified marksman/observer team personnel should complete the SRT Phase II course or the CPEC in addition to Phase I. The US Army operates the SRT courses at Fort Leonard Wood, MO, as well as, offers a Mobile Training Team capability. More information on SRT is available on the US Army Military Police School web site at: <http://www.wood.army.mil/usamps/>. **NOTE:** SRT Phase II, CPEC and ADM graduates meet requirements for marksman/observer teams as well. The CPEC and ADM are taught at the SF Regional Training Center at Fort Bliss, TX.

6.7.1. Tactics, Techniques and Procedures (TTPs). EST TTPs are consistent with the consolidated DoD standards adopted by the US Army and the US Marine Corps military police for their SRTs, which provide a tactical police/force protection capability for each respective service. Technical guidance regarding EST TTPs is provided in Army Field Manual (FM) 3-19.11, *Special Reaction Teams*, and will be used by the Air Force as the tactical reference for EST employment for high risk situations. The minimum training standards must be completed by at least one EST member, preferably the NCOIC, who will then be certified to train the additional EST members. The ultimate goal, however, should be for each EST member to attend the SRT course or equivalent.

6.7.2. Training. The goal in preparing teams is to provide a disciplined, professional response force rather than an unorganized operation assembled only when high risk situations occur. DFCs who establish an EST should seek initial training for all team members. The preferred course is the US Army SRT either in residence or through a Mobile Training Team (MTT). The two week SRT course (L5AZ3P071 0S2A, PDS Code 051) is held approximately every month, but has a maximum of 30 students per class and only a small percentage of those are allocated to the AF. SRT MTTs must be requested through the parent MAJCOM/A7S to the Headquarters, Department of the Army, G3 DAMO-ODO Provost Marshal. MTTs allow units to maintain team integrity and continuity and are much more cost effective than sending team members through the resident courses piecemeal. Every effort should be made to qualify EST members. Installation DFCs may seek initial and continuing training through the local law enforcement, FBI training programs, or private tactical schools as long as the basic standards in paragraph 6.1.1.3. are met.

6.7.2.1. All training must be documented in the individual's Air Force Training Record (AFTR) Section III. A copy of the documentation of training will be maintained by EST OIC/NCOIC.

6.7.3. Sustainment. Recurring training frequencies will be conducted IAW NTOA guidelines dependent upon member participation (i.e., Fulltime or Collateral). The DFC is responsible for team proficiency and sustainment training. The perishable nature of individual and collective skills necessary to perform effectively in the high risk environment requires allocation of optimum training time for EST members. Proficiency training must be continual and include realistic scenarios. ESTs must incorporate and utilize Standard Operating Procedures (SOP) battle drills and immediate action drills during training and rehearsal. Heavy emphasis must be placed on physical conditioning and teamwork drills to develop necessary skills and build individual and team confidence in stressful situations. Training sessions must be structured around a triad of 60% tactics, 20% marksmanship, and 20% physical conditioning. Following an initial training program/course, each EST member must meet continuation training standards established per applicable local Operating Instructions (OIs). EST DM/observers must meet the qualification standards outlined in AFI 36-2226 and AFMAN 36-2227, Volume 1, *Combat Arms Training Programs, Individual Weapons*. Units must develop local training programs for EST DM to augment qualification training and are encouraged to conduct more frequent live-fire sustainment training. Refer to AFCAT 21-209, Volume 1, *Ground Munitions*, Table 2.22, 2.37 and 2.38 for authorized EST, sharpshooter and designated marksman training munitions support requirements.

6.7.4. Other Training Topics.

6.7.4.1. Integration of crisis negotiations, Emergency Medical Service (EMS), Explosive Ordnance Disposal (EOD) and AFOSI/ Security Forces Investigations (S2I) capabilities to include management, analysis and support for EST operations/response.

6.7.4.2. Designated marksman/observer observation and recording skills and command and control mechanisms.

6.7.4.3. Performance oriented team leader/member skills.

6.7.4.4. Advanced physical fitness to include approved defensive tactics per AFMAN 31-222. At a minimum, all EST members must meet USAF fitness standards and establishing a higher physical standard for team members is recommended.

6.7.4.5. Individual and small group training activities/exercises.

6.7.4.6. Reading building schematics. This will assist in the familiarization of local systems used by CE and how to obtain a specific plan quickly.

6.7.4.7. Training should be realistic and based on local threats and conditions. Practical training conducted to rehearse contingency plans will enhance EST effectiveness during actual high risk situations.

6.8. EST Relationship with CNT. EST members do not participate in or influence negotiations. They should, however, pass on-scene information to the CNT regarding the evolving situation regardless of type. In turn, the CNT can provide information to the EST. If the EST is ordered to assault, the CNT may provide assistance by indirectly distracting the subject through continued contact. EST team leaders should attempt to employ AFOSI and S2I to gather additional information on criminal elements during contingency responses. Close coordination with these organizations is essential to effective EST employment across the spectrum of force protection contingencies. Information sharing between EST and CNT should

be managed through the BDOC. If possible, the principal negotiator should not know when the assault order has been given. Inadvertent disclosure could jeopardize the operation.

6.9. MWD Team Use. Employment of the MWD is most effective when searching for a possible subject/suspect(s) within a facility or concealed in an outdoor environment. If MWDs are used, the team must also be included in regular EST training. Immediately follow any MWD entry with EST entry to conduct a search and secure the area. The MWD handler will control and direct the tactical movement of the MWD and the EST leader will control and direct the tactical movement of the EST.

6.10. Emergency Medical Readiness. Planning for any high-risk situation or tactical mission should include first-aid and buddy care. Ideally, the team should include a member(s) dedicated and trained as emergency medical technicians (EMTs). EST members should train for medical contingencies on a regular basis. If the EST doesn't have a dedicated EMT, training and exercise scenarios should include EMS personnel, when possible. It is essential for installation contingency planning to include careful coordination between installation EMS, CNT, FES, EOD and SF to ensure participants understand the mission requirements of one another. This will help clarify expectations of additional responding agencies.

6.11. Information. EST operations are dependent on the timely availability/delivery of reliable information. Training and exercise scenarios should include the collection and use of operational information. ESTs should seek assistance from S2I, AFOSI, and/or wing intelligence as needed and authorized.

6.12. Interagency Cooperation. In addition to mandatory exercises and training events, ESTs should meet and train with counterparts from other federal, state and local agencies (MOA with FBI, FAA and local law enforcement) whenever possible. The shared experience of actual or exercise response operations are mutually beneficial and may increase mission success.

6.13. Exercises. Rehearsing the EST in conjunction with supporting base agencies is essential. This is best achieved through a robust base exercise and evaluation program.

6.13.1. Joint agency exercises test command and control arrangements outlined in MOAs and operation plans. They also provide a means to assess the installation's ability to provide timely criminal intelligence, demonstrate team capabilities to the IC, build team confidence, and inter/intra-agency teamwork while affording the opportunity to refine EST TTPs.

6.13.2. Scenarios should be consistent with the local threat and should include situations dealing with workplace violence, hostage incidents, barricaded subjects, terrorist attacks, hijackings, school violence and counter-sniper operations.

6.14. Reporting Requirements. Report all initial and updated information on Force Protection/Suspicious Activity events to the Command Post. Command Post will ensure events meeting OPREP-3 (Ref AFI 10-206, *Operational Reporting*) reporting channels are submitted as required. The DFC will submit SF lessons learned reports within 60 days of an EST (or local civilian SWAT) response through the AF Joint Lessons Learned Information System (AF JLLIS) to the respective MAJCOM. The MAJCOM will in turn forward a copy of the report to HQ AFSFC/SFOP within 90 days of the incident.

Chapter 7

CIVIL DISTURBANCES

7.1. Introduction. Civil disturbances present unique challenges to the armed forces. The roles and missions of the armed forces inherently make the DoD a likely target for civil disturbances both at home and abroad. The disturbances may range from peaceful demonstrations and rallies outside a main gate to full scale riots that include burning and looting government property inside the perimeter fence (see Attachment 5). The information, technology and weapon systems entrusted to our care require absolute protection. The challenge arises in dealing with civil disturbance situations. Attempting to understand, predict and control crowd behavior is a highly technical field that requires specialized training. Complicating this challenge is the fact that most of the specialized training is not common to any of our everyday missions and is extremely perishable. Army Field Manual (FM) 19-15, *Civil Disturbances*, can provide the reader with additional information on the topic.

7.2. Definition. Civil disturbances arise from acts of civil disobedience. These acts occur most often when participants in mass acts of civil disobedience become antagonistic towards authority and authorities must struggle to take the initiative from an unruly crowd. In the extreme, civil disturbances include acts of criminal terrorism. Civil disturbances, in any form, are prejudicial to public law and order. The installation commander is responsible for maintaining law and order on the military installation. Installation commanders respond to disturbances using installation resources. Violence and disorder by any individual or group of individuals will not be tolerated. Installation commanders must be prepared to counter a disorder if preventative measures fail. This preparation should consist of the following elements:

- 7.2.1. Know the statutory and directive authority on which control actions rest.
- 7.2.2. Maintain accurate operational information.
- 7.2.3. Ensure all personnel assigned civil disturbance related tasks are adequately trained.
- 7.2.4. Ensure personnel are properly equipped to handle civil disturbances.
- 7.2.5. Develop plans that are flexible enough to ensure available manpower and equipment is used to the best advantage when violence occurs.

7.3. Federal Intervention and Aid. The US Constitution and US Code (USC) empower the President to direct federal intervention in civil disturbances as listed below. However, other than in extreme emergency situations, only the President or SECDEF may authorize federal troops to intervene. The installation SJA should always be consulted before using forces in any of these capacities.

- 7.3.1. Respond to state requests for aid in restoring order.
- 7.3.2. Enforce the laws of the United States.
- 7.3.3. Protect the civil rights of citizens.
- 7.3.4. Protect federal property and functions.

7.4. Roles of the States. Under the Constitution, each state is responsible for protecting life and property within its boundaries. State and local governments use their civil forces to maintain law and order and quell civil disturbances.

7.5. Presidential Powers. The Constitution and federal statutes authorize the President to direct the use of armed federal troops within the 50 states, District of Columbia, Puerto Rico and US possessions and territories and their political subdivisions. The President also has the power to federalize the National Guard of any state to suppress rebellion and enforce laws.

7.5.1. Law. The President can also employ federal troops to ensure the execution of US law when a state opposes or obstructs US law or impedes the course of justice under those laws. The President can employ armed federal troops to suppress insurrection, domestic violence, unlawful assemblies and conspiracy. The key is, if such acts deprive the people of their constitutional rights or privileges and a state's civil authorities cannot or will not provide adequate protection, then employment of federal troops is authorized.

7.5.2. Property. The President may also choose to use armed federal troops to protect federal property and functions when the need for protection exists and local civil authorities cannot or will not give adequate protection. The US has a right to protect all federal property and functions regardless of their location.

7.5.3. Limits. While federal law authorizes domestic use of military force to suppress violence or insurrection, the Constitution and federal law provide certain restrictions. Under the *Posse Comitatus Act* neither active nor reserve personnel (USC, Title 10) may execute the law in place of duly appointed law enforcement officials without specific presidential or congressional approval and direction. The *Posse Comitatus Act* does not apply to the National Guard (USC, Title 32) until those personnel have been federalized.

7.6. Causes. Civil disturbances may arise from a number of causes. Most often they arise from political grievances, social unrest, terrorist acts or foreign influences. A single cause may trigger the event or it may arise from a combination of causes.

7.6.1. Political Grievances. Demonstrations of political grievances range from simple protests on specific issues to full-scale civil disobedience. Many forms of political protest, while disruptive, are not unlawful. These protests may be spontaneous, but most often are planned events. Often political protesters coordinate with local authorities. Most protesters are law-abiding citizens and intend for their protests to be nonviolent. Violence occurs mainly when control forces must try to contain a protest or arrest protesters involved in civil disobedience. The presence of agitators increases the chance of violence. Agitators want to provoke the control force into overreacting, which will embarrass the authorities. Violence and overreaction by the control force can also gain media and public sympathy for the protesters.

7.6.2. Social Unrest. Urban conflicts and community unrest arise from highly emotional socio-economic issues. Economically deprived inner-city residents may perceive themselves as being treated unjustly or ignored by the people in power. When tension is high, it takes only a minor incident or a rumor of an injustice to ignite a civil disturbance. This is particularly true if community relations with the local police are part of the problem.

7.6.3. Terrorist Acts/Foreign Influences. Many disaffected groups seek to embarrass the government. Disturbances may be a cover for terrorism. Often an overriding goal is to cause

an overreaction by authorities with the intent to gain sympathy from the general population. Foreign nations may employ surrogates. These surrogates create activities that promote the sponsor-state's interests. Agents of the foreign nations may be part of the disturbances and can be in key leadership positions. If the agents can get the targeted government to overreact, then the repression serves to further expand support for the foreign influence.

7.7. Locations. Civil disturbances usually occur at places symbolic of a grievance, near the cause of the grievance or close at hand to an aggrieved crowd. Examples of such places are nuclear weapons facilities or power plants, in urban areas, at refugee camps or at government facilities. Nuclear weapons facilities and power plants are subject to demonstrations by anti-nuclear activists. These activists demonstrate at places they know or believe develop, build, transport or store nuclear weapons, weapons-grade (nuclear) material or their components.

7.7.1. Government Facilities. US government facilities such as recruiting offices, federally leased buildings, Reserve Officer Training Corps (ROTC) buildings and federal courthouses can also be the targets of demonstrations. A group may target a government facility simply because they attach a symbolic value to it or perceive a connection between it and the policy they are protesting. This is especially true of anti-war and anti-nuclear protest groups. They may choose a facility because they see it as the source of their grievance. Likewise, they may target a facility because people working there are seen as having the power to address the group's grievance.

7.7.2. Refugee Camps. Refugee and resettlement camps can become the focus of a civil disturbance. Large numbers of refugees attempting to enter the US in mass are often placed temporarily in refugee camps until they can be resettled. These camps can either be in the US, a US-controlled area like Guantanamo Bay or in friendly allied nations. Regardless of the location, resettlement can be a slow and difficult process. The boredom, frustration and uncertainty refugees experience in these camps can create tensions that may erupt into violence. Agitators may infiltrate refugee camps to exploit these tensions in ways to embarrass and/or force the US into action.

7.7.3. Other Demonstration Sites. Demonstrations at US government facilities are not limited to those in the US. US facilities in foreign nations can be locations of civil disturbances. DoD installations, US embassies and US consulates in foreign nations are favorite targets of demonstrators. DoD installations in foreign nations are often scenes of protest against US foreign policy. The actual installation and its mission may or may not be the true target. Often the installation is just a highly visible symbol of the US government.

7.8. Role of Military Forces. The preservation of law and order in the civilian community is the responsibility of state and local governments and law enforcement authorities. The preservation of law and order on the federal property of a military installation is the responsibility of the installation commander and military law enforcement authorities.

7.8.1. Scope. Within the Air Force, the Security Forces act as the primary control force for civil disturbances that occur on Air Force installations. Under certain circumstances, Security Forces personnel may also act as the control force for civil disturbances that occur in the local community, if called upon by competent authority. Additionally, Security Forces may act as the control forces for any migrant or refugee operations when directed by command authorities. Requests for military support to civilian law enforcement officials in connection with civil disturbances will be addressed in accordance with AFI 10-802, *Military*

Support to Civil Authorities, Department of Defense Directive (DoDD) 3025.12, *Military Assistance for Civil Disturbances*, and DoDD 3025.18 *Defense Support of Civil Authorities*.

7.8.2. Responsibilities. Regardless of the nature of the disturbance, Security Forces personnel must display fair and impartial treatment during all contacts with the civilian population and any other participants in any civil disturbance. In all cases, personnel must adhere to the principle of minimum force as outlined in AFI 31-207, *Arming and Use of Force by Air Force Personnel*. Whenever possible, have civilian police apprehend, process, and detain civil law violators. Security forces perform these functions only when necessary and only to the minimum extent required. Return these functions to civil authorities as soon as possible. As the disturbance subsides, the commander should take steps to restore control to civil authorities. The control force gradually reduces the number and scope of its operations and should begin removing equipment from the area. Caution is required. Past experience has shown that rapid and complete withdrawal of military forces creates a dangerous vacuum. The vacuum often causes the disturbance to flare up since protesters believe civil authorities cannot maintain control. The security forces goal should be a phased return of control to civil authorities.

7.9. Levels of Disturbances. In most cases, crowd behavior escalates through many stages before violence erupts. When personnel can recognize key aspects of each stage, they have the best chance to control or disperse the crowd before it gets violent. The most recognizable stages are listed below with essential components of each stage identified.

7.9.1. Periods of Increased Tension. There are many indications that a base or community is in a period of increased tension as far as human relations are concerned. Identifiers marking this phase may appear as increased polarization in living, dining and work areas. Graffiti on walls or overheard conversations may indicate periods of increased tension. The biggest mistake at this stage is an overreaction to these situations by civil or military authorities. Block watch or community meetings are solid avenues to reduce tensions, air grievances and establish understanding.

7.9.2. Scattered Minor Incidents of Violence. This phase may include incidents of harassment between individual members of opposing groups. Increase first-line supervision and community policing in high-incident areas to avoid escalation.

7.9.3. Group-Oriented Violence. Roaming, unorganized groups bent on either destruction of property or assaults on people begin to show up with greater frequency and in larger groups. Leaders of these groups intentionally defy orders and authority. This is the first level of actual disturbance requiring direct police action. Riot control forces should assemble early in this phase, deploy to the scene and employ necessary measures (including force) to maintain order. Attempt to isolate and/or apprehend leaders and agitators. Use command action to stabilize the situation without force, if possible.

7.9.4. Full Riot Phase. Riots include widespread destruction of property, total defiance of authority, open mob action and serious breaches of the peace. This level could result in serious injury or death to innocent persons. At this time, a full civil disturbance operation should already be in force and the mission becomes one of mob dispersal and restoration of order as rapidly as possible. It is best to apprehend individuals after the mob is broken into small groups.

7.9.5. Summary. These levels of confrontation do not necessarily occur in order. Any phase could occur at any time and more than one phase could occur at the same time at different locations on the base or in the local community. A peaceful, orderly demonstration outside one gate could occur while others demonstrating for the same cause could be uncooperative and violating the law at a different gate.

7.10. The Participants

7.10.1. The Environment. A civil disturbance occurs only in a particular environment--that environment is a fusing of cause, place and willing confrontational participants. Civil disturbance participants come from all backgrounds. Participants cover the broad spectrum from the far right to the far left. Participants may be members of special interest groups, disgruntled or unemployed persons. They may be environmentalists, anti-nuclear agitators, anti-abortion activists or foreign and domestic opponents of US policy. They come from all age groups and from all socioeconomic classes. Civil disturbance participants may be curious onlookers who have become swept away by the excitement of an event or demonstrators or counter demonstrators who have become emotional about their cause. Whoever they are, they have become subject to the social and psychological factors that can turn a large gathering of people into a disruptive, disorderly mob. Understanding these factors can help reduce disturbances and permit restoration of order with a minimum of force.

7.10.2. The Human Factor. The basic human element sparking a disturbance is the presence of a crowd. There are almost as many types of crowds as there are reasons for people to assemble. There are casual crowds like those that assemble for a football game or gathers at an accident. Persons in such a crowd probably have no common bonds other than the enjoyment of the game or curiosity about the accident. There are "planned" crowds that assemble at the call of a leader to accomplish a goal. Members of a planned crowd have common bonds of interest and purpose.

7.10.3. Impact of Social Factors on a Crowd. The presence or absence of social factors like leadership, moral beliefs and social uniformity affect crowd behavior. Psychological factors also impact crowd behaviors. Typically a crowd only does those things that the majority of its members want to do. However, the emotional stimulus and protection of being in a crowd (anonymity) can lead to a violent synergy that individuals typically avoid. This dynamic, coupled with the fact that a crowd is open to manipulation, is what makes a crowd particularly volatile and a threat to public order.

7.10.3.1. Leadership. Crowd situations are ripe with confusion and uncertainty. Members seek direction. The first person to give orders in an authoritative manner is likely to be followed. A skillful manipulator can channel the energy of a crowd toward violence or calmness. In riot situations, target the group leadership at the early stages for apprehension. Leaderless crowds are much easier to disperse.

7.10.4. Emotional Contagion. Emotional contagion, a high state of excitement, provides the crowd psychological unity. Although temporary, this unity or contagion may be the only momentum a crowd needs to turn to mob action. Mob behavior is highly emotional, often unreasonable and always potentially violent.

7.10.5. Panic. Panic prompts unreasoning and frantic efforts in seeking safety. It is extremely contagious, spreads rapidly and endangers everyone in the area of the panicked crowd. Common panic scenarios include perceptions like:

7.10.5.1. Danger is so close at hand that the only action is to flee.

7.10.5.2. Escape routes are limited, blocked or have just been opened. Very often this form of panic causes people to stampede. The onslaught of a fleeing human mass may result in people being crushed, smothered or trampled.

7.10.5.3. Riot control agents have been used; crowd members cannot disperse quickly and therefore believe their lives are at risk.

7.10.6. These scenarios point to a critical concept in crowd control operations: Unless the mission is to contain and capture, always provide a number of open, easily identifiable escape routes that a crowd may access at any time.

7.11. Control Force Social Factors.

7.11.1. It is critical to remember that control force members are also susceptible to crowd behaviors--particularly panic. Do not allow control force members to develop a feeling of anonymity. Helpful measures include:

7.11.1.1. Leadership elements must know their people's names and use them at every opportunity.

7.11.1.2. Personnel with questionable emotional stability or strong prejudices (particularly against the crowd being controlled) should not participate in operations.

7.11.1.3. Do not dehumanize or depersonalize the crowd. It is easier to harm or fight an idea than a person. Fair and impartial performance of control force duties is imperative.

7.11.1.4. Maintain a gender, ethnic and racial balance to offset the perception of a disturbance being an "us" versus "them" situation. Mob leaders often count on sympathy generated from the appearance of an overwhelming military force "attacking" old people, women and children.

7.11.2. Rigorous training, effective supervision and immediate corrective action of control force members are an absolute requirement during civil disturbance operations. The fundamental fact is all members of a control force are accountable for all of their actions.

7.12. Crowd Tactics. In civil disturbance situations, crowd tactics run the full spectrum. Typically, the more organized a demonstration is, the more likely personnel will confront well-planned tactics. Keep in mind the underlying purpose for most tactics is to make the authorities, including the control force, look bad. The perception of a heavy-handed response may add support to the protest, escalate demonstrator acts (more violence) or serve to justify (in the minds of the crowd) outright acts of terrorism. This is why each and every member of the control force must maintain a calm, professional demeanor--regardless of the tactics.

7.12.1. Nonviolent Tactics.

7.12.1.1. Nonviolent tactics may range from name-calling to building barricades. Demonstrators may converse with the control force members to distract, dissuade or gain

their sympathy. Do not respond to verbal barrages. “Civil disobedience” is the most common nonviolent tactic. Examples include:

7.12.1.1.1. Trespassing--requiring control force apprehensions. Dissidents often view being apprehended as a “victory” and stage tactics to force mass apprehensions in an attempt to saturate the support functions behind control force units.

7.12.1.1.2. Passive resistance--blocking entrances, driveways, and offices--and then going limp, thus requiring control force members to carry protesters away.

7.12.1.1.3. Chaining, handcuffing or tying themselves together and/or to an object associated with the authorities (e.g. an aircraft, door, fence, or building).

7.12.1.2. Sometimes women, children and the elderly are placed in the front ranks. Consider this real-world example: Mob planners prearranged media coverage. Their plan was to use only female demonstrators in acts of civil disobedience. An astute installation commander deployed only female Security Forces and augmentees in blues, with no weapons or utility belts. The Security Forces women effectively worked in pairs to carry away the passive female demonstrators who had staged a sit-in across the main gate thoroughfare. The image of Battle Dress Uniform-riot-clad Security Forces males removing these protesters never materialized. Result: The media blitz turned against the protesters--commending the restraint and professionalism displayed by the United States Air Force! Again, adapt a firm but impartial demeanor when and if personnel must apprehend protesters.

7.12.1.3. Another common tactic (mentioned above) is to attempt to overwhelm the system by staging groups for mass apprehensions. Consider how best to process violators:

7.12.1.3.1. In mass, all receive the same process.

7.12.1.3.2. Selectively--process and turn over to civil authorities the leaders, agitators and repeat offenders while all others receive a debarment/expulsion letter.

7.12.1.3.3. Hold, identify and turn over to civil authorities.

7.12.1.3.4. The processing procedures will vary depending on each situation. Preplanning for this phase of the contingency among civil authorities, the installation commander, judge advocate and Security Forces is critical.

7.12.2. Violent Tactics.

7.12.2.1. A violent mob is potentially one of the most dangerous threats Security Forces will ever face. Violent mobs are notorious for firebombing, brick throwing and breaking into and entering secured facilities. Here are some less known, but just as deadly, tactics and weapons:

7.12.2.1.1. Balloons filled with paint to use as “bombs” on aircraft, buildings or control force members.

7.12.2.1.2. Bolt cutters to cut through fences.

7.12.2.1.3. Clubs disguised to look like protest signs.

7.12.2.1.4. Lead pipes wrapped in newspaper to use as clubs or be thrown as deadly missiles.

7.12.2.1.5. Firecrackers dipped in glue and covered with BBs or small nails to use as miniature shrapnel grenades.

7.12.2.1.6. Plywood shields and motorcycle helmets to protect against riot batons.

7.12.2.1.7. Goggles to protect against smoke and gas.

7.12.2.1.8. Ropes, chains, and grappling hooks to pull down fences. Mattresses, furniture pads or heavy blankets to lie on top of barbed wire during breaching (trespass) movements.

7.12.2.1.9. Firearms, explosives and vehicle assaults (using vehicles to crash a gate, etc.) are the most extreme forms of crowd violence.

7.12.2.2. Control force members disrupt a mob's desired activity which makes the control force the mob's most immediate target and threat. Controlled, measured responses will ultimately subdue any crowd. Control force members who get out of hand will only fuel and potentially escalate violence.

7.13. Civil Disturbance Training. Crowd control situations, particularly those with a potential for violence, are best handled by a combination of planning and training. It is too late to train once a crisis begins. As discussed earlier, given the out-of-mission role, coupled with the specialization required for civil disturbance operations, just-in-time (JIT) training may be the most effective and efficient course of action, if time allows. Lessons learned from several civil disturbance operations praised this training methodology. Solid training, both JIT and annual sustainment, remains the best avenue to prepare security forces for any contingency. Accurate information is the basis for appropriate training. Unit-level trainers should utilize the Confrontation Management curriculum located in the eTTPG Library located on the Air Force Security Forces Center website. The library is at <https://afsfmil.jackland.af.mil>, on the left column, click 'eTTPGs'.

7.13.1. Generic Unit Training. Because we cannot train for every specific civil disturbance, Security Forces should conduct some generic training which can cover different situations. Critical to any security forces operation is fitness for duty consideration. DFCs must accurately plan, organize and equip personnel who will deploy, whether to the front gate or around the world. Two absolutes, regardless of the mission, are:

7.13.1.1. Appropriate selection and training for deployment teams are critical to proper mission preparation.

7.13.1.2. Tailoring of the deployed UTCs logistics detail for the specific deployment to ensure the proper equipment is taken to complete the mission. In the near future, capability kits will be completed and propositioned at various locations to assist with these types of deployments.

7.13.2. Domestic Civil Disturbance Training.

7.13.2.1. Selection of the control force should draw on the unit's most stable personnel. Training should always emphasize tactics designed to present a disciplined show of force. Design training to examine the degrees of force to use and priority of each. Every control

force member must realize they are responsible for their actions while performing civil disturbance duties. Following the guidelines that established in AFI 31-207, *Arming and Use of Force by Air Force Personnel*, is critical to the outcome of any situation. Much of the training conducted for Security Forces has direct application in the realm of civil disturbance operations. Continually teaching and evaluating these topics should provide positive benefits when, and if, Security Forces employ troops in civil disturbance missions:

- 7.13.2.1.1. Arming and use of force.
 - 7.13.2.1.2. Unarmed self-defense.
 - 7.13.2.1.3. Use of riot control agents and munitions.
 - 7.13.2.1.4. Human relations and stress management.
 - 7.13.2.1.5. Dealing with panic.
 - 7.13.2.1.6. Weapons retention for the M-9, M-4 and M-870.
- 7.13.2.2. Specialized civil disturbance topics ideal for JIT training include:
- 7.13.2.2.1. Civil disturbance mission orientation and intelligence briefing.
 - 7.13.2.2.2. Crowd control tactics.
 - 7.13.2.2.3. Formations and movements.
 - 7.13.2.2.4. Use of the baton and other nonlethal weapons.
 - 7.13.2.2.5. **(Rapid)** Flexi-cuffing.
 - 7.13.2.2.6. The military working dog (MWD) in a civil disturbance environment.
 - 7.13.2.2.7. Transporting large numbers of apprehended personnel.
 - 7.13.2.2.8. Processing large numbers of apprehended personnel. **NOTE:** The above list is not all-inclusive; therefore, commanders must adapt training to the local environment.
- 7.13.3. Foreign Civil Disturbance Training. Clearly, a foreign civil disturbance mission requires more specialized JIT training in addition to the above-listed topics. Often an in-place country team will conduct this training. These missions require an especially stable, properly selected control force. Experience shows tours beyond 120 days induce considerable stress--even for the best prepared. Third world nations rife with poverty, disease and different customs add to an already stressful environment. Again, training should always emphasize a disciplined show of force, subject to the government, organization or individual in charge (e.g., UN, US State Department, US ambassador). Additional JIT training topics include:
- 7.13.3.1. Intelligence briefing.
 - 7.13.3.2. SJA briefing.
 - 7.13.3.2.1. Cultural orientation--we need to overcome cultural barriers by learning about the nation/ culture we're deployed to and make efforts to share our culture with them. Often, simple things are overlooked.

7.13.3.2.2. Morale strategies for US personnel and dissidents (particularly useful in migrant, internment and relocation camps).

7.13.3.2.3. . Rumor control plan--for BOTH the control force and dissidents.

7.13.3.2.4. . Control forces escape, evasion, recovery and reconstitution plans--should mob violence get out of hand or become life threatening to the control force.

7.14. Information Needs. Regardless of the home station or deployment location, accurate and timely information is the key to developing effective civil disturbance training plans. Process raw data and feed it up the chain of command. Analyze information and flow it back down the chain to those who need it the most--control force members. The information focus must assess the social, economic and political climate of the area and determine the likelihood of active participation or support from the local populace. Federal law has strict limitations on the armed forces collecting, storing or disseminating personal data on US citizens. The control force commander should coordinate with civil and military attorneys throughout any operation.

7.15. Threat Analysis. Threat information is the most vital information force planners have when determining appropriate countermeasures. Threat information constantly changes and must be reviewed on a consistent basis. Procedures need to be established for gathering, analyzing, and disseminating this information in a timely fashion, both up and down the chain of command, this will help determine the appropriate countermeasures and guard against overreaction. Three kinds of information produce a threat analysis:

7.15.1. Intelligence and criminal. Provide information on the goals, methods of operation, techniques, strategies, tactics and targets of individuals or groups.

7.15.2. Threat. This information identifies and defines individuals and groups.

7.15.3. Vulnerability. This information focuses on security weaknesses and high-risk targets (e.g. military installations, utility plants, dams or dike works). To assess the vulnerability of the installation, consider:

7.15.3.1. Installation and surrounding community characteristics that would make an attractive target for terrorists or civil disturbance (e.g., nuclear mission, research and development facilities, antiterrorism units, unique training missions).

7.15.3.2. Status of training. Readiness can be a powerful deterrent.

7.15.3.3. Communications availability/vulnerability.

7.15.3.4. Nonmilitary law enforcement resources.

7.15.3.5. Time and distance from other US military installations that could provide support.

7.15.3.6. Time and distance from urban areas. Large urban areas offer choice targets; ease of infiltration, concealment and escape; and large concentrations of ethnic populations that may be sympathetic to a particular cause.

7.15.3.7. Geographic region and proximity to foreign borders.

7.15.3.8. Access to the installation or community--power grids, fuel depots and pipelines.

7.15.3.9. Population density of the installation or community.

7.15.3.10. Terrain.

7.15.3.11. Weather.

7.16. Operations

7.16.1. Restore Order. Security Forces must isolate any civil disturbance threatening military order and prevent the disturbance from spreading. Security Forces protect people, facilities and services. Mob demonstrators usually view control force members as defenders of the “status quo” and thereby consider them targets. Above all, the control force mission is to provide disciplined restraint to maintain law and order. The nature of control force operations can vary greatly. Adopt operational strategies from AFH 31-305, *Security Police Deployment Planning Handbook*. Use this manual to prepare specific mission plans.

7.16.2. Isolate the Disturbance.

7.16.2.1. The initial control task is to isolate the crowd and seal off the disturbance area. Once isolated, time becomes the commander’s ally. To achieve this end, initiate measures to:

7.16.2.1.1. Prevent disorder from spreading to unaffected areas.

7.16.2.1.2. Move uninvolved people from the area immediately.

7.16.2.1.3. Prevent unauthorized people from entering the disturbance area.

7.16.2.1.4. Apprehend disturbance leaders/agitators.

7.16.2.2. Once the four control measures above are in place, allow the crowd to disperse peacefully. Isolate the affected area much the same as we do restricted areas: use signs, barriers and mobile patrols. Apprehend individuals in the mob who refuse to leave immediately and remove them from the area so they cannot reorganize or rekindle the crowd into an unruly mob.

7.16.3. Protect Targets. In most civil disturbance missions, Security Forces will be assigned to protect “targets” from the crowd. Targets include people and facilities. Adapt procedures from AFI 31-101, *Integrated Defense* and DOD S-5210.41-M_AFMAN 31-108V1, *Nuclear Weapon Security Manual: The Air Force Nuclear Weapon Security Manual*, to fulfill this aspect of the mission.

7.16.4. Crowd Control.

7.16.4.1. The control force uses carefully selected tactics and wisely committed resources to exert control over disorderly crowds. Installation/operation commanders have four basic options available to them. Their order can be to monitor, disperse, contain or block the crowd. Implement these options alone or in combination. Variables that might influence the tactic(s) applied include:

7.16.4.1.1. Severity of the disturbance.

7.16.4.1.2. Public opinion.

7.16.4.1.3. Current policies.

7.16.4.1.4. Crowd demographics (mood, intent, composition and activity).

7.16.4.1.5. Capabilities and preparedness of control forces.

7.16.4.1.6. Immediate and long-term benefits of control force action.

7.16.4.1.7. Weather, terrain and time of day.

7.16.4.2. Monitor.

7.16.4.2.1. Monitoring does not antagonize peaceful gatherings and is appropriate when more decisive action is inappropriate. Monitoring is particularly useful in large, non-violent demonstrations. This is also an ideal stage to meet demonstration leaders, determine their intent and gain their cooperation. Contact with the leadership may be the only control measure needed, persuading leaders to police (literally) their own gathering. Planned demonstrations usually require coordination of the following options:

7.16.4.2.1.1. Formal issuance of permits to march or demonstrate.

7.16.4.2.1.2. Planned starting point, route and rally point(s) for the demonstration.

7.16.4.2.1.3. Time schedule.

7.16.4.2.1.4. The need to marshal/escort the demonstration and which organization will provide personnel to serve as marshals.

7.16.4.2.1.5. Violence, litter and property damage prevention.

7.16.4.2.1.6. Personnel safety.

7.16.4.2.2. Assigning a member of the control force to photograph faces of crowd members is an extremely effective part of monitoring. When individuals in crowds realize they are being photographed, Security Forces neutralize the anonymity that adds to their brazenness. Crowd members need to see the photographer. The photographer needs to be in uniform. There should be no doubt in anyone's mind that individuals in the crowd are being photographed (still or video) by the control force. Ensure the safety of the photographer. Should the mob turn violent, photographic evidence can be remarkably beneficial.

7.16.4.3. Disperse.

7.16.4.3.1. The control force may disperse the crowd. Key to any dispersal operation is control and orderliness. An uncontrolled, fragmented crowd may actually spread violence and damage. Clearly inform the crowd of the requirement to disperse. Detail authorized egress routes. Maintain (likely) target countermeasures. Apprehend any small groups that resist or loiter in the area after dispersal. A hierarchy of dispersal options includes:

7.16.4.3.1.1. Violent, destructive confrontations. Format: Top (first resort) to bottom (last resort):

7.16.4.3.1.1.1. Monitor, release/read a proclamation "this *may* display a show of force."

7.16.4.3.1.1.2. Increase four-person and MWD patrols.

7.16.4.3.1.1.3. Employ crowd control formations.

7.16.4.3.1.1.4. Implement riot tactics.

7.16.4.3.1.1.5. Employ water cannon.

7.16.4.3.1.1.6. Employ chemical agents.

7.16.4.3.1.1.7. Employ lethal force.

7.16.4.3.2. Peaceful demonstrations. Adapt this hierarchy to specific situations.

7.16.4.4. Contain. Containment is a suitable option for keeping disorder from spreading and when the commander directs apprehensions. Vehicles, which are under the control of the on-scene commander, may be an excellent force multiplier. Used jointly with dismounted troops, the 33-ton crash (fire) trucks are a ready resource (known to be resoundingly successful) and have a tremendous psychological impact on mobs. Lights, sirens and public address systems on law enforcement vehicles—used judiciously—can aid containment efforts. When using vehicles in a containment operation, establishment of a mobile command post is recommended.

7.16.5. Block. Blocking may be necessary to protect specific targets in the path of an advancing crowd (e.g., keeping an unruly mob off the flight line to protect aircraft). Control force members on line or in vehicles are common barricades. Depending on the severity of the violence or threat, erect concertina wire, earthen-filled barrels or jersey barriers to counter higher level threats like speeding vehicles or mass breaches.

7.16.6. Serious Threats. Control forces may encounter high-level threats that pose grave danger to all persons in the area. These threats include hostage/barricade situations, snipers, bomb threats and fires. Immediate-action responses must be in place so control forces can minimize the tragedy caused by these events. Air Force security forces shall adapt the guidance from AFI 31-101 and DoD S-5210.41-M to effectively deal with serious threats. Fires offer unique challenges beyond the capabilities of most military control forces. The specialization required of firefighters precludes control forces from direct engagement. Control force members can help by remaining vigilant to the threat and reporting fires immediately. At a fire scene, military control force members may:

7.16.6.1. Establish a protective cordon around the firefighters' area of operations. The cordon should provide security for firefighters (sniper suppression) as well as hydrant and hose security.

7.16.6.2. Maintain observation posts (i.e. tall buildings) to prevent sniping, watch for other fires and coordinate the approach of responding units. Ensure Security Forces thoroughly coordinate posting control force members on top of buildings to preclude others from mistaking them as snipers.

7.16.6.3. Establish crowd and traffic control.

7.16.7. Riot Control Formations and Maneuvers. Information and training material on specific riot control techniques can be found in the Electronic Tactics, Techniques, & Procedures Guides (e-TTPGs) Library located on the Air Force Security Forces Center's web site. The library is at <https://afsfmil.lackland.af.mil> in the middle column under e-TTPGs.

Select “*Confrontation Management*” under the Nonlethal Weapons Section. A detailed study guide, lesson plan, and task performance checklist are available.

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

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

- AFPD 31-2**, *Air Provost Operations*, 10 Apr 2009
- AFCAT 21-209 V 1**, *Ground Munitions*, 9 Nov 2007
- AFMAN 33-363**, *Management of Records*, 1 March 2008
- AFMAN 10-2502**, *Air Force Incident Management System (AFIMS) Standards and Procedures*, 25 September 2009
- AFMAN 10-2504**, *Air Force Incident Management Guidance for Major Accidents and Natural Disasters*, 1 December 2009
- AFH 31-305**, *Security Forces Deployment Planning Handbook*, 26 February 2003
- AFI 10-802**, *Military Support to Civil Authorities*, 19 April 2002
- AFI 10-2501**, *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007
- AFI 31-101**, *Integrated Defense*, 8 October 2009
- AFI 31-201**, *Security Forces Standards and Procedures*, 30 March 2009
- AFI 31-202**, *Military Working Dog Program*, 16 May 2009
- AFI 31-206**, *Security Forces Investigations Program*, 16 September 2009
- AFI 13-207**, *Preventing and Resisting Aircraft Piracy (Hijacking)*, 21 June 2010
- AFI 31-207**, *Arming and Use of Force by Air Force Personnel*, 29 January 2009
- AFI 35-101**, *Public Affairs Responsibilities and Management*, 18 August 2010
- AFI 36-2226**, *Combat Arms Program*, 24 February 2009
- AFI 40-301**, *Family Advocacy*, 30 November 2009
- AFI 44-153**, *Traumatic Stress Response*, 31 March 2006
- AFI 44-154**, *Suicide and Violence Prevention, Education, and Training*, 2 January 2003
- AFI 51-201**, *Administration of Military Justice*, 21 Dec 2007
- AFI 51-701**, *Negotiating, Concluding, Reporting, and Maintaining International Agreements*, 6 May 1994
- AFI 71-101 Volume 1**, *Criminal Investigations*, 1 December 1999
- AFMAN 23-220**, *Reports Of Survey for Air Force Property*, 01 Jul 1996
- AFMAN 31-219**, *The USAF Military Working Dog Program*, 20 June 2009
- AFMAN 31-222**, *Use of Force Manual*, 18 February 2009
- AFMAN 31-229**, *USAF Weapons Handling Manual*, 12 May 2004

AFMAN 36-2227, Volume 1, *Combat Arms Training Programs, Individual Weapons*, 21 May 2004

AFPAM 44-160, *The Air Force Suicide Prevention Program*, 1 Apr 2001

AFTTP (I) 3-2.46, *Nuclear, Biological, And Chemical (NBC) Protection*, (2003)

FM 3-19.11, *Special Reaction Teams*, 13 May 2005

FM 4-02.18, *Veterinary Services Tactics, Techniques and Procedures*, 30 December 2004

FM 3-19.15, *Civil Disturbances*, 18 April 2005

DoDD 3025.12, *Military Assistance for Civil Disturbances*, 4 February 1994

DoDD 3025.18, *Defense Support of Civil Authorities*, 29 December 2010

DoD 3150.8-M, *Nuclear Weapon Accident Response Procedures (NARP)*, 22 February 2005

DoDI 5200.08, *Security of DOD Installations and Resources*, 10 December 2005

DoD S-5210.41-M_AFMAN 31-108V1, (S) *Nuclear Weapon Security Manual (U): The Air Force Nuclear Weapon Security Manual*, 1 February 2010.

DoD 0-2000-12-H, *DoD Anti-Terrorism Handbook*, 1 February 2004

DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*. 7 January 1980

DoDD 5210.56, *Use of Deadly Force and the Carrying of Firearms by DoD personnel Engage in Law Enforcement and Security Duties*, 1 April 2011

DoD 5400.7-R_AFMAN 33-302, *DoD Freedom of Information Act Program*, 21 October 2010

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

DoDD 7730.47, *Defense Incident-Based Reporting System (DIBRS)*, 15 Oct 1996

DoDI 1030.02, *Victim and Witness Assistance Procedures*, 4 Jun 2004

DoDI 5525.07, *Implementation of Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigative and Prosecution of Certain Crimes*, 18 June 2007

FM 3-19.15, *Civil Disturbance Operations*, April 2005

5 USC §552: *Public information; agency rules, opinions, orders, records, and proceedings*

18 U.S.C. § 1385: *Use of Army and Air Force as posse comitatus*

50 U.S.C. **Chapter 36** — FOREIGN INTELLIGENCE SURVEILLANCE

Homeland Security Presidential Directive-5, 28 February 2003

Air Transportation Security Act of 1974; Public Law 93-366.

CEMP 10-2, *Major Accidents, Natural Disasters, Enemy CBRNE Attacks & Terrorist Use of CBRNE*

Adopted Forms

AF 53, *Security Forces Desk Blotter*, 1 Dec 2000

AF Form 1098, *Special Task Certification and Recurring Training*, 1 Apr 1985

AF Form 1109, *Visitor Register Log*, 1 May 1999

AF Form 1314, *Firearms Registration*, 19 Oct 2005

AF Form 3545, *Incident Report*, 11 May 2005

AF Form 847, *Recommendation for Change of Publication*, 22 Sep 2009

DD Form 2701, *Initial Information for Victims and Witnesses of a Crime*, May 2004

Abbreviations and Acronyms

ACOG—Advanced Combat Optic Gunsight

ADM—Advanced Designated Marksman

AFB—Air Force Base

AFI—Air Force Instruction

AFCESA—Air Force Civil Engineering Support Agency

AFIMS—Air Force Incident Management System

AF—JLLIS-Air Force – Joint Lessons Learned Information System

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFRIMS—Air Force Records Information Management System

AFSFC—Air Force Security Forces Center

AFSWC—Air Force Service Watch Cell

AT—Antiterrorism

ATO—Antiterrorism Officer

ATP—Antiterrorism Plan

BDOC/ECC—Base Defense Operations Center/Emergency Communication Center

CBRNE—Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive

CCA—Contamination Control Area

CDC—Center for Diseases Control

CEMP—Comprehensive Emergency Management Plan

CISD—Critical Incident Stress Debriefing

CINC—Commander in Chief

CNT—Crisis Negotiation Team

CPEC—Close Precision Engagement Course

DARE—Drug Abuse Resistance and Education

DC—Decontamination Corridor
DCG—Disaster Control Group
DFC—Defense Force Commander
DHS—Department of Homeland Security
DL—Decontamination Line
DM—Designated Marksman
DoD—Department of Defense
DoJ—Department of Justice
DoS—Department of State
DRF—Disaster Response Force
ECP—Entry Control Point
EM—Emergency Management
EOC—Emergency Operations Center
EOD—Explosive Ordnance Disposal
ESF—Emergency Support Function
EST—Emergency Services Team
eTTPGs—Electronic Tactics, Techniques, & Procedures Guides
FAA—Federal Aviation Administration
FBI—Federal Bureau of Investigations
FC—Fire Chief
FEMA—Federal Emergency Management Agency
FES—Fire and Emergency Services
FOIA—Freedom of Information Act
FPCON—Force Protection Condition
HAZMAT—Hazardous Material
HE—High Explosive
HNT—Hostage Negotiation Team
HSPD—Homeland Security Presidential Directive
HTA—High Threat Areas
IC—Incident Commander
ICC—Installation Control Center
ICP—Incident Command Post

IDP—Integrated Defense Plan
IFAK—Individual First Aid Kits
IOTV—Improved Outer Tactical Vest
IPE—Individual Protective Equipment
IRB—Initial Response Base
JOC—Joint Operations Center
LEA—Law Enforcement Agency
LRS—Logistics Readiness Squadron
MAJCOM—Major Command
MOA—Memorandum of Agreement
MRE—Meals-Ready-to-Eat
MTA—Medium Threat Areas
MTF—Medical Treatment Facility
MTT—Mobile Training Team
MWD—Military Working Dog
NARP—Nuclear Weapon Accident Response Procedures
NBC—Nuclear, Biological, and Chemical
NCO—Non-Commissioned Officer
NCOIC—Non-Commissioned Officer in Charge
NDA—National Defense Area
NIMS—National Incident Management System
OPCON—Operational Control
OpsSC—Operations Section Chief
OPR—Office of Primary Responsibility
OSC—On-scene commander
PA—Public Affairs
PAO—Public Affairs Officer
PL—Protection Level
PPE—Personal Protective Equipment
RDS—Records Disposition Schedule
ROTC—Reserve Officer Training Corps
RTF—Response Task Force

SAC—Special Agent in Charge

SAR—Suspicious Activity Reports

SF—Security Forces

SFLEO—Senior Federal Law Enforcement Official

SRT—Special Reaction Team

SJA—Staff Judge Advocate

SWAT—Special Weapons and Tactics

TACON—Tactical Control

TSR—Trauma Stress Response

TTP—Tactics, Techniques, and Procedures

USC—United States Code

UTC—Unit Type Code

Attachment 2

CATEGORIES OF SUSPICIOUS ACTIVITY

A2.1. ACQUISITION OF EXPERTISE. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A2.2. BREACH OR ATTEMPTED INTRUSION. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (e.g., police, security, or janitorial personnel).

A2.3. ELICITING INFORMATION. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

A2.4. EXPRESSED OR IMPLIED THREAT. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

A2.5. FLYOVER OR LANDING. Suspicious overflight of or landing near a DoD facility or infrastructure by any type of flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).

A2.6. MATERIALS ACQUISITION OR STORAGE. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

A2.7. MISREPRESENTATION. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

A2.8. RECRUITING. Building operations teams and developing contacts, or collecting personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A2.9. SABOTAGE, TAMPERING, OR VANDALISM. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A2.10. SURVEILLANCE. Monitoring the activity of DoD personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A2.11. TESTING OF SECURITY. A challenge to or a series of interactions with DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities or vulnerabilities.

A2.12. THEFT, LOSS, OR DIVERSION. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents, whether classified or unclassified) that are proprietary to the facility, or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

A2.13. WEAPONS DISCOVERY. Discovery of weapons or explosives, as defined in section 930 of title 18, U.S.C. (Reference (n)). The discovery of personal weapons legally owned by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity if the discovery is solely the result of the owner's failure to properly store or secure the weapon(s).

Attachment 3

BEHAVIORAL THREAT INDICATORS

A3.1. Foreword. This list is a compilation of behavioral threat indicators derived from multiple credible open source documents from various DoD, DoS, DoJ, State and University studies or directives. NOTE: Not all indicators are independently actionable, but when put to together or demonstrated in conjunction with one another, they could indicate a threat.

A3.2. Overt Indicators - Preparations/Activities.

A3.2.1. Indicators that May Demonstrate Intent.

A3.2.1.1. Talk knowingly about a future terrorist event, as though the person has inside information about what is going to happen.

A3.2.1.2. Statement of intent to commit or threatening to commit a terrorist act, whether serious or supposedly as a “joke,” and regardless of whether or not you think the person intends to carry out the action.

A3.2.1.3. Deliberate probing of security responses, such as deliberately causing a false alarm, faked accidental entry to an unauthorized area, or other suspicious activity designed to test security responses without prior authorization.

A3.2.1.4. Statements of support for suicide bombers who have attacked the United States or U.S. personnel or interests abroad.

A3.2.1.5. Expressing sympathy for violence promoting organizations.

A3.2.1.6. Advocating violence, the threat of violence, or use of force to achieve goals that are political, religious or ideological in nature.

A3.2.1.7. Advocating support for international terrorist organizations or objectives.

A3.2.1.8. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

A3.2.1.9. Knowing membership in, or attempt to conceal membership in, any group which: (1) advocates the use of force or violence to cause political change within the U.S., (2) has been identified as a front group for foreign interests, or (3) advocates loyalty to a foreign interest over loyalty to the U.S.

A3.2.1.10. Statements disparaging the United States in favor of an alternative system.

A3.2.1.11. Statements that the U.S. Government is trying to destroy or suppress people of a particular race, religion, or ethnicity (for example, statements that the U.S. Government is engaging in a crusade against a faith or destroying the purity of a culture or race).

A3.2.1.12. Distribution of extremist publications or posting information on the Internet, including e-mail and on-line discussions, which supports or encourages violence or other illegal activity. Frequent viewing of web sites that promote extremist or violent activity (unless this is part of one’s job or academic study).

A3.2.1.13. Advocating or participating in violence against any individual based on their race, creed, color, sexual orientation, religion, or national origin.

A3.2.1.14. Statements of support for violence against U.S. military forces either at home or deployed abroad.

A3.2.1.15. For U.S. military personnel only: Any action that advises, counsels, urges, or in any manner causes or attempts to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the armed forces of the United States.

A3.2.1.16. Expressing outrage against U.S. military operations.

A3.2.1.17. Seeking spiritual sanctioning for unlawful violence.

A3.2.2. Indicators that May Demonstrate Opportunity.

A3.2.2.1. Providing financial or other material support to a terrorist organization or to someone suspected of being a terrorist.

A3.2.2.2. Family ties to known or suspected international terrorist or terrorist supporters.

A3.2.3. Indicators that May Demonstrate Capability.

A3.2.3.1. Statements about having a bomb or biological or chemical weapon, about having or getting the materials to make such a device, or about learning how to make or use any such device—when this is unrelated to the person’s job duties.

A3.2.3.2. Suspicious overflight of and/or landing near a DoD facility or infrastructure by any type of (unauthorized) flying vehicle (e.g., airplane, helicopter, unmanned aerial vehicle, hang glider).

A3.3. Covert Indicators - Subversive Activities

A3.3.1. Elicitation and Data Collection.

A3.3.1.1. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

A3.3.1.2. Monitoring the activity of DoD personnel, facilities, processes, or systems, including showing unusual interest in a facility, infrastructure, or personnel (e.g., observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A3.3.1.3. Collection of unclassified information that might be useful to someone planning a terrorist attack, e.g., pipeline locations, airport control procedures, building plans, etc. when this is unrelated to the person’s job or other known interests.

A3.3.1.4. Inappropriate, Unusual, or Excessive Interest in Classified Information (*outside current assignment or without the “need to know”*).

A3.3.1.5. Mishandling of Classified Information to include revelations to unauthorized personnel, leaks to media, unauthorized contact with media, unauthorized removals, collecting or storing outside of approved facilities, lax security protocols.

A3.3.1.6. Misuse of computers/technology to include accessing databases without authorization, unauthorized searching or browsing through computer libraries, or unauthorized destruction of information or agency computer files (e.g. deleting data).

A3.3.1.7. Unexplained or excessive copying of files—particularly blueprints of buildings or systems such as security and fire suppression.

A3.3.2. Acquisition of Expertise.

A3.3.2.1. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities.

A3.3.3. Acquisition of Material/Resources.

A3.3.3.1. Acquisition of unusual quantities of precursor material (e.g., cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; and/or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

A3.3.3.2. Recruiting or building operations teams and contacts, personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A3.3.3.3. Theft or loss associated with a DoD facility or infrastructure (e.g., of badges, uniforms, identification cards, emergency vehicles, technology, or documents, whether classified or unclassified) that are proprietary to the facility, and/or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

A3.3.3.4. Handling, storing, or tracking hazardous materials in a manner that puts these materials at risk.

A3.3.4. Misrepresentation.

A3.3.4.1. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

A3.3.5. Criminal/Suspicious Activity.

A3.3.5.1. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, military members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

A3.3.5.2. Ominous, specific threats.

A3.3.5.3. Association with any of the following criminal precursors to terrorist activities: front businesses & charities, counterfeit money, counterfeit goods, narcotics, smuggling & import/export violations, robbery/theft, fraud (credit card, benefits, food stamps, etc), phone scams, bribery, immigration & identity crimes, or incitement to commit terrorist acts.

A3.3.6. Foreign Contact.

A3.3.6.1. Unreported contact with foreign intelligence services, governments, organizations, or unreported contact with unauthorized foreign personnel seeking classified information.

A3.3.6.2. Unreported personal foreign travel.

A3.4. General Risk for Violence Indicators.

A3.4.1. This list is a compilation of indicators derived from multiple sources that may indicate a higher risk for violence. If an individual demonstrates these indicators, this information should be shared up the chain of command and the commander or first sergeant should consider all the information to decide whether the individual should be referred to the appropriate helping agencies on base for further screening and/or evaluation by medical authorities. If the individual is demonstrating an immediate threat of violence, contact the appropriate law enforcement agencies. NOTE: Not all indicators are independently actionable, but when put together or demonstrated in conjunction with one another, could indicate a threat.

A3.4.1.1. Past conflicts (especially if violence was involved) with coworkers.

A3.4.1.2. Tendency to blame others for problems.

A3.4.1.3. Defensive or hostile attitude, increasing belligerence, or outbursts of anger.

A3.4.1.4. A history of frequent job changes.

A3.4.1.5. Hypersensitivity to criticism.

A3.4.1.6. Recent acquisition/fascination with weapons.

A3.4.1.7. Apparent obsession with a supervisor or coworker or employee grievance.

A3.4.1.8. Preoccupation with violent themes.

A3.4.1.9. Interest in recently publicized violent events.

A3.4.1.10. Extreme disorganization.

A3.4.1.11. Increased use of alcohol and/or illegal drugs.

A3.4.1.12. Noticeable decrease in attention to appearance and hygiene.

A3.4.1.13. Resistance and overreaction to changes in policy and procedures.

A3.4.1.14. Repeated violations of policies.

A3.4.1.15. Increased severe mood swings.

A3.4.1.16. Noticeably unstable, emotional responses.

A3.4.1.17. Explosive outbursts of anger or rage without provocation.

A3.4.1.18. Suicidal; comments about "putting things in order."

A3.4.1.19. Behavior which is suspect of paranoia, ("everybody is against me").

A3.4.1.20. Increasingly talks of problems at home.

- A3.4.1.21. Escalation/introduction of domestic problems into the workplace; talk of severe financial problems.
- A3.4.1.22. Talk of previous incidents of violence.
- A3.4.1.23. Empathy with individuals committing violence.
- A3.4.1.24. Increase in unsolicited comments about firearms, dangerous weapons, or violent crimes.
- A3.4.1.25. Patterns of inaccurate statements or making excuses for irregular behaviors.
- A3.4.1.26. Excessive tardiness or absences - Beyond simply missing work; an employee may also reduce his or her workday by leaving early, departing the work site without authorization, or presenting numerous excuses for otherwise shortening the workday.
- A3.4.1.27. Increased need for supervision; reduced productivity; inconsistent work patterns.
- A3.4.1.28. Blames others for problems in life or work; suspicious, holds grudges.
- A3.4.1.29. Unwelcome obsessive romantic attention.
- A3.4.1.30. Unshakable depression as exhibited by low energy, little enthusiasm or despair.
- A3.4.1.31. Recently has withdrawn from normal activities, family, friends, co-workers; is isolated or a loner.
- A3.4.1.32. Feels wronged, humiliated, degraded; wants revenge.
- A3.4.1.33. Morally superior, self-righteous / feels entitled to special rights and that rules don't apply to him/her.
- A3.4.1.34. Demonstrating desperation over professional or personal problems.
- A3.4.1.35. Believes to have no choices or options for action except violence.
- A3.4.1.36. A history of drug or alcohol abuse.
- A3.4.1.37. Past convictions for violent crime.

Attachment 4
SAMPLE MOA

Memorandum of Agreement Between Local County Sheriff's Office (or Local Police Department) and the XXX Security Forces Squadron

1. PURPOSE: The purpose of this agreement is to outline responsibilities, and define major actions required to support confrontation management and emergency services situations occurring on XXX Air Force Base.

2. AUTHORITY: DoDI 5200.08 and 31-101, XAFB (Installation Security Plan)

3. GENERAL:

a. SCOPE: This provides guidance and outlines tasking necessary to maintain an acceptable level of security for the XXX AFB community and resources. During the implementation of Force Protection Conditions (FPCON) and security contingencies, the Local County Sheriff's Office may be asked to render support in the form of personnel and emergency services.

b. ASSUMPTIONS: Neighboring military installation will be contacted and may render limited aid under emergency situations. The use of the XXX County Sheriff's Office is understood to be only a contingency measures until a federal agency can respond to handle the emergency situation.

c. FRIENDLY FORCES: The XXX Wing Commander will be in operational control of all forces unless relieved by a Federal agency (FBI, ATF, U.S. Marshals, etc.). There is no legal impediment to civilian law enforcement providing assistance where required; however local law enforcement officers are deployed in support of, not in place of, Security Forces or other federal agencies. Local law enforcement will be relieved when appropriate federal resources are in place.

4. RESPONSIBILITIES: Local County Sheriff's Office – Phone (000) 000-0000, will be notified by a member of the XXX Security Forces Squadron with a request for assistance. The Local County Sheriff's Office will provide an estimated time of arrival to a designated safe staging area for the incident. The Local County Sheriff's Office will respond to the incident as soon as possible. The XXX Security Forces Squadron and Local County Sheriff's Office will conduct an exercise of this agreement annually.

a. OPERATIONAL ASSISTANCE: The Local County Sheriff's Office may be requested to provide law enforcement assistance for a crowd confrontation team, civil disturbances, law enforcement emergencies, large protest demonstrations, aircraft disasters, boating or watercraft disasters, fires, hurricanes, tornadoes or other weather related crisis, sporting events, concerts, parades, escapes from detention facilities, and incidents requiring utilization of specialized units capable of responding within two hours to assist with public disturbances beyond control of XXX Security Forces Squadron.

b. SPECIAL WEAPONS AND TACTICS TEAM: The Local County Sheriff's Office will be asked to provide S.W.A.T. capabilities with Support vehicle as quickly as circumstances permit for serious situations beyond XXX Security Forces Squadron capabilities involving

armed intervention.

5. COMMAND AND CONTROL: Due to federal requirements, the XXX ABW/CC or their designated on-scene commander must exercise control over the actions of the S.W.A.T. team. Specifically, before any use of force by the team, the Air Force on-scene commander must grant permission.

6. AGREEMENT AND ADMINISTRATION: This MOA becomes effective immediately on signature by all parties. It will be reviewed annually. It may be revised, cancelled, or rescinded in total on 60-day written notification by either party.

7. LIABILITY: This MOA will address liability issues specific to the installation and the jurisdiction it lies within.

Signature Block
Sheriff of Local County --or--
Chief of Police, Local Municipality

Signature Block
Wing Commander

NOTE: Add Wing Commander Signature Block if required. Separate MOU/MOA must be established with each agency SECURITY FORCES enters into agreement with.

Attachment 5

POSSIBLE SITUATIONS REGARDING ENFORCEMENT OF ORDER WITHIN OR NEAR AIR FORCE INSTALLATIONS

Table A5.1. Possible Situations Regarding Enforcement of Order Within or Near Air Force Installation

<u>Possible Situation</u>	<u>Action</u>
1. Notice of impending or actual demonstration.	Notify HQ USAF via Installation Command Post IAW AF or OSD directions. Coordinate with local United States Attorney and other appropriate civil authorities. Review and write installation anti demonstration plans. Notify MAJCOM/A7S.
2. Peaceful demonstration outside perimeter of installation without interference to USAF mission.	Ignore demonstrators while being alert to any change in status.
3. Demonstrators interfere with base operation to a minor degree, by obstructing traffic moving on- and off-base.	Use alternate means of access. If necessary ask civil authorities to remove the obstruction. NOTE: Commanders are reminded that request for USAF assistance by civil authorities should be routed through the appropriate command channels for approval before any action is taken.
4. Demonstrators cause serious interference with base operations and endanger USAF personnel or property.	SF should request assistance from civil authorities. If necessary, contact higher headquarters for instructions on the use of USAF resources. To protect USAF personnel and property, use the absolute minimum degree of force to restore order.
5. Demonstrators gain access to the installation proper.	Detain, issue a letter of Debarment IAW AFI 31-201, Chapter 5, Attachment 13, and escort them off-base. If necessary, ask local United States Marshals for assistance since they have the power of Federal arrest on United States government property.
6. After being ejected, demonstrators return or attempt to force their way into the installation.	SF should ask local federal and civil authorities to control the demonstrators. If this control is beyond their capability, the commander uses whatever means possible to protect government personnel and property. The guiding principle here should be a minimum application of a force consistent with the restoration of order.
NOTE: The guidance provided will be modified on a country by country basis in the overseas commands. International pact or bilateral agreements will provide local policy and guidance to handle civil disturbances and demonstrations.	