Testable Lectures
TECHNICAL TRAINING

SECURITY FORCES BASIC DEFENDER COURSE

37 TRANING WING

37 TRAINING GROUP

343 TRAINING SQUADRON

343 TRS/TRR

01 April 2025

DESIGNED FOR AETC COURSE USE

NOT INTENDED FOR USE ON THE JOB

Basic Defender Course - Fox Flow - New Course Flow CAO 24 Feb 2025						
DOT	**LOCATION**	**OBJECTIVE**	**DOT**	**LOCATION**	**OBJECTIVE**	
BLK 2	**SECURITY FORCES FUNDAMENTALS**		**25**	950	Participate in or Lead Progressive Physical Education (1.5) Pro Firing (7), Weapons Safety	
9	CTA	Participate in or Lead Progressive Physical Education ***Intro Ruck*** (2), Utilize Tac and Non Tac Comm Devices (2), Weapons Safety *Armory Procedures* (4)	**26**	CTA	Apply Concepts and Principles of UoF **(APP) (8),** Participate in or Lead Stress Drills (.25)	
10	CH	Participate in or Lead Progressive Physical Education (1.5), ***Lectures*** SF Mission, Vision & Mission Essential Tasks (1), Career Field History (2), SF Ethics/Mindset (1), Media/Social Media (.5), PRAP (.5), Lautenberg/Gun Control (.5), SF in Joint Enviornment (1)	**27**	CTA	Apply Concepts and Principles of UoF **(APP) (8),** Participate in or Lead Stress Drills (.25)	
11	CH	**Blues Inspection *Lectures*,** Military Authority & Jursidiction (2), Military Law (1), Apprehend a Subject (1.5), Transport Offender (.5), Suicide Prevention (1), Bloodborne Pathogens (1), Supervised Study (1)	**28**	CTA	Apply Concepts and Principles of UoF **(PC) (8), Participate in or Lead Stress Drills** (.25)	
12	CTA	Participate in or Lead Progressive Physical Education (1.5), Weapons Retention (6), Participate in or Lead Stress Drills (.25)	**29**	CH	***Gear Inspection*** Ops Sec Indicators (1), ID Concepts (1), Threats/Threat Levels (1), Terrorism (.5), Domestic Threats (.5), Insider Threats (.75), Near Peer Threats (1), FPCONs (.5), RAMs (.25), IDP (1)	
13	CH	Written Test #1 (2), Field Interview (1), Rights Advisement (1), Comm Etiquette (1), Interpersonal Skills (1), De-Escalate Conflict (2), Impaired Persons (1)	**30**	CH	***Lectures*** Incident Command (1), Emergency Action Plan (.5), Control Center Ops (.5), Search Areas/Barrier/Obstacle Plans (.5), Area Searches (.5), Bldg. Searches (.5), Crime Scenes (1), AF Fm 1109 (.5), CBRNE (.75), EAL (1), Escorted/Unescorted Entry (.75), Stop Check Pass (.5)	
14	950	Participate in or Lead Progressive Physical Education ***Ruck*** (1.5), Pro Firing M4/M18 (7), Weapons Safety	**31**	CH	***Lectures*** Installation Breach Procedures (1), Entry/Exit Point Checks (2), Alarmed Responses (1), Unauthorized Entry (.5), Duress (.5), Sign/Countersign (1), Building Checks (2)	
15	CLAB	Control Tactics (10)	**32**	CTA	***Lectures*** Entry/Exit Point Checks (2), Respond to Threat (2), React to Bomb Threat (2), ABGD/Resource Security Duties (2)	
16	CLAB	Control Tactics (10)	**33**	CTA	Entry/Exit Point Checks **(APP)** (3.5), Entry/Exit Point Checks **(PC)** (3.5), Respond to Threat (1.5), React to Bomb Threat (1.5)	
17	CLAB	Control Tactics (8)	**34**	CH/CTA	Written Test #2 (2), Participate in or Lead Progressive Physical Education *Ruck* (3.5) ***BLK Pass - 149.5 hrs***	
18	CLAB	Control Tactics (8)				
19	CLAB	Apply Restraints (Handcuffing/Flexi Cuffs) (8), Participate in or Lead Stress Drills (.25)				
20	CLAB	Individual Searches (8)				
21	CLAB	Individual Searches (8)				
22	Peterson	Challenge Individuals and Vehicles (4), Vehicle Searches (4), Participate in or Lead Stress Drills (.25)				
23	RF FIELD	Partcipate in or Lead Progressive Physical Education (1.5), Rifle Fighting Techniques (10.5), Participate in or Lead Stress Drills (.5)				
24	0:00	Participate in or Lead Progressive Physcial Education (2) Apply Concepts and Principles of UoF ***Lecture* (6)**				

BASIC DEFENDER COURSE BLOCK II

TABLE OF CONTENTS

UNIT 16 - INCIDENT COMMAND.....[PG. NO 44-58]

a. Can Identify basic facts and terms about Principles of Incident Command and receive a minimum passing score of 70% on the written test
b. Can Identify basic facts and terms about Execute the Emergency Action Plan and receive a minimum passing score of 70% on the written test
c. Can Identify basic facts and terms about Control Center Operations and receive a minimum passing score of 70% on the written test
d. Can Identify the basic facts and terms about Search Areas, Barrier and Obstacle Plans, Additive Procedures and receive a minimum passing score of 70% on the written test
e. Can Identify basic facts and terms about Area Searches and receive a minimum passing score of 70% on the written test
f. Can Identify basic facts and terms about Building Searches and receive a minimum passing score of 70% on the written test
g. Can Identify basic facts and terms about Secure a Crime Scenes/Protect Evidence and receive a minimum passing score of 70% on the written test
h. Can Identify basic facts and terms about AF Form 1109 and receive a minimum passing score of 70% on the written test
i. Can Identify basic facts and terms about CBRNE Hazmat and receive a minimum passing score of 70% on the written test
j. Can Identify basic facts and terms about Entry Authority List and receive a minimum passing score of 70% on the written test
k. Can Identify basic facts and terms about Escorted and Unescorted Entry Procedures and receive a minimum passing score of 70% on the written test
l. Can Identify basic facts and terms about Stop-Check-Pass and receive a minimum passing score of 70% on the written test

UNIT 17 - INSTALLATION ACCESS.....[PG NO. 59-65]

a. Can Identify relationship of basic facts and state general principles about Conduct Installation Breach Procedures and receive a minimum passing score of 70% on the written test
b. Can Identify relationship of basic facts and state general principles about Conduct Installation Entry/Exit Point Checks (IACP) and receive a minimum passing score of 70% on the written test
c. Can Identify relationship of basic facts and state general principles about Conduct Alarmed Response and receive a minimum passing score of 70% on the written test
d. Can Identify basic facts and terms about Conduct Unauthorized Entry Procedures and receive a minimum passing score of 70% on the written test
e. Can Identify basic facts and terms about Utilize Duress Procedures and receive a minimum passing score of 70% on the written test
f. Can Identify relationship of basic facts and general principles about Utilize Sign, Countersign and Emergency Response Codes and receive a minimum passing score of 70% on the written test
g. Can Identify relationship of basic facts and state general principles about Conduct Building and Repository Checks and receive a minimum passing score of 70% on the written test

UNIT 18 - RESOURCE CONTROL DUTIES.....[PG NO. 66-68]

d. Can Identify basic facts and terms about Perform or Lead ABGD and Resource Security Duties Tasks and receive a minimum passing score of 70% on the written test

UNIT 14 - USE OF FORCE .....[PG NO. 69-73]

a.Placed in a training environment, can identify why and when the task must be done and why each step is needed for Apply Concepts and Principlesof Use of Force IAW PC 11-14a

UNIT 3 - SF TASKS

3a. IDENTIFY BASIC FACTS AND TERMS ABOUT SECURITY FORCES MISSION, VISION, AND MISSION ESSENTIAL TASKS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Security Forces Mission

Security Forces protect, defend, and fight to enable Air Force (AF), Joint and Coalition missions

Security Forces Vision

Mission-ready, resilient, and air-minded Security Forces

Organized, trained and equipped to deliver enduring Integrated Defense against threats to the AF, Joint and Coalition missions

Recognized and respected for our air-centric expertise

Security Forces Mission Essential Tasks

Form the foundation upon which we train and are the cornerstones of our strength as an organization

PROVIDE INSTALLATION AND ASSET PROCTECTION

Plan for and employ the capabilities of Integrated Defense to mitigate potential risks. Defeat adversarial threats to the AF operations within the Base Boundary and Base Security Zone.

CONDUCT LAW AND ORDER OPERATIONS

Defenders directly contribute to installation's integrated defense via law and order operations, which encompasses crime prevention, criminal investigations, traffic enforcement, and corrections. In planning, the specific authorities for law and order operations may depend upon jurisdictional status of the installation.

PROVIDE SECURITY AND PROTECTION FOR NUCLEAR ASSETS

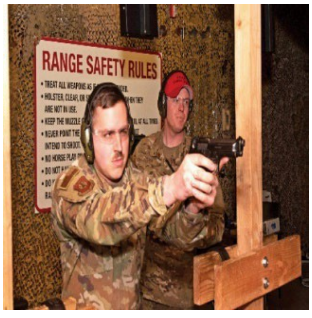
Defenders provide the highest degree of security possible for nuclear munitions in all circumstances (e.g., weapons storage areas, nuclearconvoys, and uploaded aircraft). In accordance with (IAW) applicable Department of Defense, AF, and National Security Presidential Directives.

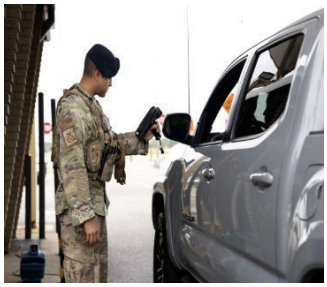
PROVIDE TRAINING AND MAINTENANCE OF SMALL ARMS AND LIGHT WEAPONS

Defenders provide weapons qualifications training, forecast for sufficient ammunition in support of training, inspect, and service small arms and light weapons for AF personnel.

PROVIDE MILITARY WORKING DOG SUPPORT

Defenders equip, train, and manage military working dog teams to integrate into defense operations. Supporting Department of Defense military working dog taskings and the integrated defense plan.





3b. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT CAREER FIELD HISTORY AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

1940s

1941 Army Air Force (AAF) Established

- MP companies still fall under Army Provost Marshal

MARCH 29, 1943

- Gen Henry H. Hap Arnold established Office of the Air Provost Marshal for the AAF Marking what Security Forces celebrate as its birth ate.

World War II to Korea – 1940s – National Security Act of 1947 (July 26) Authorized creation of the United States Air Force
Took over personnel, aircraft, and mission of the Army Air Force including Military Police (MP) force, which would eventually become Security Forces.

January 2, 1948

- HQ USAF General Order No.1 designated all prior MP units and personnel serving under them as "Air Police." HQ USAF General Order No.1 established the USAF Air Provost Marshal.

1950s

Korean War Era-1950s - American and South Korean forces were ill-prepared. Air Police were only armed force on the base Forward Air Bases overrun by the enemy. Faced to fall back hurriedly. Led to decision that the Air Force needed to develop a more extensive base defense capability. Concentrated on the training of Air Police who would then train other members of the Air Force.

Milestones 1950s

- **Sept 1, 1950** - the first Air Police School established at Tyndall AFB, FL
- **1952 -** Air Police School moved to Parks AFB, CA and re-designated as the Air Base Defense School
- **13 Oct 1956 -** Air Police training transferred to Lackland AFB TX (Home of the Defender)

1960s

Vietnam and Air Base Defense – 1960s

- **1 July 1965 -** SSgt Terrance Jensen, first Air Policeman killed in action in Vietnam (Da Nang Air Base)
- **1966**-Name of career field changed from Air Police (AP) to Security Police (SP)
- **1967 Operation SAFESIDE –** Created to bolster protection of Air Bases
    - Trained Security Police in light infantry tactics and special weapons
    - 1041st Security Police Squadron (Test) was formed
        - Trained for deployment to Southeast Asia
        - Deployed to Phu Kat AB, Vietnam
        - Established LP/OP, conducted recon/ambush patrols, provided mobile response forces
        - Unit success led to development of ground combat skills training for Security Police

January 31, 1968 Battle of Tan Son Nhut (Tet Offensive)- Biggest test of Security Police combat effectiveness. Tan Son Nhut AB attacked by a force totaling more than 2,500 enemy troops. Five-man team positioned in Bunker 051, held off enemy assault long enough for backup forces to respond. Four of the five-man team were killed in action including Sgts Louis Fischer, William Cyr, Charles Hebron and Roger Mills lost their lives, Sgt Alonzo Coggins was the only survivor, and all five men were awarded the Silver Star.

1970s

March 1971 - Enlisted career field split into two separate specialties as Law Enforcement Specialist and Security Specialist requiring formal training.

November 1971 - 12 female Airman entered Law Enforcement Specialist training.

May 1975, SS Mayaguez - First time Security Police tasked with high priority rescue mission. Mission was to recapture ship and rescue crew. SS Mayaguez was a merchant ship seized by communist forces (Khmer Rouge) in Cambodia. Upon assembling prior to mission, one rescue helicopter crashed shortly after takeoff from Nakhon Phanom AB, Thailand. Eighteen Security Policeman, one linguist, and a crew of four all perished and were awarded posthumous Bronze Star with Valor.
November 1976 - 100 female volunteers were selected for Security Specialist training.

1980s

1981-1989 - Ground Launched Cruise Missiles were developed (GLCM).
1983 Operations URGENT FURY (Grenada) - Eastern Caribbean nations called upon US for help. Security Police among the first US forces to arrive.
February 1985 - First female Security Specialist since 1976 entered the career field.
1987 - Air Base Ground Defense School moved from Camp Bullis TX to Ft Dix NJ.
December 1989 Operation JUST CAUSE (Panama) - Security Police units tasked with securing landing strips. Participated in drug interdiction.

1990s

THE GULF WAR ERA
August 1990 Operation DESERT SHIELD - Defense of Saudi Arabia in wake of invasion of Kuwait by Iraq.
January 1991 Operation DESERT STORM - Objective was to liberate Kuwait from Iraqi occupation.
August 1995 - Air Base Defense training moved back to Camp Bullis TX under control of USAF.
December 1995 Operation JOINT ENDEAVOR (Bosnia) - Security Police conducted convoys and acted as a peacekeeping force.
June 1996 KHOBAR TOWERS

- Khobar Towers bombed in Saudi Arabia
- Three Security Policeman performing sentry duty on roof of dormitory
- SSgt Alfredo Guerrero, SrA Corey Grice and A1C Christopher Wager
- Detected suspicious vehicle parked outside the perimeter fence and the occupants
- 19 USAF members died and more than 260 were injured
- The 3 sentries were awarded the **Airman's Medal** Bombing led to major **Force Protection** changes

October 31, 1997 - Career fields merged to one field. Law Enforcement Specialist, Security Specialist, Combat Arms, now called Security Forces (SF). New mission "**Force Protection**."

2000s

The Global War of Terror
September 11, 2001 - Terrorist attacks on September 11, 2001 changed how Security Forces conducted home station and deployed missions.
Operation ENDURING FREEDOM (OEF)/Operation IRAQI FREEDOM - Security Forces provided Force Protection, Counter insurgency operations, developed rapport with the Villagers, secured airfields, and assisted Army and Marines.
March 26, 2003 - First Air Force combat parachute assault. There were 14 SF members assigned to the 86 CRG jumped into Bashur Airfield in northern Iraq.
January 1, 2005, Operation DESERT SAFESIDE - Task Force 1041 formed (820SFG) Mission: Stop the individuals/groups responsible for the attacks of Balad AB. TF 1041 implemented the aggressive base defense doctrine the 1041st SPS was designed for in Vietnam.

January 2005 to December 2009 - Security Forces tasked in joint effort at Camp Bucca housing over 20,000 detainees, provided security, conducted detainee in-processing, provided entry control, and provided tactical response.

August 2006 - Security Forces tasked to train and deploy a Police Transition Team to Baghdad. Helped Iraqi people take back some of the cities most dangerous neighborhoods from insurgents.

Summer 2008 - 332nd Expeditionary Security Forces Group stood up at Balad AB, Iraq. Was most important hub for air activity in Iraq Theater of Operations.

Since September 11, 2001, fifteen SF members have lost their lives in the Global War on Terror

Airman 1st Class Elizabeth Jacobson
EOW: September 28, 2005
Cause: Improvised Explosive Device
Description: Amn Jacobson was killed on September 28, 2005 near Camp Bucca, Iraq when the vehicle she was riding in was struck by an Improvised Explosive Device (IED) . She was the first security forces member killed in the War on Terror and the first killed in action since the Vietnam War.

SSgt Brian McElroy
EOW: January 22, 2006
Cause: Improvised Explosive Device
Description: SSgt McElroy and Tech. Sgt. Jason Norton were killed on the same patrol 18 miles north of Baghdad when their vehicle struck by an improvised explosive device.

Technical Sergeant Jason Norton
EOW: January 22, 2006
Cause: Improvised Explosive Device
Description: Tech. Sgt. Norton and SSgt Brian McElroy were killed on the same patrol 18 miles north of Baghdad when their vehicle was struck by an improvised explosive device.

Airman 1st Class Leebernard Chavis
EOW: October 14, 2006
Cause: Hostile Gunfire
Description: Airmen Chavis was killed in Baghdad, Iraq by an enemy sniper while supporting an Iraqi police convoy.

Staff Sergeant John T. Self
EOW: May 14, 2007
Cause: Improvised Explosive Device
Description: While on his 79th combat patrol, Staff Sgt. Self was killed while assisting Iraqis in the streets of Baghdad when the vehicle he was riding in was struck by an Improvised explosive device.

Airman 1st Class Jason Nathan
EOW: June 23, 2007
Cause: Improvised Explosive Device
Description: Airman Nathan was killed, June 23, 2007 in Iraq when the vehicle he was riding in was struck by an improvised explosive device.

Staff Sergeant Travis Griffin
EOW: April 3, 2008
Cause: Improvised Explosive Device
Description: Staff Sgt. Griffin was killed during his fourth tour in Iraq while on patrol near Baghdad. The vehicle he was riding in was struck by an improvised explosive device.

1st Lieutenant Joseph Helton
EOW: September 8, 2009
Cause: Improvised Explosive Device
Description: Lt. Helton was killed while on a patrol near Baghdad, Iraq when his vehicle was struck by an improvised explosive device. A 2007 Air Force Academy graduate, he was the first security forces officer killed in action in the War on Terror.

Staff Sergeant Todd "T.J." Lobraico
EOW: 5 September 2013
Cause: Hostile Gunfire
Staff Sergeant Lobraico was killed after his unit was ambushed and attacked by insurgents by small arms fire while on patrol outside Bagram Air Base, Afghanistan.

Senior Airman Nathan Sartain
United States Air Force Security Forces
EOW: 2 October 2015
Cause: Aircraft Crash
SrA Sartain and 11 others were killed when a C-130 crashed while serving in Afghanistan. Senior Airman Nathan C. Sartain, 29; and Airman 1st Class Kcey E. Ruiz, 21; were both assigned to the 66th Security Forces Squadron at Hanscom Air Force Base, Massachusetts. They performed fly-away security team missions, guarding aircraft, cargo, crew and passengers.

Airman First Class Kcey E. Ruiz
United States Air Force Security Forces
EOW: 2 October 2015
Cause: Aircraft Crash
AIC Ruiz and 11 others were killed when a C-130 crashed while serving in Afghanistan. AIC Kcey E Ruiz and SrA Nathan C. Sartain; were both assigned to the 66th Security Forces Squadron at Hanscom Air Force Base, Massachusetts. They performed fly-away security team missions, guarding aircraft, cargo, crew and passengers.

TSgt Joseph Lemm
United States Air Force Security Forces
EOW: 21 December 2015
Cause: Taliban Suicide Bomber Attack
TSgt Joseph Lemm and SSgt Louis Bonacasa of the 105th Security Forces Squadron were part of an off-base movement when a Taliban suicide bomber on a motorcycle crashed into the movement and detonated his bomb. Security Forces members Lemm and Bonacasa along with four AFOSI special agents were all killed in the attack. TSgt Lemm is also a Detective with the NYPD.

SSgt Louis Bonacasa
United States Air Force Security Forces
EOW: 21 December 2015
Cause: Taliban Suicide Bomber Attack
SSgt Louis Bonacasa and TSgt Joseph Lemm of the 105th Security Forces Squadron were part of an off-base movement when a Taliban suicide bomber on a motorcycle crashed into the movement and detonated his bomb. Security Forces members Bonacasa and Lemm along with four AFOSI special agents were all killed in the attack.

Senior Airman Nicholas Alden
United States Air Force Security Forces
EOW: 2 March 2011
Cause: Open Gunfire
SrA Nicholas Alden was killed as a result of a Frankfurt gunman opening fire with a handgun on a busload of U.S. airmen at Frankfurt's airport, killing two and wounding two others. He was on his way to a deployment in Afghanistan.

Senior Airman Nicholas Khai Phan
United States Air Force Security Forces
EOW: 12 September 2020
Cause: Automobile crash
While deployed to Ali Al Salem Air Base in Kuwait, SrA Jason Phan was killed in a single-vehicle crash while patrolling the perimeter.

ONLY 2 AIR FORCE CROSS RECIPIENTS IN SF HISTORY

Highest military decoration awarded to an AF member not justifying the Medal of Honor. Awarded for extraordinary heroism in combat.

Capt Reginal Maisey
Awarded posthumously for actions at Bien Hoa AB, Vietnam during Tet Offensive (1968).

Capt Garth Wright
Awarded for actions at Phan Rang AB, Vietnam (1969).

NUCLEAR OPERATIONS

ALLIANCES & PARTNERSHIPS

Department of Energy (DOE) - Oversees tech research, development, testing, and acquisition programs that produce, maintain, and sustain the nuclear warheads. DoE convoys are conducted to deliver nuclear warheads from testing facilities to DoD Installations and transfer custody to the DoD. At times, SF will be tasked to secure DoE convoys as part of a SAFE HAVEN.

U.S. NAVY - Provides security for nuclear weapons on Naval Installations. At times, conducts Joint exercises with the USAF to ensure nuclear security and surety across the DoD.

Defense Threat Reduction Agency (DTRA) - Enables the DoD and USG to counter and deter Weapons of Mass Destruction and Emerging Threats. Assess threats to US Nuclear Stockpile and Identifies Vulnerabilities.

NATO ALLIES - NATO nuclear policy is covered under ACO Directive 80-6, which governs the alliance nuclear security program in conjunction with DoD 5210.41M. NATO Installations will sometimes have US Munitions, which will be guarded by US Forces while NATO forces guard the installation.

NUCLEAR CAPABLE ALLIES

FRANCE – Developed its first nuclear bomb in 1960, Maintains a nuclear arsenal independent of NATO influence.

UNITED KINGDOM – Maintains a nuclear arsenal, Considered one of the 5 Nuclear Capable states (U.S., UK, France, Russia and China).

AIR FORCE GLOBAL STRIKE COMMAND

HISTORY

- **June 1st, 1992 -** Strategic Air Command (SAC) was inactivated.
- **August 2007-** Nuclear missile was accidentally transferred from Minot AFB, ND to Barksdale AFB, LA.
- **October 2008 -** "Nuclear Roadmap" released and called for over 100 changes to the nuclear enterprise, including the Establishment of Air Force Global Strike Command.
- **January 12, 2009 -** Air Force Global Strike Command, (AFGSC) established at Bolling Air Force Base, Washington D.C.
- **August 7, 2009 -** AFGSC assumes control of all Nuclear Capable bomber and ICBM Forces a Headquartered at Barksdale Air Force Base, Louisiana.

MISSION

Provide strategic deterrence, global strike, and combat support.

.

VISION

Innovative leaders providing safe, secure, and lethal combat-ready forces for nuclear and conventional global strike…today and tomorrow.

Assigned to two Numbered Air Forces (NAF)

- **20th Air Force**
  - **90th Missile Wing, F.E. Warren AFB, WY**
  - **91st Missile Wing, Minot AFB, ND**
  - **341st Missile Wing, Malmstrom AFB, MT**
  - **377th Air Base Wing, Kirtland AFB, NM**

- **8th Air Force**
    - **2d Bomb Wing, Barksdale AFB, LA**
    - **5th Bomb Wing, Minot AFB, ND**
    - **7th Bomb Wing, Dyess AFB, TX**
    - **28th Bomb Wing, Ellsworth AFB, SD**
    - **509th Bomb Wing, Whiteman AFB, MO**

SECURITY FORCES ROLE IN NUCLEAR OPERATIONS - Nuclear operations remain the most important "No Fail" mission in the United States Air Force and the Department of Defense. The strategic deterrent of the nuclear arsenal enables America to advance its political objectives and maintain a credible defensive posture against potential nuclear strikes. Security Forces serves as the primary Defender of all USAF nuclear weapons.

EXERCISING AND CERTIFYING THE NUCLEAR FORCE - The Department of Defense and the branches responsible for nuclear weapons conduct frequent exercises to train and certify the nuclear forces responsible for security. Security Forces personnel at the flight level are required to conduct tactical exercises at frequent intervals to ensure proper training exercises can range from recapture and recovery operations to Bomb Threats and IEDs. Installations conduct wing exercises to build upon the frequent exercising at the tactical level by integrating other mission partners on a quarterly, semi-annual, or annual basis.

HIGHER HEADQUARTER EXERCISES

GLOBAL THUNDER – An annual command and control exercise designed to train and assess all U.S. Strategic Command forces' readiness as a strategic deterrent force. Designed around realistic training activities against simulated adversaries with the goal of evaluating areas to further improve nuclear readiness.

This exercise includes: ▪Increased bomber sorties ▪Missileer training and exercising ▪Nuclear Submarine Readiness
The Goal is to verify the reliability of the entire nuclear triad

ROAD WARRIOR - An annual 3-week long exercise that assesses the Nuclear Convoy Operations of Missile Field Installations.

PARTNER AGENCY EXERCISES - Run at the Installation level to test Nuclear Security during abnormal or hostile environments. FBI and other State/Federal agencies respond and exercise response processes to increase synergy.

NUCLEAR SECURITY INSPECTIONS - Assesses a unit's ability to accomplish its assigned nuclear weapons mission and produce a reliable nuclear weapon in a safe and secure environment. Conducted every 2 years and can also be conducted on a no notice basis.
Inspects every mission set at the Nuclear Installation: ▪ Maintenance ▪Convoys ▪Security (Missile Field &WSA) ▪ Recapture/Recovery ▪Administrative Security ▪Command and Control

AIR BASE GROUND DEFENSE IN NUCLEAR OPERATIONS - Tactics employed in day-to-day and hostile operations are core Air Base Ground Defense Principles. Flight Commanders must be subject matter experts in the tactics they are likely to employ in their operating environment. Air Base Ground Defense principles apply in all operating environments, with leaders making small adjustments due to METT-TC.
Common task associated with NUCLEAR OPERATIONS:

- Conducting presence patrols
- Establishing patrol zones
- Conducting Battle Drills to ensure proficiency in recapture and recovery operations
- Conducting PCCs/PCIs during Guard mounts to ensure all posts are armed as required by DoDI 5210.41M
- Providing dislocated C2 during contingency operations

3c. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT SECURITY FORCES ETHICS & MINDSET AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

ETHICS

Rules of behavior understanding what's morally good vs. morally bad.

SF CODE OF CONDUCT

Guides our ethical behavior as SF Defenders.

Exercising Authority - Accept your authority entrusted to you, be fair, be firm, be impartial, build public trust.

Professional Demeanor and Military Bearing - Treat everyone in a dignified and respectful manner at all times. Escalate if this approach does not work. Once in control demonstrate good discipline and remain respectful.

Personal Appearance - Defenders set the initial impression of the Air Force to the public entering the installation. Maintain a high standard of appearance. Set the example for all to follow.

Personal Attitudes - No matter your life background, perform your duties in an impartial, professional and helpful manner. Discrimination based on race, color, religion, national origin, sexual orientation, age, disability or gender,

Assistance To Others - Render assistance to the public. Assist injured or ill individuals. Assist to the best of your ability.

Attention To Duty - Remain alert and vigilant on post at all times. Do not consume any form of alcoholic beverage while on duty or within 8 hours prior to duty.

Seeking Favors - Do not seek personal advantage through status as Security Forces. Do not try to gain favor or popularity by showing favoritism, overlooking violations, and failing to enforce laws. Do not accept any advantage, gratuity or reward for performing official duties.

Off-Duty Conduct - SF is a high visibility career field and should remain above reproach at all times, on and off duty.

Protection Of Privacy - SF must protect private information collected during the course of their duties. Do not discuss offenses or incidents, except in the line of duty.

WARRIOR MINDSET

DEFENDERS MUST ALWAYS MAINTAIN A "WARRIOR" OR WINNING MINDSET

DEFENDERS NEVER KNOW WHEN THEY WILL FIND THEMSELVES IN A LIFE-THREATENING ENCOUNTER

DEFENDERS MUST CONDITION THEMSELVES TO MAINTAIN A CONSTANT STATE OF AWARENESS

A WELL TRAINED "WARRIOR" MINDSET GIVES DEFENDERS THE CONFIDENCE TO HANDLE ANY SITUATION AND BELIEVETHEY WILL HAVE A POSITIVE OUTCOME

Defensor Fortis (Our Motto)

Our mission is Force Protection. Defensor in Latin means defend, guard, or protect. Fortis in Latin means strong, brave or powerful.

The SF Uniform

Defenders wear a unique duty uniform for the purpose of identification and as evidence of authority.
It provides a deterrent to those who seek to violate the law. Reflects a visible symbol of the Air Force's commitment to protect itself, its community, and the general public.

The SF Shield

Symbol of authority, responsibility, public faith, and trust to each member who wears it. Wear it with pride, dignity and restraint. First official Air Police shield issued in 1959. Current shield adopted in 1966.

The SF Beret

Military berets have been the trademark that identifies a particular group as being special and from the average military member. Officially worn worldwide by our career field starting in February 1976.
Shows a significant symbol of authority and should not be worn when performing base details such as picking up trash.

The SF Flash

Our symbol the Falcon over crossed runways was adopted in 1997. Derived from the heraldry of the Vietnam era Operation Safe Side 1041 SPS (Test). Blue alludes to the sky, the primary theater of AF operations. Yellow refers to the sun and the excellence required of SF members. The crossed runways represent all bases and AF operations. The Falcon, with talons extended, is swooping in on its prey symbolizing Force Protection. Our motto Defensor Fortis on lower portion of flash below. Falcon and crossed runways.

SECURITY FORCES PLEDGE

I am a Security Forces member,
I hold allegiance to my country,
devotion to duty and personal
integrity above all.
I will wear my badge
of authority with dignity and restraint,
and will promote by example
high standards of conduct,
appearance, courtesy,
and performance.
I seek no favor
because of my position.
I perform my duties in a firm,
courteous, and impartial manner,
irrespective of a person's
color, race, religion, national
origin or sex.
I strive to merit
the respect of my fellow Airmen
and all with whom I
come in contact.

GENERAL ORDERS

1. I will take charge of my post and protect personnel and property for which I am responsible, until properly relieved.
2. I will report all violations of orders that I am entrusted to enforce and call my superior in any case not covered by instructions.
3. I will sound the alarm in any case of disorder or emergency.

3d. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT MEDIA/SOCIAL MEDIA RELATIONS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

MEDIA AND SOCIAL MEDIA RELATIONS

Units using social media to communicate with the public is a function of Public Affairs (PA) offices. Social media is any internet based or mobile device based public communication. The unit commander is responsible for all content on the unit's social media page. Every public Air Force social media presence is a direct reflection of the Air Force. Official government use of private or closed social media groups is not authorized.

INAPPROPRIATE MATERIAL AND PROHIBITIONS INCLUDE

- Links to offensive or unrelated commercial material
- Any information that would reveal sensitive movements/locations of military assets or personnel
- Personal information protected by the Privacy Act
- Copyrighted material without written permission from the owner
- Links to any sites that discuss political activity to include presidential or governor elections and or rallies
- No surveys may be conducted without proper approval
- Do not forge live streamed events should have capability to be taken off-line in event of violence, crime or imagery unsuited for the public or manipulate identifiers in your post to disguise, impersonate, or misrepresent your identity or affiliation

PERSONAL USE OF SOCIAL MEDIA

Air Force respects the right of Airman to use social media as a medium of self-expression. However, all Airman have limitations of free speech to ensure good order and discipline. Social media actions are punishable under the UCMJ. Airmen are free to repost publicly released information on their personal social media accounts. If unsure, contact supervisor to discuss proposed post.

- **DO NOT** post something that is questionable and may reflect negatively on the Air Force
- **DO NOT** use government e-mail accounts to establish personal accounts
- **DO NOT** use official positions on personal accounts

3e. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT PERSONNEL RELIABILITY ASSURANCE PROGRAM (PRAP) AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

PERSONNEL RELIABILITY ASSURANCE PROGRAM (PRAP)

An overarching designation for the Air Force's two nuclear reliability programs, the Personnel Reliability Program (PRP), and Arming Use of Force (AUoF). Security Forces personnel holding the 31P or 3P0 series Air Force Specialty Code require continuous evaluation for reliability to perform armed duties to include security and law and order duties.

ESSENTIONAL ELEMENTS FOR SECURITY FORCES PRAP

In order to maintain the clearance required to retain the Air Force Specialty Code of 31P or 3P0. Security Forces individuals must be US Citizens as outlined in DoDM 5200.02 (DoD Personnel Security Program). All Security Forces personnel require and must maintain Secret Clearence eligibility for Air Force Specialty Code of 31P or 3P0.

COMMANDERS OF SECURITY FORCES PERSONNEL

Commanders are responsible for determining suitability to bear arms based on information obtained through continuous evaluation. The command will conduct a weekly review of the "do not arm" status of assigned personnel with known mental, physical, behavioral, or emotional elements that affect suitability to bear arms. This at-risk review must include the First Sergeant or Commander designated NCO in the absence of the First Sergeant. Commanders may ask military treatment facility medical providers with pertinent knowledge of the Airman's

medical history to participate in At-Risk Reviews. Personnel who are determined to be disqualified and currently possess their PRP code will be placed on the Do Not Arm Roster.

SECURITY FORCES MEMBER RESPONSIBILITIES

Personnel are required to notify their Commander immediately when they believe they are not physically, emotionally or mentally fit to bear arms. Prior to receiving medical, mental health, or support agency assistance, Security Forces personnel will notify the provider or counselor of their requirement to bear firearms as part of their official duties Security Forces personnel will notify their Commander, or appropriate person in their chain of command, if medical treatment was received, the source of the medical treatment (e.g., military or civilian provider), or medication prescribed that could impair judgment. Any time prior, during, or after performing armed duty, all Security Forces have an obligation to report mental, physical or emotional indicators of themselves or another. Security Forces personnel that may cause a negative impact on people, resources or mission. Any Airman can make a recommendation to temporarily withdraw someone's authority to bear firearms when another. Airman verbalizes or displays behavior deemed unsafe or unsuitable for armed duty.

3f. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT THE LAUTENBERG/GUN CONTROL ACT AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

GUN CONTROL ACT OF 1968

A federal law that regulates the firearms industry and firearms ownership. Due to constitutional limitations, it primarily regulates interstate commerce in firearms (manufacturers, dealers, importers, transfers). Several amendments have been added throughout the years to include background checks and individuals to whom the sale of firearms is prohibited.

LAUTENBERG AMENDMENT TO THE GUN CONTROL ACT OF 1968 (1996)

Makes it a crime for any person subject to a restraining order to possess a firearm or ammunition. Commanders are responsible for ensuring all military personnel are briefed annually on the Gun Control Act of 1968, the Lautenberg Amendment, and its consequences. No exception for military or law enforcement personnel engaged in official duties.

18 U.S.C. 922 (g)(9)- It shall be unlawful for any person who is subject to a court order that:

- Was issued after a hearing of which such person received actual notice, and at which such person had an opportunity to participate.
- Restrains such person from harassing, stalking, or threatening an intimate partner of such person or child of such intimate partner, person, or engaging in other conduct that would place an intimate partner in reasonable fear of bodily injury to the partner or child.
- Includes a finding that such person represents a credible threat to the physical safety of such intimate partner or child.
- By its terms explicitly prohibits the use, attempted use, or threatened use of physical force against such intimate partner or child that would reasonably be expected to cause bodily injury.
- Who has been convicted in any court of a misdemeanor crime of domestic violence.
- Ship or transport in interstate or foreign commerce, or possess in or affecting commerce, any firearm or ammunition.
- Receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.
- It shall be unlawful for any individual, who to that individual's knowledge and while being employed for any person described in any paragraph of subsection (g) of this section, in the course of such employment.
- Receive, possess, or transport any firearm or ammunition in or affecting interstate or foreign commerce; or receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.

3g. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT SECURITY FORCES IN JOINT ENVIRONMENT (ADCON, OPCON, TACON) AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

JOINT OPERATIONS

A joint force is one composed of significant elements, assigned, or attached, of two or more Military Departments operating under a single joint force commander (JFC). The protection function encompasses Force Protection (FP), Force Health Protection (FHP), and other protection activities.

FOUR PRIMARY FORCE PROTECTION AREAS

Active Defense - Measures that protect the joint force, its information, its bases, necessary infrastructure, and Lines of Communications from enemy attack.

Passive Defense - Measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy by reducing the probability of, and minimizing the effects of damage caused by hostile action without the intention of taking the initiative.

Application Of Technology and Procedures - To reduce the risk of friendly fire incidents.

Emergency Management Response - Measures to reduce the loss of personnel and capabilities due to isolating events, accidents, health threats, and natural disasters.

FORCE HEALTH PROTECTION (FHP)

Complements Force Protection by promoting, improving, preserving, or restoring the mental or physical wellbeing of service members.

PROTECTION CONSIDERATIONS FOR JOINT OPERATIONS

Campaigns and major operations involve large scale combat against a capable enemy, and typically will require the full range of protection tasks. Threats may also include terrorism, criminal enterprises, environmental threats and hazards, and cyberspace threats. Force Protection is achieved through the tailored selection and application of multi-layered active and passive measures commensurate with the level of risk.

Functions In Physical Security Include:

- Facility security
- Law enforcement
- Guard and patrol operations
- Special land and maritime security areas
- Military Working Dog
- Emergency and disaster response support

OPERATIONS IN THEATER

Defensive Counter Air (DCA) - Supports protection using both active and passive air and missile defense measures.

Global Ballistic Missile Defense - Overarching cumulative planning and coordination for those defensive capabilities designed to neutralize, destroy, or reduce effectiveness of enemy ballistic missile attacks that cross AOR boundaries.

Defensive Use of Electronic Warfare (EW) - Action taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum (EMS) that degrade, neutralize, or destroy friendly combat capability. Examples include expendables (chaff and active decoys), jammers, towed decoys, directed energy infrared countermeasure systems, and counter radio controlled improvised explosive device (IED) systems.

Personnel Recovery (PR) - PR missions use military, diplomatic, and civil efforts to recover and reintegrate isolated personnel. There are five PR tasks necessary to achieve a complete and coordinated recovery of US military personnel, DOD civilians, DOD contractors, and others designated by the President or SecDef: Report, Locate, Support, Recover, and Reintegrate.

CBRN Defense - Preparation for potential enemy use of CBRN weapons is integral to joint planning. Focuses on avoiding CBRN hazards (contamination), protecting individuals and units from CBRN hazards, and decontaminating personnel and material to restore operational capability.

Counter-Improvised Explosive Device (C-IED) Operations - Measures to neutralize the infrastructure supporting the production and employment of IED's. The development of tactics, techniques, and procedures to counter the IED threat at the tactical level.

Identify and Neutralize Insider Threats - Typically persons with authorized access, who commit any of a variety of illicit actions against friendly force personnel, material, facilities, and information. Countering these threats involves coordinating and sharing information among security, cybersecurity, law enforcement, and other personnel and staffs.

Protection of Civilians - Persons who are neither part of nor associated with an armed force or group, nor otherwise engaged in hostilities are classified as civilians and have protected status under the law of war. Protection of civilians may be the primary purpose of a mission or a supporting task.

Administrative Control (ADCON) - Direction or exercise of authority over subordinate or other organizations in respect to administration and support. Includes control of resources and equipment, personnel management, unit logistics, unit and individual training, readiness, mobilization, demobilization, discipline, and other matters.

Operational Control (OPCON) - Command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives and giving authoritative direction necessary to accomplish the mission.

Tactical Control (TACON) - Command authority over assigned or attached forces or commands, or military capability of forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers.

UNIT 4 - MILITARY LAW

4a. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT MILITARY AUTHORITY AND JURISDICTION AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

AUTHORITY TO APPREHEND

SF are representatives of the U.S. Government, the U.S. Armed Forces, the installation commander and the Defense Force Commander (DFC).

The MCM, Rules for Courts-Martial (RCM), Rule 302(b)(1), and the UCMJ, Article 7(b), give SF the authority to apprehend military members. It is essential all SF carry out this duty in a fair, impartial, and professional manner.

Officers, noncommissioned officers and on duty SF or SF augmentation duty personnel have the authority to administer oaths to suspects, subject's, witnesses, and victims, as required.

Jurisdiction

The authority, capacity, power or right to apply the law in both investigations and disposition.

Subject Matter Jurisdiction

This is the jurisdiction of the court over the offense.

Personal Jurisdiction

This is the jurisdiction of the court over the offender or the accused. If a person is subject to the UCMJ at the time of the offense and at the time of trial, a court-martial would have personal jurisdiction over the accused.

Legislative Jurisdictions

Determines the limits of the power of the court with regard to the physical location of a crime or event.

UCMJ is extra-territorial, meaning it is applicable worldwide to those subject to the UCMJ, Article 2.

For example, a magistrate court (civilian court) would not have subject matter jurisdiction over an offense of insubordination because it is not an offense prohibited by federal, state or local criminal code that can be assimilated.

Exclusive

The federal government has total or complete Jurisdiction of offenses occurring on federal lands.

Concurrent

Both the federal and state governments retain all their legislative authority.

Proprietary

The military exercises the same rights as a property owner only.

Partial

Both federal and state governments have some authority, but neither has exclusive power. For example, a state may have retained criminal jurisdiction over an installation or part of an installation (housing area).

Title 10 of the United States Code - outlines the role of the Active Duty and Reserve Armed Forces-Being in Title 10 status means Active Duty and Reserve personnel fall under federal military jurisdiction.

Title 32 of the United States Code - outlines the role of the United States National Guard.

- Activation under title 32 U.S.C. is when a state governor has been authorized or directed by the president to mobilize or activate the National Guard under state control.
- Title 32 orders are normally for state level or natural disasters, while title 10 are for national defense. Guard members must be in a federal (Title 10) status for federal military jurisdiction to attach to them. If a Guard member commits an offense while under Title 32 orders, they may be subject to discipline by state authorities. When questions arise concerning a Guard member, consult the SJA.

THE POSSE COMITATUS ACT

Prevents U.S. Army and Air Force personnel from executing the laws of the states or the laws of the United States except when acting under the authority of:

- United States Constitution
- Act of Congress
- Direction of the President of the United States (POTUS)

Does not apply to off installation investigations of violations of the UCMJ. The Posse Comitatus Act governs the use of Army and Air Force personnel only within the continental United States.

4b. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT MILITARY LAW AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

MILITARY LAW

Requires a separate judicial system geared to the needs of the military and was designed to operate outside of the federal court system. The purpose is to promote justice, assist in maintaining good order and discipline in the armed forces, and promote efficiency and effectiveness in the military establishment, and thereby strengthen the national security.

THREE SOURCES OF MILITARY JURISDICTION

U.S. Constitution - Article 1, Section 8- Authorizes the U.S. Congress to make rules for the government and regulation of the land and naval armed forces. Article 2, Section 2-Provides for the President of the United States (POTUS) to be Commander in Chief of the U.S. Armed Forces.

Federal Statutes - Laws passed by the U.S. Congress. Most of the statutes that directly affect the USAF are compiled in Title 10 USC.

International Law - Customs, written agreements among nations and the writings of authorities. The Law of War is included under international law.

JURISDICTION APPLICATION APPLIES TO PERSONS, PLACES AND OFFENSES.

Person-Article 2 of the UCMJ - States exactly who is subject to military jurisdiction.

- Members of the regular component of the Armed Forces

- Cadets, aviation cadets and midshipman
- Members of the reserve components while on inactive training, but in the case of the Army National Guard or the Air National Guard, only when in federal service
- Retired, regular component members of the military entitled to pay
- Retired, reserve component members receiving military hospitalization
- Members of the fleet reserve and the fleet marine reserve
- Persons in Armed Forces custody serving with a sentence imposed by a court martial
- Prisoners of war in custody of the armed forces
- In time of declared war or contingency operation, persons with or accompanying the Armed Forces in the field (news reporters, contractors, U.S. civilian employees), subject to certain limitations
- Members of the National Oceanic and Atmospheric Administration, Public Health Service and other organizations, when assigned to and serving with the armed force

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

Offense - The UCMJ Punitive Articles are the primary source for charging military offenders with Articles 77-134 of the UCMJ known as the "Punitive Articles." Articles 77-134 are specific offenses that if violated may result in punishment by courts martial.

CIVIL LAW

Body of laws of a state, or nation regulating ordinary private matters. Distinct from laws regulating criminal, political, or military matters. Example:

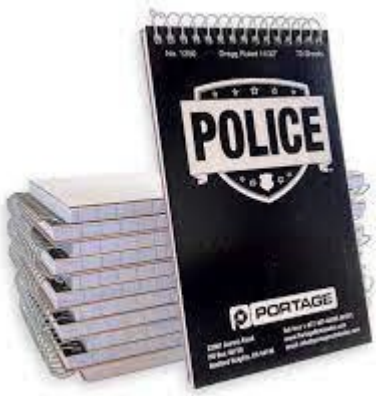
- Dispute of borrowed money is a private matter; SF do not get involved unless a criminal offense occurs

FEDERAL ASSIMILATIVE CRIMES ACT (18 U.S.C. 13)

Allows for adoption of state law in the absence of applicable federal law. Adoption by Congress of state criminal laws for areas of exclusive or concurrent federal jurisdiction, provided federal criminal law, including the UCMJ (for those subject), has not defined an applicable offense for the misconduct committed.

JENCKS ACT (MCM RULE 914)

Governs production of statements and reports of prosecution witnesses during federal criminal trials. Identifies what could be called upon as evidence in a court proceeding.



Typically, it may consist of:

- Police notes
- Memoranda
- Reports
- Summaries
- Letters
- Verbatim transcripts used by government agents or employees to testify at trial

FEDERAL TORT LAW

A body of rights, obligations and remedies applied by courts in civil proceedings to provide relief for persons who have suffered harm from the wrongful acts of others. SF who chooses to operate outside of established guidance or act in an unprofessional manor may be subject to a civilian lawsuit (Federal Tort).

SEARCH

Conducted to uncover evidence of a crime, evidence surrounding a crime or contraband. Must be conducted in places where objects sought could be reasonably found. **ONLY** military judges and qualified Commanders have the authority to grant search authorizations. The installation commander's authority to search does not apply to off base. SF will coordinate with the servicing SJA for all probable cause searches.

SEARCH AUTHORIZATIONS

Based upon probable cause and describe the person, place, or thing to be searched and specific objects being sought. Will be completed via **AF Form 1176,** *Authority to Search and Seize* . Should be completed before the search or as soon as possible after oral permission is received, not to exceed 3 duty days.

PROBABLE CAUSE

Exists when there is a reasonable belief the person, property or evidence sought is located in the place or on the person to be searched. A search authorization may be based upon hearsay evidence in whole or in part.

SEARCH AFFIDAVIT

A statement of "Probable Cause" supporting the request for authorization to search and seize. Completed by the person requesting search authority and must be read word for word to a judge advocate, military magistrate, or commander with authority to authorize the search. If time is critical, the person requesting the search authority may orally relay the "Probable Cause" information and complete the affidavit within 24 hours.

CONSENT FOR SEARCH AND SEIZURE

Should be in writing but may also be verbal. Verbal consent should be witnessed by a reliable second party, preferably another SF member. If possible, obtain written documentation as soon as possible after verbal consent. Use **AF Form 1364**, *Consent for Search and Seizure* , if form is not available written consent may be given in any format.

SEARCH INCIDENT TO APPREHENSION

SF may search, incident to the arrest, the area within an apprehended person's immediate control for weapons or destructible evidence. Immediate control is the area which the SF member searching could reasonably believe that the person apprehended could reach with a sudden movement to obtain such property.

STOP AND FRISK

SF may stop another person temporarily when they have information or observe unusual conduct that leads them reasonably to conclude that criminal activity has been, is being, or may be committed by a suspect. The purpose of the stop must be investigatory in nature. When a lawful stop is performed, and if there is reasonable suspicion the person is armed and possess an immediate threat to the Defender or others, the person stopped may be frisked for weapons.

RANDOM INSTALLATION ENTRY/EXIT VEHICLE CHECKS (RIEVC)

Installation Commanders may order SF to inspect all or a percentage of motor vehicles/property entering or leaving the installation.

COMMON AREA SEARCH

An area which is available for use by more than one person (dormitory dayroom). It does not require prior approval from competent authority. Any questions concerning what is considered a common area should be directed to the SJA prior to conducting the search.

SEIZURE

The taking of items or persons by authorities, for use at a court-martial or other judicial or administrative proceeding.

WHAT TO SEIZE

- Illegally gained property of the United States Contraband, which is defined as anything illegal for an individual to possess
- Stolen property, the possession of which resulted from the commission of a crime (considered "fruits of a crime")
- Items used to commit a crime, which is considered tools of a crime
- Weapons or other articles that might be used by a person in custody to affect an escape or inflict injury
- Anything that is of evidential value, such property is subject to lawful seizure when listed in a search authorization, search warrant or when it is the object of a lawful consent search

PLAIN VIEW DOCTRINE

All property subject to search and seizure may be seized without further authority whenever seen in plain view during the course of any legal activity. The property must be in an area the person seizing it has a legal right to be without obtaining further authority.

EXIGENT CIRCUMSTANCES

When probable causes exist, SF may search without search authorization or warrant. When there is reasonable belief that the delay necessary to obtain a search warrant or search authorization would result in the removal, destruction or concealment of the property or evidence sought. In this case search does not require approval from competent authority.

4c. CAN IDENTIFY BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT APPREHEND OR DETAIN A SUBJECT AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

APPREHENSION

Equivalent of "arrest" in civilian terminology but is not the same as an "arrest" under the UCMJ. Title 10 USC Section 807 and Rules for Courts-Martial (RCM) Rule 302 defines apprehension as the taking of a person (military member) into custody. SF personnel performing official police or guard duties have the authority to apprehend any person subject to the UCMJ regardless of rank.

WHO MAY APPREHEND?

RCM 302(b) states the following officials may apprehend any person subject to a trial by courts-martial (UCMJ):

- Military Law Enforcement Officials
- All commissioned officers, warrant officers, petty officers, and turning, whether on active or inactive duty status
- Civilians Authorized to apprehend deserters

WHEN TO APPREHEND?

Based on probable cause, which means there are reasonable grounds to believe that an offense has been or is being committed and the person to be apprehended committed or is committing the offense. If the facts and circumstances reasonably indicate a person committed or is committing an offense, then apprehension is justified. An investigative detention may be made on less than probable cause and normally involves a relatively short period of custody.

CIVILIAN DETENTION

The DFC, with the advice of the SJA, will establish local procedures for detaining civilian offenders and turning them over to other federal or state LE officials for arrest, issuing them a federal citation, a barment, or other legitimate military purpose. Civilians may be detained for offenses committed on a military installation.

CUSTODY

The restraint of free movement. An apprehension or detention occurs when SF clearly notifies a suspect they are under apprehension/detention.

4d. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT TRANSPORT OFFENDER AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

TRANSPORTING PERSONNEL

SF safety, and the safety of the military suspect or civilian offender, must be ensured when transporting persons in custody. Suspects in custody will be handcuffed during transport and when available, a patrol vehicle equipped with a transport cage, which must be used. If a cage equipped patrol is not available, then a second SF member must accompany the transport officer.

*Note: The offender **WILL NOT** be seated next to or directly behind the driver.*

TRANSPORT PROCEDURES

- Personnel apprehended for a criminal offense must be prior to transport
- Prior to transport, the interior of the patrol car will be searched for any items that don't belong or should not be within reach of the suspect
- Place suspect in patrol vehicle and utilize safety belt
- Patrolman must contact BDOC upon initiation and upon termination of suspect transport
- Passenger information, beginning and ending mileage, and origin/destination of transport must be recorded in the blotter or incident report
- Upon completion of transport, the patrol vehicle will again be searched for any contraband that may have been discarded by the suspect

4e. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT SUICIDE PREVENTION TECHNIQUES AND ACTIONS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

THEORIES RELATED TO SUICIDE

Perceived Burdensomeness - A sense that "I am a burden to others, I do not contribute to the group, and I am a liability to the groups wellbeing or safety.

Thwarted Belongingness - A sense that "I have no connection to others and those previously meaningful relationships that I did have, have been strained beyond recovery or lost outright.

BOTH CAN BE "CORRECTED" WITH INCREASED SOCIAL SUPPORT

It is the leader's responsibility to ensure Airman understand: That seeking help is encouraged and not a statement that they are somehow incompetent **AND** that negative career impact for seeking counseling is unlikely when Airman seek help on their own and when it occurs before any misconduct.

PROTECTIVE FACTORS	BASIC RISK FACTORS
(Associated with preventing suicide)	(Associated with suicidal behavior)

Unit cohesion and camaraderie	Current/pending disciplinary or legal action
Peer support	Relationship problems
Easy access to helping resources	Substance abuse
Belief that it is ok to ask for help	Financial problems
Optimistic outlook	Work related problems
Effective coping and problem-solving skills	Transitions (retirement, PCS, discharge, etc.)
Social and family support	Relationship problems
Sense of belonging to a group or organization	A serious medical problem
Marriage	Significant loss
Physical activity	Setbacks (academic, career, personal)
Participation and membership in a community	Severe, prolonged, or perceived unmanageable stress
A measure of personal control of life and its circumstances	A sense of powerlessness, helplessness, or hopelessness
	Presence of a weapon in the home
	Religious or spiritual connectedness
	History of previous suicide attempts

ADVANCED WARNING SIGNS

*Expresses an intention of harming self or others *Decreased or impaired emotional

*Thoughts of suicide *A suicide plan *Access to the method of suicide described

*Stating they intend to complete the plan

*Behaves in a manner which would lead you to conclude that there was imminent risk of this harm status

RESOURCES AND REFERRAL AGENCIES

- Financial counseling
- Employment assistance
- Couples support groups

- Parenting support groups
- Military & Family Life Counseling for adults and children (MFLC, MFLC-C)
- Infant and toddler play groups
- Life skills groups (stress management, depression, anxiety, anger, etc)
- Workshops (conflict resolution, dealing with difficult people, supervising etc)
- Respite care (short-term care offered to Airman enrolled in the Exceptional Family Member Program)

WINGMAN CONCEPT OF ASK, CARE, ESCORT(ACE)

ASK- "Are you thinking of killing yourself?" while remaining calm.
CARE- Calmly control the situation, do not use force, be safe while actively listening to show.
ESCORT- Never leave your friend alone. Escort to your chain of command, chaplain, mental health professional, primary care provider, or call the Suicide Prevention Lifeline.

SUICIDE BY COP

Subject's 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 Defenders in a manner they know will require the use of deadly force.

Suicide By Cop Indicators:

- Subject initiated a hostage or barricade situation and refuse to negotiate
- Subject has killed a significant other in their life, especially if the victim was a child or parent
- Subject demands law enforcement kill them
- Subject has recently learned they have a life-threatening illness or disease
- Subject indicates an elaborate plan for their death, one that has taken both thought and preparation
- Subject says they will only surrender in person to the officer in charge, police chief or ranking officer with influence
- Subject indicates they want to go out in a big way
- Subject presents no demands that include escape or freedom
- Subject provides law enforcement authorities with a verbal will
- Subject appears to be looking for a "manly" or "macho" way to die
- Subject has recently given away money or personal possessions
- Subject has a criminal record indicating past assaults
- Subject has recently experienced one or more traumatic events in their life that effects their family or career
- Subject expresses feelings of hopelessness and helplessness

NEGOTIATION STRATEGY

The purpose of intervention is to defuse intense emotions and return the subject to a normal functioning level. Defenders must ask about suicide, buy time, establish report, communicate empathy and gain information. The goal is to influence the subject's thinking to a normal functioning level in an attempt to get them to decide not to commit suicide.

4f. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT BLOODBORNE PATHOGENS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

BLOODBORNE PATHOGENS (BBPS)

Pathogenic microorganisms that are present in human blood and can cause disease in humans.

OTHER POTENTIALLY INFECTIOUS MATERIALS (OPIMS) (CAN CAUSE EXPOSURE)

- Semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid

- Pericardial fluid, peritoneal fluid, amniotic fluid, saliva in dental procedures
- Blood, any unfixed tissue, or organ from a human

TRANSMISSION OF BBPS AND OPIMS

- Needle stick injury
- Any other laceration by a contaminated object, such as broken glass, blade, sharp object etc.
- Open cut, wound, weeping lesion (non-intact skin)
- Eyes, mouth, nose (mucous membrane)

BLOOD BORNE PATHOGEN PROTECTIVE KIT

Required in all Defender vehicles:

- One-way respiratory cardio-pulmonary resuscitation (CPR) mask
- Surgical gloves
- Eye protection
- Surgical
- Mask and gloves

SAFETY RESPONSIBILITY

Each individual has the safety responsibility of ensuring universal precautions and personal protective equipment is utilized when an exposure hazard is present or could be present at an accident or incident scene.

TRAINING

Each unit will take all reasonable measures to allow its members to perform their duties in a safe and effective manner. Defenders will be trained on the use of Personal Protective Equipment (PPE) and collection and disposition of possibly contaminated materials, receiving initial and annual training.

BLOOD BORNE PATHOGENS EXPOSURE CONTROL PLANS

Each SF unit will develop a blood borne pathogen exposure control plan that will contain the following:

- Duty positions which are likely to be exposed to contaminated materials
- Tasks and procedures in which exposure may occur
- Methods available to prevent contact with blood, fluids and OPIMs
- Labeling procedures which comply with the Occupational Safety and Health Agency (OSHA) standard
- Procedures for keeping records of all incidents and occupational exposures per OSHA standard

The following personnel are reasonably anticipated to have skin, eye, mucous membrane, or other contact with blood or other potentially infectious fluids or materials:

- Flight Chiefs/Sergeants
- S2 Investigators
- Law and Order patrols
- Internal Security Response Teams
- External Security Response Teams
- Corrections supervisors
- All Access Controllers (installation and PL)
- Close Boundary Sentries
- All Traffic Control Points and cordon guards in support of emergency and normal duties

Certain tasks or duties are reasonably anticipated to have skin, eye, mucous membrane, or parental contact with blood or other potentially infectious fluids or materials which include:

- Crime scenes (responding, securing, or investigating)
- Traffic accidents (responding, securing, or investigating)
- All disaster/contingency operations
- Rendering first aid
- Searches
- Animal attack cases
- Drowning or near drowning incidents
- Handling of transients or illegal aliens
- Handling domestic violence cases or sex offenses
- Handling of evidence from above incidents

EXPOSURE PROCEDURES

Any person who has unprotected physical contact with blood or other bodily fluids of another person while in the line of duty shall be considered to have been potentially exposed to HIV, HBV, or other blood borne pathogens. If an exposure has occurred or the individual believes they have been exposed, they should immediately wash off or flush the affected area and other skin areas as soon as possible and report the incident to their supervisor. During duty hours immediately report to your servicing medical facility, during non-duty hours report to the emergency room. If the exposure occurred by the individual biting, scratching, spitting, or transferring blood or other bodily fluids on the Defender, that individual is subject to a court ordered blood borne pathogens test. The Defender will be informed if the source individual tests positive for HIV or HBV.

CUSTODY AND TRANSPORTATION OF PRISONERS

Individuals with bodily fluids on their persons will be transported in separate vehicles from other persons and may be required to wear a suitable protective covering. During a transfer of custody when the suspect has bodily fluids present on their person, or states they have a communicable disease, Defenders must notify the receiving agency. Defenders will document when a suspect taken into custody has bodily fluids on their person or has stated they have a communicable disease.

DECONTAMINATION

Any unprotected skin surfaces that come into contact with bodily fluids shall be thoroughly washed as soon as possible with hot running water and soap for at least 15 seconds before rinsing and drying. Alcohol or antiseptic towelettes may be used where soap and water are unavailable. Defenders will remove clothing that has been contaminated with bodily fluids as soon as practical and with as little handling as possible and placed in leak proof containers/bags. Any excess bodily fluids in vehicles will be removed with an absorbent cloth, paying attention to any cracks, crevices, or seams, and then disinfected using hot water and detergent or alcohol and allowed to air dry.

SUPERVISED STUDY

UNIT 15 - THREATS

15a. CAN IDENTIFY BASIC FACTS AND TERMS OF OPERATIONS SECURITY INDICATORS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

OPERATIONS SECURITY INDICATORS

The process of tasking, collecting, processing, analyzing, and disseminating intelligence is called the Intelligence Cycle. Four critical sources for gathering intelligence in defending US bases and its interest are Human, Signals, Image and Open-Source Intelligence.

HUMAN INTELLIGENCE (HUMINT)

Intelligence gathered by means of interpersonal contact. A category of intelligence derived from information collected and provided by human sources. HCTs collect information about people and their associated documents and media sources to identify elements, intentions, capability, strength, disposition, tactics, and equipment.

SIGNALS INTELLIGENCE (SIGINT)

SIGINT involves collecting foreign intelligence from communications and information systems and providing it to customers across the U.S. government.

The National Security Agency (NSA) is the lead agency for collecting signals intelligence. NSA is responsible for providing foreign signals intelligence (SIGINT) to our nation's policymakers and military forces. The information is used to help protect our troops, support our allies, fight terrorism, combat international crime and narcotics, support diplomatic negotiations, and advance many other important national objectives. SIGINT is gathered from various sources, including foreign communications, radar and other electronic systems.

IMAGERY (IMINT)

IMINT includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. Image intelligence (IMINT) is obtained from the electro-optical and infrared sensors and from synthetic aperture radars (SAR), possibly capable of detecting moving targets.

OPEN-SOURCE INTELLIGENCE (OSINT)

Open-Source Intelligence (OSINT) utilizes information that is openly available to all. The world overflows with information, facts and figures, writing and descriptions, pictures, videos and audio recordings. Some of it is secured or classified.

The OSINT process consists of four steps:

Discovery - Open-Source Data, a complex field of primary reference sources Photographs, images, documents, audio and video recordings, satellite images, oral debriefing, etc.

Discrimination - Open-Source Information's secondary raw data emerged and appropriately filtered by OSD data analysis. They generally consist of raw data that can be agglomerated, usually with an editing process.

Distillation - OSINT information derived from a voluntary process of analysis, filtering, distillation, and dissemination to a specific selected category. Designed to meet particular information needs, using their own. Intelligence processes. For example: a significant article from an

online newspaper is used to support a military operation. A photo accompanying the article can be useful for the geographical identification of the insurgents' location and could be used to support a tailored operation to attack the rebels.
Dissemination - Validated Open-Source Intelligence (OSINT-V) is Information to which a high degree of certainty has been attributed.

15b. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT INTEGRATED DEFENSE CONCEPTS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

INTEGRATED DEFENSE (ID)

ID bridges the gap between peacetime and wartime actions to protect the force. It provides all personnel with the necessary tools to determine how to mitigate risk to their assets. Each Commander should be capable of applying tailored, risk and effects-based security planning after thorough analysis of the operational environment and available resources. Some assets remain secured in accordance with higher headquarters (HHQ) directives, such as nuclear weapons, arms, ammunition, and explosives (AA&E), and classified information. ID occurs during all facets of DAF operations, from normal peacetime activities through crisis development and contingency operations. It also makes no distinction between CONUS and OCONUS, garrison or deployed locations.

CONCEPT OF INTEGRATED DEFENSE (ID)

ID is the incorporation of multidisciplinary active and passive, offensive and defensive capabilities.
THE GOAL: Employed to mitigate potential risks to DAF, joint, and coalition operations within the Base Boundary (BB) and the Base Security Zone (BSZ) in order to ensure mission accomplishment. The formal decision-making process used to support ID is the Integrated Defense Risk Management Process (IDRMP). Whereby the commander manages risks based upon the association of the criticality of assigned assets and associated systems, a comprehensive analysis of the threat, and the respective vulnerabilities to those assets and associated systems.

ID CONSIDERATIONS

Threats include, but are not limited to, terrorists, insiders, Foreign Intelligence Entities (FIEs), and criminals.

The range of potential adversaries includes the three traditional levels of threats:

Level I - threats include enemy agents and terrorists whose primary missions include espionage, sabotage and subversion.
Level II - threats include small scale, irregular forces conducting unconventional warfare that can pose serious threats to military forces and civilians.
Level III - threats have the capability of projecting combat power by air, land or sea anywhere into the operational area.

Theaters of Operation: ID is conducted worldwide, and Commanders adapt to a variety of operational requirements. Regardless of location, forces conducting ID employ the basic tactics, techniques, and procedures (TTPs) as those employed at home station during normal peacetime operations; however, ID forces adjust TTPs to counter evolving enemy tactics. Adjustments to TTPs should be based on the specific threat, the dynamics of operating in an international environment, or the manner ID efforts are integrated with joint, civilian and host nation forces.

COORDINATION WITH OTHER PROGRAMS

ID does not stand alone to protect personnel and resources; planners create an effective security program by coordinating with other DoD and DAF programs. Protection and defense of air bases requires the coordinated effort of: Integrated Defense (ID), Emergency Management (EM), Anti-Terrorism (AT), Critical Asset Risk Management (CARM), Continuity of Operations (COOP), Force Health Protection, Cybersecurity and Other mission support function forces under the Mission Assurance (MA) umbrella.

ID FORCE CONTRIBUTORS

The Integrated Defense Council (IDC) identifies units and personnel specifically tasked with ID responsibilities and defines their roles in the IDP ID force personnel tasked in the IDP typically fall into one of several categories:

- SF; armed SF Augmentees; armed owner/user protection personnel (civilians can be armed as prescribed in their position description/assigned duties)
- Authorized Unit Marshal Program personnel, unarmed owner/user protection personnel; and ID force contributors (both civilians and military personnel not assigned specific ID roles, but through their situational awareness and vigilance provide the ID effort another layer of detection and ability to sound the alarm)

MANPOWER UTILIZATION

SF units are organized, trained, and equipped for an 8-hour duty schedule. Associated post time (arming, guard mount, report completion, weapons turn-in, etc.) extends the normal duty day to approximately 10 hours. For ID forces in schedules with 12-hour shifts or considering 12-hour shifts for a prolonged period of time (in excess of 30 calendar days), Installation Commanders will be the approval authority. Installation Commanders will be briefed on associated risks and presented possible courses of action (COA) to mitigate risks associated with extended shifts.

DEFENSE FORCE COMMANDER (DFC)

Serves as the Installation Commander's primary advisor for ID. On AF installations, the SF squadron commander is the DFC. On installations with more than one SF squadron, the DFC is the SF commander responsible for installation security. The DFC's tactical role serves to ensure unity of effort, command and control of defense forces, cohesive communication and deconflict issues, including fires, to lessen the likelihood of fratricide.

15c. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT THREATS/THREAT LEVELS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

THREATS

May include Conventional military units, Special Forces, foreign intelligence agents and services, terrorist groups, aggressive civil populations, criminal elements, extremist groups, insider threats operating in and across multiple domains. The enemy may use weapons such as: Improvised explosive devices (IED), vehicle borne IEDs, mortars, rockets, man portable air defense systems, Computer viruses, CBRN material and agents, explosive ordinance, small arms.

Threat Levels - JP 3-10 Joint Security Operations in Theater lists three levels of threat which require security responses to counter them.

LEVEL I THREATS - Include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion.

- Agents
- Saboteurs
- Sympathizers
- Terrorists
- Civil disturbances

Tactics may include random or directed killing of military and civilian personnel, kidnapping, and guiding special purpose individuals or teams to targets. Integrated Defense Forces must be capable of countering a Level I threat.

LEVEL II THREATS

Include small scale forces conducting irregular warfare that can pose serious threats to military forces and civilians.

- Small tactical units
- Unconventional warfare forces
- Guerrillas
- Standoff weapon threats

These forces are capable of conducting well-coordinated, small scale, hit and run attacks, IED and VBIED attacks, ambushes, and may include significant standoff weapons threats such as rockets, mortars, rocket propelled grenades (RPG), and surface to air missiles. These attacks can cause significant disruptions to military operations as well as to the orderly conduct of local governments and services. Integrated Defense Forces must be capable of deterring and defeating Level II threats.

LEVEL III THREATS

May be encountered when an enemy has the capability to project combat power by air, land, sea, or space anywhere into the operational area.

- Large tactical force operations
- Airborne
- Heliborne
- Amphibious
- Infiltration
- Air and Space operations

May involve infiltration operations involving large numbers of individuals or small groups infiltrated into the operational area and committed against friendly targets. Air and missile threats to bases, base clusters, lines of communication, and civilian targets may also pose risks to joint forces, presenting themselves with little warning time. Level III threats are beyond the capability of base and base cluster security forces and can only be effectively countered by a tactical combat force or other significant force.

15d. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT TERRORISM AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

TERRORISM

The calculated use of violence to instill fear and is intended to coerce or intimidate governments or societies. Pursues goals that are generally political, religious, or ideological. Often planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists. Also planned to erode public's confidence in the ability of a government to protect and govern the people.

TERRORISM ORGANIZATIONAL STRUCTURES

Hierarchical Structure - Well-defined vertical chain of command and responsibility and has a well-established command and support structure. Hierarchical organizations feature greater specialization of functions in their subordinate cells (support, operations, intelligence) Examples: Red Army Faction in Germany, Red Brigades in Italy, Provisional Irish Republican Army (IRA) and Weather Underground.

Networked Structure - Unlike hierarchies, networks distribute authority and responsibility throughout an organization, often creating redundant key functions. To be effective networks require a unifying idea, concern, goal, or ideology. Without a unifier, networks may take

actions that are counterproductive. General goals and targets are announced and individuals or cells with redundant capabilities are expected to use flexibility and initiative to conduct necessary actions.

LONE TERRORIST

Compared with a typical networked or hierarchical terrorist organization, the lone terrorist is often the hardest to detect. The lone terrorist tactics are conceived entirely on their own without any direction from a terrorist commander. Typically, the lone terrorist shares an ideological and sympathetic identification with an extremist organization and its goals but does not communicate their terroristic plans or actions with any group.

IDENTITY BASED TERRORISM (LINKED TO IDEOLOGY AND GOALS)

Ethnocentric - Groups of this persuasion see race or ethnicity as the defining characteristic of a society, and therefore a basis of cohesion.

Nationalistic - Loyalty and devotion to a nation-state, and the national consciousness derived from placing one nation's culture and interests above those of other nations or groups is the motivating factor behind these groups.

Revolutionary - Dedicated to the overthrow of an established order and replacing it with a new political or social structure.

Separatist - The goal of separation from existing entities through independence, political autonomy, or religious freedom or domination.

IDEOLOGICAL CATEGORIES- DESCRIBE THE POLITICAL, RELIGIOUS, OR SOCIAL ORIENTATION OF THE GROUP

Political - Ideologies concerned with the structure and organization of the forms of government and communities.

Religious - Terrorists see their ultimate objectives as divinely sanctioned, and therefore infallible and non-negotiable.

Social - Social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Referred to as "single issue" or "special interest" terrorism.

GEOGRAPHIC CATEGORIES (SOMETIMES USED TO CATEGORIZE TERRORIST GROUPS)

Domestic or Indigenous - "Home-grown" terrorists that typically operate within and against their home country. Frequently tied to extreme political, religious, or social factions within a particular society and focus their efforts specifically on their nation's sociopolitical arena.

International - Describe the support and operational reach of a group. Typically operate in multiple countries but retain a geographic focus for their activities. Example: Hezbollah has cells worldwide and has conducted operations in multiple countries but is primarily concerned with events in Lebanon and Israel.

Transnational - Operate internationally but are not tied to a particular country or even a region. Their objectives affect dozens of countries with differing political systems, religions, ethnic compositions, and national interests. Al-Qaeda is transnational, being made up of many nationalities, based out of multiple countries simultaneously and conducting operations throughout the world.

COMMON TERRORIST TACTICS, TECHNIQUES, AND PROCEDURES

Assassination - Deliberate act to kill a target and usually prominent individuals such as political leaders, notable citizens, collaborators, or particularly effective government officials, among others.
Arson - Has advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

Bombing - The I.E.D. is commonly found to be a terrorist weapon of choice. Can be easily and cheaply fabricated in little time. Viewed as low risk to the perpetrator.

Kidnapping and Hostage Taking - Kidnapping is the unlawful seizure, movement and/or captivity of one or more individuals. Hostage taking is when an individual(s) are restricted from freedom at the price of another to obtain benefit.

Hijacking - The forceful commandeering of a mode of conveyance.

Seizure - Involves occupying and holding a prominent building or object of symbolic value (US embassy, DOD web site, etc.).

Raids or Ambushes - Similar to a military operation, but usually conducted by smaller forces against targets marked for destruction, hijacking, or hostage/barricade operations.

Sabotage - Deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction.

Threats or Hoaxes - Any terrorist group that has established credibility can employ a hoax with considerable success.

Environmental Destruction - Although not widely used, the increasing accessibility of sophisticated weapons to terrorists has the potential to threaten damage to the environment. Tactics may include dumping hazardous chemicals into the water supply, poisoning or destroying food supplies, destroying oil fields and oil tankers.

TERRORIST USE OF ASYMMETRICAL TACTICS

Denial and Deception - Dispersing and hiding, exploitation of sensitive infrastructure and ruse.

Human Shield - Terrorists deliberately may use civilians as human shields.

Ambush and Surprise Attacks - "Shoot and Scoot" tactics such as the use of mortars and rockets in urban terrain before moving to a new location.

Information Operations - Used to disrupt popular support for coalition forces and to garner regional and international sympathy and support for insurgent forces**.** Includes spreading rumors releasing favorable combat footage, posting videos on the Internet and ensuring media access.

15e. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT DOMESTIC THREATS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

DOMESTIC TERRORISM

Terrorism perpetrated by the citizens or legal residents of one country against persons in that country. Defined by Federal Bureau of Investigations (FBI) and Department of Homeland Security (DHS) as activities that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources. It is a violation of the criminal laws of the United States or of any state or other subdivision of the United States. Domestic Terrorism is intended to intimidate or coerce a civilian population, influence the policy of a

government by intimidation or coercion, to affect the conduct of a government by mass destruction, assassination, or kidnapping, occurring primarily within the territorial jurisdiction of the United States.

DOMESTIC VIOLENCE EXTREMIST

An individual based and operating primarily within the territorial jurisdiction of the United States who seeks to further their ideological goals wholly or in part through unlawful acts of force or violence. The mere advocacy of ideological positions and the use of strong rhetoric does not constitute violent extremism. In some cases, direct or specific threats of violence must be present to constitute a violation of federal law.

DOMESTIC TERRORISM THREAT CATEGORIES

Racially or Ethnically Motivated Violent Extremism - Unlawful use or threat of force or violence in furtherance of ideological agendas derived from bias, often related to race or ethnicity, held by the actor against others or a given population group. Use both political and religious justifications to support their racially or ethnically based ideological objectives and criminal activities.

Anti Government or Anti Authority Violent Extremism - Unlawful use or threat of force or violence in furtherance of ideological agendas derived from anti-government or anti authority sentiment. Including opposition to perceived economic, social, or racial hierarchies, or perceived government overreach, negligence, or illegitimacy.

Animal Rights/Environmental Violent Extremism - Unlawful use or threat of force or violence in furtherance of ideological agendas by those seeking to end or mitigate perceived cruelty, harm, or exploitation of animals. Unlawful use or threat of force or violence in reference to the exploitation or destruction of natural resources and the environment.

Abortion Related Violent Extremism - Unlawful use or threat of force or violence in furtherance of ideological agendas relating to abortion. Includes individuals who advocate for violence in support of either pro-life or pro-choice beliefs.

All Other Domestic Terrorism Threats - Unlawful use or threat of force or violence in furtherance of ideological agendas which are not otherwise defined under or primarily motivated by one of the other Domestic Terrorism threat categories. Such agendas could flow from but are not limited to a combination of personal grievances and beliefs, including those described in other Domestic Terrorism threat categories. Some actors in this category may also carry bias related to religion, gender, or sexual orientation.

15f. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT INSIDER THREATS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

INSIDER THREAT

Comes from assigned or attached personnel (military or civilian), host country nationals (military or civilian), third country nationals (contract employees), or other persons assigned to or transiting from an area of responsibility. They may target individuals, groups, facilities, resources, infrastructure, weapon systems, information systems etc.

INSIDER THREAT EVENTS

Joint Base San Antonio Lackland- April 8, 2016- Medina Annex
Armed with 2 Glock pistols killed 2 (victim and suspect/suicide)
Lockdown was initiated / terrorism not suspected

Fort Hood, TX- November 5, 2009-Processing Center
13 killed (plus unborn child)/32 wounded/Resolution- sentenced to military death row

Afghanistan, Sherzad District, Nangahar Province- February 8, 2020- Military Headquarters 3 Suspect Individuals in dressed in Afghan Army uniform/3 killed (2 US soldiers, 1 Afghan soldier)/ 9 wounded (6 US soldiers, 3 Afghan soldiers)
Resolution- resolved by lethal force by US forces

Frankfurt Airport, Germany- March 2, 2011- Occurred on USAF bus at Airport 2 killed/2 wounded/Resolution- suspect apprehended by German police

15g. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT NEAR PEER THREATS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

NEAR PEER

An individual who has recently gone through experiences that someone one or two stages behind is now or soon will be facing. The United States faces an array of threats from near peer competitors that have not been seen since before the fall of the Berlin Wall. As we emerge from two decades of operations in Afghanistan and over fifteen years of operations in Iraq, dramatic efforts are necessary to position our forces for the intense challenges anticipated if we were to engage near peer adversaries in combat. We will not enjoy the same technological superiority that we have grown accustomed to during Operations Enduring and Iraqi Freedom.

The National Defense Strategy specifically addresses China and Russia as the most likely competitors globally, challenging US allies in Europe, the Indo-Pacific, and the Middle East.

GRAY ZONE

The area between war and peace, where weaker adversaries have learned how to seize territory and advance their agendas in ways not recognized as "war" by Western democracies. Gray zone conflicts can offset superior US economic and security structures.

EXAMPLES OF ADVERSARY SUCCESS IN GRAY ZONE CONFLICT:

- Russian and Chinese near unrestricted thefts of US intellectual property, Office of Personnel Management data theft, and penetrations of US civil, utility, and military data and electoral voting systems
- Russian seizure of Ukrainian territory
- Chinese seizure of the South China Seas and the building of military islands in defiance of international court rulings
- China using bilateral economic deals to marginalize US multilateral frameworks in Asia, Africa, Latin America, and the Pacific
- Iran realigning the Middle East by using proxy forces to create friendly governments including Syria, Iraq, and Yemen at the expense of US leadership in the region
- Russia attempting to resurrect former Soviet client state relationships with Syria, Egypt, and Libya, and potentially with additional countries in the Middle East and North Africa

NEAR PEER THREATS

China- Marshalling its diplomatic, economic, and military resources to facilitate its rise as a regional and global power.

Russia- Increasing its capability to challenge the US across multiple warfare domains. Increasing its military and political presence in key locations across the world. Maintains a nuclear triad of nuclear tipped, road mobile and silo based ICBMs / Missiles delivered by submarines / Missiles delivered by long range bombers.

North Korea- Developing capabilities to strike North America and its allies with long range missiles and may produce significant numbers of intercontinental ballistic missiles.

Iran- Expanding its influence by increasing the size and capabilities of its network of military, intelligence, and surrogate forces, while increasing economic activities in other areas of the world.

India & Pakistan- Fighting over claim to the Kashmir region, which both countries claim to hold, these nuclear armed countries have fought a series of wars since becoming independent of Great Britain in 1947.

15h. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT FORCE PROTECTION CONDITIONS(FPCONS) AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

FORCE PROTECTION (FP)

Defined as preventive measures to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease.

FORCE PROTECTION CONDITIONS (FPCONS)

A graduated series of FPCONs ranging from FPCON Normal to FPCON Delta. There is a process by which commanders at all levels can raise or lower the FPCONs based on local conditions, specific threat information, or guidance from higher headquarters. FPCONs may be generated by a force protection condition alerting message or declared locally by the installation commander.

FPCON Normal- This condition applies when a general global threat of possible terrorist activity exists and warrants *a routine security posture*. At a minimum, access control will be conducted at all DOD installations and facilities.

FPCON Alpha- This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the *nature and extent of which are unpredictable*, and circumstances do not justify full implementation of FPCON Bravo measures. The measures in this force protection condition must be capable of being maintained indefinitely.

FPCON Bravo- This condition applies when *an increased and more predictable threat of terrorist activity exists*. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

FPCON Charlie- This condition applies when an incident occurs, or intelligence is received indicating some form of *terrorist action against personnel and facilities is likely*. Implementation of measures in this FPCON for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

FPCON Delta- This condition applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that *terrorist action against a specific location or person is imminent*. Normally, this FPCON is declared as a localized condition.

Condition	Application	Considerations
FPCON DELTA	Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent.	Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.
FPCON CHARLIE	Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.	Implementation of CHARLIE measures will create hardship and affect the activities of the unit and its personnel.
FPCON BRAVO	Applies when an increase or more predictable threat of terrorist activity exists.	Sustaining BRAVO measures for a prolonged period may affect operational capabilities and relations with local authorities.
FPCON ALPHA	Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature, and extent of which are unpredictable.	ALPHA measures must be capable of being maintained indefinitely.
FPCON NORMAL	Applies when a general global threat of possible terrorist activity exists.	Warrants a routine security posture.

15i. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT RANDOM ANTI-TERRORISM MEASURES(RAMS) AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

THREAT ASSESSMENTS AND VULNERABILITY ASSESSMENTS

Used to generate targeted random antiterrorism measures and any Anti-Terrorism (AT) related physical security or protection enhancements. RAMs are instituted to enhance deterrence and detection efforts and should be implemented without a set pattern, either in terms of the measure selected, time, place or other variables.

Lessons learned have highlighted unpredictability in security activities as one of the best and most cost-effective deterrents available to a commander. Randomly changing AT measures enable integrated defenses to appear formidable and prevent threats from easily discerning and predicting patterns or routines that are vulnerable to attack. To be effective, RAM execution should be conducted for sufficient periods of time to increase the visibility and disruption of terrorist operational cycles. Enduring (or prolonged) RAMs will have a greater impact on an adversary's planning cycle.

RAMs should be employed in conjunction with site-specific FPCON measures in a manner that portrays a highly visible and robust security posture from which terrorists cannot easily discern AT measures from security patterns or routines. Implement daily RAMs to include weekends and holidays. The frequency will be increased as the threat increases. RAM implementation shall be compatible and coordinated with ongoing law enforcement or Counterintelligence (CI) surveillance detection and ID measures.

When random vehicle inspections (RVI) are employed as a RAM, ensure pre-coordination with the installation legal office. Follow existing law enforcement rules when employing RVIs as a RAM. Consider methods to make RAMs visible in order to confuse or expose enemy surveillance attempts and preoperational planning.

EXAMPLES OF RAMS INCLUDE

- Irregular guard changes (time, number, location, TTP)
- Roving security patrols varying in size, timing, and routes
- Surprise inspections and searches of personnel and vehicles

15j. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT INTEGRATED DEFENSE PLAN RESPONSIBILITIES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

INTEGRATED DEFENSE PLAN (IDP)

Codifies installation defense efforts among responsible internal/external agencies to ensure all aspects of ID are accomplished, considered, and compensated for. Provides an understanding of security requirements for all units involved in ID and describes how commanders employ available ID forces, capabilities, and concepts to accomplish the overall ID mission.

RESPONSIBILITIES

Installation commanders are the approving authority of the IDP. When a new installation commander is assigned, they must approve the IDP within 120 days. Installation commanders are responsible for the security of their assigned assets and must have a thorough understanding of the IDP for their installation, Geographically Separated Units (GSUs) and Dispersed Sites. The installation commander will direct the IDC to make changes, updates, or conduct a re-write of the IDP as needed based on changes to mission, ID environment, or other unidentified factors.

The DFC will write the IDP in the standard five-paragraph operations order format. The IDP will be a limited release document and contain the assessment data, risk tolerance decision and executed COAs from the installation IDRMP. Each DFC will designate an installation-level OPR for the IDP.

IDP REQUIREMENTS

Requires security plans for each asset with a PL designation (whether on the installation or a dispersed site/GSU supported by the installation) and assets identified in the IDRMP as exceeding the commander's risk tolerance level and not designated a PL resource. Examples of assets not designated as a PL resource that may require security plans are Critical Asset Risk Management (CARM) assets, water/power distribution centers, child development centers, on base schools, commissaries, etc.

Security plans for these assets will include:

- Building Numbers or name of the area involved
- Clearly defined restricted and controlled area locations, boundaries, and markings
- Do not include detailed directions to the area or other information about the restricted or controlled areas in unclassified plans that might aid terrorist, criminal or dissident elements
- External and internal circulation control measures, to include escort authority and entry authorization list procedures, for all restricted and controlled areas in accordance with AFI 31-101
- Clearly defined security patrol response times to PL resources based upon site specific METT-TC factors and thorough analysis of the IDRMP
- Security Response Teams will be capable of responding immediately to the resource to defeat the adversary before any negative effects against the resource can occur
- Intrusion Detection System certification procedures for PL-4 Controlled Areas as determined by the Resource Protection Program Manager and DFC
- Procedures for gaining photography authorization of restricted areas
- Funds protection requirements in accordance with AFI 31-101, if applicable
- Routine and contingency SF posting requirements documented in the post priority chart. After analysis of the IDRMP, the DFC determines which posts go unmanned during funding or personnel shortages
- Normal security support tasks for owners/users providing ID forces on the installation
- Identification of significant locations along the installation perimeter that prohibit entrance without consent of the installation commander (i.e., waterways, key terrain features, installation access control points, and fencing.)
- Persons authorized to grant or restrict entry into installations and authorize searches. The authority may
- be delegated to Mission Support Group commanders
- Vehicle search plans during normal and increased FPCONs

CONTINGENCY PLANS

The IDP is the basic planning document for installation defense planning. Contingency plans are those plans dealing with events that could possibly occur at an installation.

Develop contingency action plans which outline the actions necessary to mitigate each event listed in this paragraph and those mandated in a MAJCOM supplement:

- Department of Energy and Department of Transportation Safe Havens
- Civil disturbances or riots affecting the installation or PL resources
- Overt attack on the installation, to include restricted and controlled areas
- Requirements and C2 processes to deploy or receive follow-on ID forces
- Receipt of no-notice presidential aircraft
- Anti-hijack and anti-robbery measures
- Bomb threat and hostage situations
- Plans for expedited emergency entry for off-base fire, medical or law enforcement personnel (as identified in mutual aid agreements) and installation first responders that reside off base
- Protection of resident and transient distinguished visitors and resources secured by civilian or contract police if work stoppages or walkouts occur
- Protection of AA&E shipments and Non-nuclear Munitions Storage Areas
- Arrival of unidentified aircraft or unannounced military or commercial aircraft
- Safe parking for transuranic waste material, where applicable
- Response to workplace, child development centers and school violence situations (if the installation hosts an educational institution)
- Unplanned arrival of Prime Nuclear Airlift Force aircraft

PLANNING CONSIDERATIONS

Base Boundary Sectors- The DFC will divide installations into ID sectors, if applicable, to ensure adequate response to PL resources or mission assets. Do not create only one sector, nor overload any particular sector response times to designated resources by ID forces will be reasonable and outlined in the IDP.

Post Priority Charts- Post priority charts are driven by the IDRMP assessment. The DFC determines posts that will be unmanned during funding or personnel shortages.

SF Checklists- SF checklists should be derived from local operating instructions, the IDP and other installation response plans. Condense long, complicated instructions into concise, step by step checklists for Base Defense Operations Center (BDOC) controllers and posted sentries to use.

Special Security Instructions (SSIs)- SSIs are furnished to each ID force member and posted sentry. They define post limits, communications available, physical security deficiencies on post, compensatory measures, entry requirements, applicable special instructions and special equipment required.

Increased Readiness Procedures- Detection screens using security patrols, posted sentries and Military Working Dog teams to provide surveillance over logical avenues of approach to the installation and restricted areas. Provide response elements to support the detection screen. Organize additional response elements (Security Response Teams, Fire Teams). Activate the alternate BDOC. Train supporting ID force personnel who work in or around restricted and controlled areas supporting installation operations, so they are prepared to meet and defend threats against resources.

Actions During an Attack- Immediate response is required after a confirmed attack on the installation or against AF resources. An attack may range from sabotage against an individual resource to an overt attack by a hostile force against an installation. Allocate only the forces needed to neutralize an attack; be wary of diversions. If an attacking force is large enough to exceed the neutralizing capability of on duty ID forces, recall off-duty forces or divert forces from an area containing lower or like PL resources. After neutralizing an attack, transition to a normal security posture or implement a FPCON designed to detect secondary activity (surveillance, hostile element prepositioning/posturing) and attacks as determined by the installation commander. The first priority in implementing a higher defense posture or FPCON is to establish security of identified localities. There may not be sufficient in-place SF available to satisfy all peacetime security requirements and simultaneously provide adequate security for defended localities, particularly in the early stages of a hostile event. Curtail day-to-day functions not contributing directly to the security of the defended locality or have supporting ID force personnel perform those duties. Apply the bulk of the security effort outside restricted areas as opposed to the peacetime concept of close-in security. This tactic enhances the ID desired effects of detect, deter, assess, and warn.

UNIT 16 INCIDENT COMMAND

16a. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT PRINCIPLES OF INCIDENT COMMAND AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

INCIDENT COMMAND SYSTEM (ICS)

A standardized approach to the command, control, and coordination of on scene incident management that provides a common hierarchy within, which personnel from multiple organizations can be effective. Used by all levels of government and non-government organizations. Applies across disciplines and is meant to enable incident managers from different organizations to work together seamlessly. Flexible, standardized, on scene, all hazards incident management approach. It can be used not only for emergencies but also planned events. ICS is a component of the National Incident Management System (NIMS).

MANAGEMENT CHARACTERISTICS

Common Terminology- Establishes common terminology that allows diverse incident management and support organizations to work together.

Modular Organization- The ICS organization may expand based on the incidents size and complexity and functional responsibilities are delegated.

Management by Objectives- Developing and issuing assignments, plans, procedures, and protocols to accomplish identified tasks.
Incident Action Planning- Concise, coherent means of capturing and communicating overall incident priorities, objectives, strategies, tactics and assignments.
Manageable Span of Control- Number of individuals or resources that one supervisor can manage effectively during an incident.
Incident Facilities and Locations- Various types of support facilities:

- Incident Command Post (ICP)
- Incident base, staging areas, and camps
- Mass casualty triage areas
- Point of distribution
- Emergency shelters

Comprehensive Resource Management- Mechanism to identify requirements, order and acquire, mobilize, track and report, demobilize, and reimburse and restock resources such as personnel, teams, facilities, equipment, and supplies.

Integrated Communications- Communication processes and systems that include voice and data links.

Establishment and Transfer of Command- Command should be clearly established at the beginning of an incident. Transfer of command may occur during the course of an incident and should include a thorough briefing.

Unified Command- Established when no single jurisdiction/organization has the authority/resources to manage the incident on its own.

Chain of Command/Unity of Command- Orderly line that details how authority flows through the hierarchy of the incident management organization. All individuals will have a single supervisor to report to. Assignments will be received only from your ICS supervisor.

Accountability- Abide by agency policies and guidelines and applicable local, tribal, state, or federal rules and regulations.

Dispatch/Deployment- Resources should be deployed only when requested or dispatched by an appropriate authority through established resource management systems.
Information and Intelligence Management- Establish process for gathering, analyzing, assessing, sharing, and managing incident related information and intelligence.

16b. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT EXECUTE THE EMERGENCY ACTION PLAN AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

INTRODUCTION TO INSTALLATION EMERGENCY ACTION PLANS

Installations have base specific Emergency Action Plans. SF will utilize locally produced Quick Reaction Checklists and Emergency Checklists when responding to incidents of this nature. These plans identify procedures to be followed in the event of major accidents, natural disasters, attacks, and terrorist use of Chemical, Biological, Radiological, or nuclear (CBRN) weapons or materials. Describes specific actions to be accomplished during an event that would negatively impact a military installation or surrounding areas. Implemented when an event occurs that is beyond the control of on duty responders or is serious enough to warrant an installation response.

RESPONSES THAT CAN BE CONDUCTED

Major Accident Responses Include:

- Hazardous material (HAZMAT)
- Aircraft
- Munitions

- Explosives
- Various modes of transportation
- Facility or industrial site emergencies

Natural Disaster Responses Include:

- Tornadoes
- Ice storms
- High winds
- Flooding
- Earthquakes
- Blizzards

Attack Response-Conventional attack
Response to Terrorist Use of Chemical, Biological, Radiological, and Nuclear (CBRN)

RESPONSE PHASE

Actions- The Incident Action Plan is used throughout an incident. Codifies and distributes tactical objectives and support activities required for one operational period, which generally, lasts 12 to 24 hours.

Prevention- Actions taken to avoid an incident or to intervene to stop an incident from occurring.

Preparedness- Critical tasks and activities necessary to build, sustain and improve the operational capability to prevent, protect against, respond to and recover from domestic incidents. Preparedness is a continuous process. Within the National Incident Management System (NIMS) preparedness focuses on establishing guidelines, protocols and standard for planning, training and exercises, personnel qualification, and certification.

Response- Immediate actions to save lives, protect property and meet basic human needs. Limit the loss of life, personal injury, property damage and other unfavorable outcomes.

Recovery- Begins when emergency responders have completed the emergency response and lifesaving actions. Usually includes firefighting, casualty treatment, UXO safety, runway repair and facility and utility restoration.

Mitigation- Designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

16c. CAN IDENTIFYBASIC FACTS AND TERMS ABOUT CONTROL CENTER OPERATIONS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

(BDOC)/EMERGENCY COMMUNICATIONS CENTER (ECC)

The command and control (C2) center for ID operations during normal and emergency operations. Control center for both garrison and expeditionary operations. Performs both security and law and order functions. A controlled area manned 24/7, 365 days a year.

BDOC/ECC AT A MINIMUM WILL

- Monitor notification, alarm, and alerting systems
- Direct and dispatch all assigned forces
- Document and record activities
- Oversee ID tactical response and make notifications to key personnel to support the incident commander when required
- Implements the security reporting and alerting system, when required
- Up channels reports when required
- Monitors detention facilities (where required)
- Receives public walk in and telephonic/electronic incident reports

SF BLOTTER

The AFJIS Global Blotter is used to maintain a daily blotter of significant events that occur during a shift. Vital to the compilation of higher headquarter reports of incidents occurring across all USAF installations, as well as SF unit crime prevention programs. Distributed to those personnel who have a daily requirement to monitor installation incidents.

BDOC/ECC EQUIPMENT

- Base Station Radio-Primary means of communication between the control center and patrols
- Radio or E-911 system capable of communicating with local civilian police and fire
- National Law Enforcement Terminal System (NLETS) / National Crime Information Center (NCIC)
- When no other facilities offer 24 Hr. storage, classified and evidence storage capabilities
- Primary and alternate telephone systems augment the radio systems
- Emergency generator
- Clocks which show local and ZULU time zones
- Installation crash maps or computer-based mapping system
- Surveillance camera systems
- Method of positive entry control and hardened entry door
- Interior to exterior intercom
- Walk up window must offer one way viewing out of the BDOC/ECC
- Appropriate weapons racks

EXPEDITIONARY BDOC

Tactical considerations determine expeditionary BDOC facility and infrastructure requirements. Established expeditionary BDOC facilities should be developed to meet minimum garrison criteria.

16d. CAN IDENTIFY THE BASIC FACTS AND TERMS ABOUT SEARCH AREAS, BARRIER AND OBSTACLE PLANS, ADDITIVE PROCEDURES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

BARRIER & OBSTACLE PLANS

Barriers and obstacles are designed or employed to channel, direct, restrict, delay, or stop the movement of an opposing force. They impose additional losses in personnel, time, and equipment to the opposing force. Barriers and obstacles can exist naturally, be man-made or be a combination of both.

VEHICLE BARRIERS

Must be effective to stop active vehicle threats at Access Control Points (ACPs) and must be effective to stop stationary vehicle threats at critical facilities.

INTEGRATE SYSTEMS

Defensive reinforcement is achieved by integrating systems of barriers and fields of fire. Barriers serve to fix opposing maneuver elements within a "target window", thus increasing lethality of supporting arms. The objective is to degrade threat movement and assist counterattacks and friendly offensive operations Barriers are a combat multiplier, amplifying friendly force firepower effectiveness by creating optimum fields of fire.

TEMPORARY BARRIERS

Used primarily for indicating higher levels of security for short periods of time, such as when aircraft are on alert status or for national defense areas. May consist of nothing more than an elevated rope, which indicates a demarcation line.

CLEAR ZONES

Should be maintained on both sides of the barrier. Ensures any approach to the barrier from the outside or the inside can be readily observed.

AIRFIELD BARRIERS

Coordinate the placement of any barriers on or near the airfield environment through the Airfield Manager, Civil Engineering and Flying Safety Office prior to installation. May not be located within the mandatory zone of frangibility for runways or taxiways without a waiver.

BOUNDARIES

Mark the legal and physical limits of installations, restricted/controlled areas, free zones, and National Defense Areas. Barriers for boundaries can vary and range from visual (painted red lines) to physical (dual chain link fences). Barriers are the primary means to designate the physical boundary where use of deadly force is authorized in accordance with AFI 31-117.

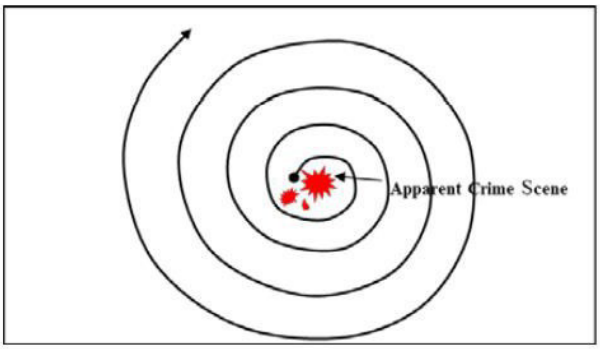
FENCING

Serves as a legal and physical demarcation of the area perimeter. Provides an obstacle and limited delay capability that must be breached by an intruder. A breach of the barrier by anyone without authorization is evidence of illegal entry. Fences located within the mandatory zone of frangibility for runways or taxiways need to be constructed to meet aircraft wingtip clearance requirements and be made frangible. Warning signs should be placed on or near controlled/restricted area fencing.

16e. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT AREA SEARCHES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

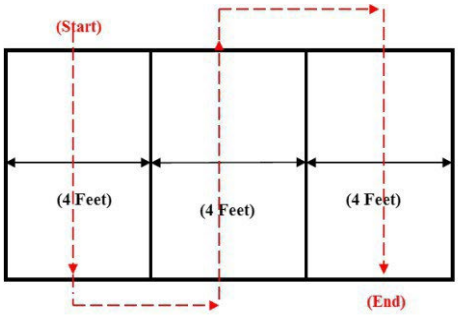
CONCENTRIC CIRCLE

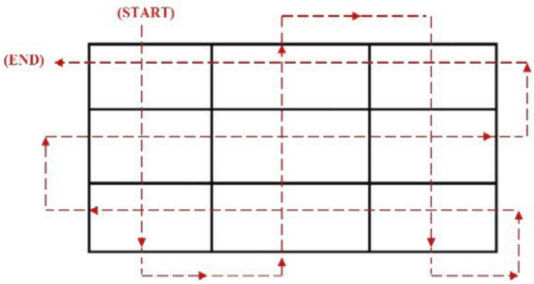
Used in buildings, rooms, and small outdoor areas. Conducted by proceeding in ever widening or ever narrowing circles. For uniformity it is recommended to utilize a clockwise movement.



STRIP AND GRID SEARCH

Used in large outdoor areas and conducted by dividing the area into strips approximately four feet wide. Start at one end of the strip and move back and forth from one end to the other. Once the strip search portion is completed, you will then utilize the grid search. Cover the same area again, but this time search end to end instead of side to side. Once completed, each area has been searched twice (the strip then the grid.)





16f. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT BUILDING SEARCHES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

SEARCHING FOR A PERSON IN A BUILDING

Used for unauthorized personnel inside a building. Responding Defenders will identify the point of entry and set up containment around the structure in the event the individual/s attempts to flee. A contact team will be staged outside the entry point with an array of force options. One Defender will give clear, concise, verbal commands to the suspect to exit unarmed. If no contact made, Defenders should consider utilizing an MWD to aid in the search. If no MWD is available, Defenders can clear the structure slowly and deliberately. Prior to initiating the search, contact the building custodian to obtain the keys.

ITEM TO ITEM SEARCH

Used when there are several items of evidence contained in a room/building. Upon entering the crime scene go to the first apparent item of evidence and visually observe the item (Follow local SOPs for collecting evidence.) Then move to the next closest item of evidence and continue this process until you have completely and systematically reviewed the room you are in. Used for items in plain view, a thorough search of the crime scene will still have to be conducted for other items of evidence.

ZONE AND SECTOR SEARCH

Used for either large buildings or large outdoor area searches. The large indoor or outdoor area is divided into sectors or zones that are then searched as individual areas. Start the search where the incident occurred and then search the other zones or sectors.

DELIBERATE SEARCH TECHNIQUES AND EQUIPMENT

Artificial Lights- May give away position if not utilized properly.

- Handheld
- Helmet mounted
- Weapon mounted

Searching Mirrors- Allows areas to be observed without exposing Defender.

- Various sizes
- Can be pole mounted (adjustable lengths)
- Train to become familiar with them

Door Stops and Wedges- Wedge door open if necessary. Wedge door closed to prevent the possibility of someone exiting behind the team.

Pie the Corners- Search the area ahead of the team one section at a time.

SEARCHING SPEEDS

Direct to threat (dynamic) speed- Speed, surprise, domination, and violence of action is key. Used when speed is essential (Active shooter) Defenders move direct to threat.

Deliberate (covert) speed- Location of threat not known**.** Room to room search conducted**.** Movement is slow, deliberate, and tightly controlled to reduce exposure and noise.

16g. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT SECURE A CRIME SCENES/PROTECT EVIDENCE AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

CRIME SCENES

Scenes are fragile and if improperly handled valuable evidence may be lost or destroyed**.** As soon as possible, the crime scene must be protected, however do not interfere with medical personnel performing their duties. Keep the scene in the same condition it was when the first Security Forces arrive on scene (as much as possible.) Allows investigators to review the scene as it was when the crime was committed. BDOC will notify OSI, if at any time the case is suspected to fall within their investigative purview.

PROCEEDING TO A CRIME SCENE

Proceed to a crime scene quickly and safely. Observe the area as you are responding and note suspicious people, vehicles leaving/fleeing, or people loitering at the scene.

WHEN ARRIVING ON SCENE

- Advise BDOC you are on scene
- Request medical aid or backup patrols as needed
- Apprehend/Detain suspects at the scene and provide medical aid to injured personnel
- Protect the scene
- Record the date, time, and weather conditions
- Remain alert for any alterations made to the scene
- Establish a cordon and post SF to protect the scene
- Redirect traffic as needed away from the scene
- Keep witnesses, victims, subjects, and bystanders separate

SECURITY FORCES' ROLE TO PRESERVE EVIDENCE

Take steps to document everything about the scene as you originally found it.

Crime Scene Notes- Captures a detailed scene description and to document the condition of scene. Captures any actions taken by SF personnel during scene processing.

Crime Scene Sketch- Purpose is to document the scene to show location and distance relationships of evidentiary items and objects within the scene. A rough sketch should be accomplished while in scene.

DO NOT COLLECT EVIDENCE

- Act immediately to protect evidence
- Use raincoat, canvas, wooden/cardboard boxes, or other material to cover things that may be destroyed by weather conditions
- Dead bodies must not be covered until it has been processed for evidence (if in public view screens etc. may be used to provide privacy)
- Do not allow anyone to use facilities (telephones, toilets, sinks etc.)
- Do not allow unrelated materials to enter the crime scene (cigarettes, trash, etc.)
- Note any alterations to the scene, moved evidence could cause investigators to reach bad conclusions
- Before any evidence is collected, it will be photographed
- Once cleared, document collected evidence using AF FM 52 Evidence Tag

16h. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT AF FORM 1109 AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

AF FORM 1109

AF Form 1109 is maintained at controlled or restricted areas. Used to register visitors prior to entry.

PREPARED IN ONE COPY

- **Year, Month, Day-** Self-explanatory
- **Organization-** Organization using the form
- **Location-** Specific area and installation
- **Name, Grade, Organization or Firm-** Full name, grade, and organization of the visitor
- **Signature of Escort and Badge/Number-** Signature and badge number of person escorting. If no badge is used for the area, put "N/A" in the badge number column
- **Time In-** Time entered area
- **Time Out-** Time departed area

YEAR 2023	VISITOR REGISTER LOG			ORGANIZATION	LOCATION		
MONTH Aug	VISITOR IDENTIFICATION			343 TRS	Carter Hall	TIME	
DAY	NAME (Last, First, Middle Initial)	GRADE	ORGANIZATION OR FIRM	SIGNATURE OF ESCORT	BADGE NUMBER	IN	OUT
2	Snuffy, Airman M.	E-1	343 SFS	Airman Escort	N/A	0730	1630

AF IMT 1109, 19990501, V2 PREVIOUS EDITIONS ARE OBSOLETE.

16i. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT CBRNE HAZMAT AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

SPECIAL CONSIDERATIONS FOR CBRNE/HAZMAT INCIDENT RESPONSE

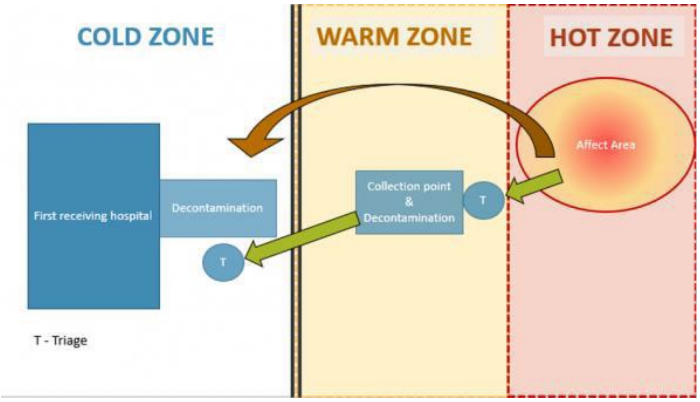
Defenders may find themselves involved in a variety of chemical, biological, radiological and nuclear (CBRN) scenarios whether during peacetime, wartime, or other operational setting. These incidents can be the result of a mishap, a leak, spill or other event involving hazardous material (HAZMAT). Defenders must always be ready to act as CBRNE can be weaponized and used by adversaries in many forms.

RESPONSE TO A CONTAMINATED INCIDENT SITE

Defenders must proceed cautiously to avoid becoming a victim of the incident and follow the directions of trained HAZMAT responders. An initial task within the emergency responder missions is that the Incident Commander (IC) must establish control of the site to protect first responders and keep out unauthorized personnel.

The Strategy Is to Establish Three Distinct Zones:

- Exclusion zone (Hot Zone)
- Contamination reduction zone (Warm Zone)
- Support zone (Cold Zone)



Defender's primary responsibility during initial response is to establish, in concert with the IC, a cordon, Incident Command Post, ACP and Decontamination Corridor. 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 resource. This decision is made before evacuating or relieving contaminated Defenders from their duty positions. The base Fire chief will develop local decontamination procedures.

SPECIAL CONSIDERATIONS FOR CRIMINAL OR TERRORITS USE OF CBRN

If evidence exists that a CBRN incident was a deliberate act, the subject should be apprehended/detained, and BDOC/IC should be notified immediately. Decontamination of all personnel should occur prior to leaving the hazard zone. The contaminated SF unit will be responsible for the suspect until released to AFOSI or FBI agents to limit further contamination exposure to other SF.

SUSPECT DECONTAMINATION AND HANDLING PROCEDURES

During the decontamination of a suspect, the safety of the first responder at the Decontamination Line must be paramount. The agency responsible for decontamination must be informed that a possible hostile suspect is being processed. The receiving unit will handcuff and search the decontaminated suspect as they leave the decontamination area. Handcuffing and searching of the suspect will take place before the suspect is taken to the next stage. SF must coordinate with the lead Federal Investigative Agency (e.g., AFOSI or FBI) as soon as possible; however, transportation of a suspect who requires medical attention to the nearest medical treatment facility takes priority. If no

coordination with the lead Federal Investigative Agency can be made, SF will be responsible for maintaining custody and guarding any suspect transported to medical treatment facilities until properly relieved.

MISSION-ORIENTED PROTECTIVE POSTURES (MOPP) LEVELS

MISSION-ORIENTED PROTECTIVE POSTURES (MOPP)






MOPP LEVEL READY	MOPP LEVEL 0	MOPP LEVEL 1	MOPP LEVEL 2	MOPP LEVEL 3	MOPP LEVEL 4
AT THE DISCRETION OF THE INSTALLATION COMMANDER	AVAILABLE FOR IMMEDIATE DONNING	WORN	WORN	WORN	WORN
INDIVIDUAL PROTECTIVE EQUIPMENT (IPE)	INDIVIDUAL PROTECTIVE EQUIPMENT (IPE) AND PERSONAL BODY ARMOR	OVERGARMENT, FIELD GEAR, AND PERSONAL BODY ARMOR	OVERGARMENT, OVERBOOTS, FIELD GEAR, AND PERSONAL BODY ARMOR	OVERGARMENT, PROTECTIVE MASK, OVERBOOTS, FIELD GEAR, AND PERSONAL BODY ARMOR	OVERGARMENT, PROTECTIVE MASK, GLOVES, OVERBOOTS, FIELD GEAR, AND PERSONAL BODY ARMOR
STORED	CARRIED	CARRIED	CARRIED	CARRIED	CARRIED
ALL IPE AND FIELD GEAR	PROTECTIVE MASK WITH C2 CANISTER OR FILTER ELEMENT AND FIELD GEAR WORN AS DIRECTED	OVERBOOTS, PROTECTIVE MASK, AND GLOVES	PROTECTIVE MASK AND GLOVES	GLOVES	N/A
PRIMARY USE	PRIMARY USE	PRIMARY USE	PRIMARY USE	PRIMARY USE	PRIMARY USE
ATTACK PREPARATION DURING PERIODS OF INCREASED ALERT WHEN THE POTENTIAL OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) CAPABILITY EXISTS BUT, THERE IS NO INDICATION OF CBRN USE IN THE IMMEDIATE FUTURE	ATTACK PREPARATION DURING PERIODS OF INCREASED ALERT WHEN THE ENEMY HAS A CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) CAPABILITY USE MOPP 0 AS THE NORMAL WARTIME IPE LEVEL WHEN THE ENEMY HAS A CBRN CAPABILITY	ATTACK PREPARATION DURING PERIODS OF INCREASED ALERT WHEN A CBRN ATTACK COULD OCCUR WITH LITTLE OR NO WARNING WHEN CBRN CONTAMINATION IS PRESENT OR SUSPECTED AND HIGHER LEVELS OF PROTECTION ARE NOT REQUIRED	ATTACK PREPARATION OR ATTACK RECOVERY DURING PERIODS OF INCREASED ALERT WHEN A CBRN ATTACK COULD OCCUR WITH LITTLE OR NO WARNING AND THE COMMANDER DETERMINES A HIGHER LEVEL OF PROTECTION IS NEEDED DUE TO ATTACK NOTIFICATION TIMELINES, GROUND CONTAMINATION OR ADDITIONAL PROTECTION IS NEEDED WHEN PERSONNEL ARE CROSSING OR OPERATING IN PREVIOUSLY CONTAMINATED AREAS AND RESPIRATORY PROTECTION IS NOT REQUIRED	ATTACK PREPARATION OR ATTACK RECOVERY DURING PERIODS OF INCREASED ALERT WHEN A CBRN ATTACK COULD OCCUR WITH LITTLE OR NO WARNING AND THE COMMANDER DETERMINES A HIGHER LEVEL OF PROTECTION IS NEEDED DUE TO ATTACK NOTIFICATION TIMELINES OR WHEN CONTAMINATION IS PRESENT AND THE HAZARD IS A NEGLIGIBLE CONTACT OR PERCUTANEOUS VAPOR HAZARD	ATTACK RECOVERY WHEN A CBRN ATTACK IS IMMINENT OR IN PROGRESS WHEN CBRN CONTAMINATION IS PRESENT OR SUSPECTED OR THE HIGHEST LEVEL OF PROTECTION IS REQUIRED USE MOPP 4 TO PROVIDE THE MAXIMUM INDIVIDUAL PROTECTION TO PERSONNEL

ADDITIONAL INFORMATION:
- INDIVIDUAL PROTECTIVE EQUIPMENT IS DEFINED IN AIR FORCE INSTRUCTION 10-2501, *AIR FORCE EMERGENCY MANAGEMENT (EM) PROGRAM PLANNING AND OPERATIONS* FOR IPE COMPONENTS AND BASIS OF ISSUE.
- DEPENDING UPON THE THREAT AND MISSION, MOPP LEVELS MAY VARY WITHIN DIFFERENT AREAS OF THE AIRBASE OR OPERATING LOCATION.
- REFER TO AFMAN 10-2503, *OPERATIONS IN A CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVE (CBRNE) ENVIRONMENT* FOR OPTIONS TO THE MOPP LEVELS AND STANDARD OPERATING PROCEDURES TO OPTIMIZE THE USE OF MOPP LEVELS AND ALARM CONDITIONS.
- WEAR FIELD GEAR AND PERSONAL BODY ARMOR WHEN DIRECTED. SPECIALIZED CLOTHING, SUCH AS WET AND COLD WEATHER GEAR, IS WORN OVER THE CHEMICAL PROTECTIVE OVERGARMENT. REFER TO THE APPROPRIATE TECHNICAL ORDERS/MANUALS TO PROPERLY MARK IPE AND THE CPO.

Prescribed by AFI10-2501
Supersedes AFVA10-2512, 24 December 2002
OPR: HQ AFCESA/CEXR

AFVA10-2512
15 August 2011
RELEASABILITY: There are no releasability restrictions on this publication

MOPP Level Ready- All Individual Protective Equipment (IPE) and field gear is stored.

MOPP Level 0- IPE and personal body armor is available for immediate donning. Protective mask carried / field gear worn as directed.

MOPP Level 1- Overgarment, field gear and personal body armor is worn. Protective mask, over boots and gloves carried.

MOPP Level 2- Overgarment, over boots, field gear and personal body armor is worn. Protective mask and gloves carried.

MOPP Level 3- Overgarment, protective mask, over boots, field gear and personal body armor is worn. Gloves are carried.

MOPP Level 4- All is worn, overgarment, protective mask, gloves, over boots, field gear and personal body armor.

16j. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT ENTRY AUTHORITY LIST AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

ENTRY AUTHORITY LIST (EAL)

EALs are used on a temporary basis for granting unescorted entry in conjunction with home base or temporary AFFM 1199s (transiting aircrew and inspection teams etc.). As support technique for is used for single badge entry procedures or in conjunction with escorted entry procedures as a means of identification prior to allowing entry**.** Requesting agencies are responsible for the accuracy of the data contained on the EAL. Requesting agencies must verify personnel data by using the Master Restricted Area Badge Listing (MRABL) for personnel assigned to the installation.

MAINTAINING EAL

EALs must be checked for accuracy prior to being submitted for approval and authentication. Failure to ensure accurate information may result in entry/access being delayed or denied.

EAL REQUIREMENTS

EALs must identify whether or not an individual is authorized unescorted entry or requires an escort. In addition, EALs must contain the following information to enhance identity verification:

- Name, OFF/ENL/CIV and Control Number
- Badge number (IG/SAV team members only)
- Clearance level
- Dates of visit
- Expiration date of the EAL

AUTHENTICATION PROCEDURES

A SF supervisor, (E-5/GS-7 or above or other designated civilian equivalent) will be responsible for validating and authenticating the EAL. Authenticate the EAL by writing the following information near the bottom of page 2 of the cover letter:

- Printed/stamped name/rank of authenticator
- Signed name of authenticator
- Date and time authenticated
- Page number authenticated. Authenticator will add their initials by the page numbers (e.g., page 1 of 3, if there are multiple pages)

ADDITIONS AND DELETIONS TO EALs,

Exercising care when making changes to EALs prevent unauthorized entry. Deletions may be made by using pen and ink changes to the existing EAL. Requesting agencies must provide an EAL showing the requested deletions. Additions may be made by simply providing separate EALs in accordance with above mentioned requirements. Requesting agencies must produce an updated version of the EAL at any time the original EAL with additions/deletions becomes cumbersome and difficult to use. Additions and deletions to EALs must be authenticated using the procedures described in the above paragraph.

***Note**: In the PL-1 nuclear environment, administrative and/or typographical errors require the re-accomplishment of the EAL*

If using the electronic signature process for EAL, all signatures on the should be electronic, to include the aircraft commander or Visiting

Agency Team Chief, the commander of the unit/base being visited and the SF Authenticator. Once electronically signed, the EAL must not be altered. Pen and ink changes to electronically signed EALs require reauthentication.

16k. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT ESCORTED AND UNESCORTED ENTRY PROCEDURES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

IMPLEMENTING ENTRY AND CIRCULATION CONTROL PROCEDURES FOR RESTRICTED AREAS

The objectives of entry and circulation control are to maintain the integrity of areas containing operational resources.

RESTRICTED AREA BADGES (RAB)

RABs are official documents used for controlling entry to restricted areas and may be used for controlled areas and must be retained by the individual issued the RAB. The RAB show the bearer's photograph, signature, and other pertinent identification data. Personnel may use RABs at more than one installation for unescorted entry when the badge is used with a valid Entry Authority List (EAL.)

***Note**: Missing or lost badges must be reported immediately*

Approved RABs are as follows:

- **AF Form 1199. AF Form 1199-1,** USAF Entry Control Credential, Front Label
- **AF Form 1199-2,** USAF Entry Control Credential, Pressure Sensitive Label
- **AF Form 1199A,** USAF Restricted Area Badge (Green)
- **AF Form 1199B,** USAF Restricted Area Badge (Pink)
- **AF Form 1199C,** USAF Restricted Area Badge (Yellow)
- **AF Form 1199D,** USAF Restricted Area Badge (Blue)

TEMPORARY BADGING SYSTEMS FOR RABs

MAJCOMs will establish procedures for implementing temporary badging systems that allow unescorted entry to authorized personnel for short periods of time. Personnel granted unescorted entry to restricted areas must be positively identified prior to being issued a temporary badge.

PL-1 AND 2 RESTRICTED AREAS

Temporary badges for PL-1 and 2 areas must never leave the restricted area for which they are authorized ECs issue these badges at the entry control points as personnel enter and retrieve them as personnel depart the restricted area.

***Note:** For PL-2 facilities where an armed EC is not posted, the owner/user will establish procedures to issue, retrieve and account for temporary badges.*

PL-3 RESTRICTED AREAS

SF or the unit responsible for controlling entry will issue and retrieve the temporary badges for these areas. The badges may leave the restricted area; however, establish procedures to ensure the badges are issued, retrieved and accounted for at the beginning and end of the duty day.

ESCORTED ENTRY TO RESTRICTED/CONTROLLED AREAS

Escorted entry applies to individuals who perform official duties within restricted/controlled areas and have not been granted unescorted entry authority. A person with a RAB for the appropriate area must escort these personnel into restricted/controlled areas. Escorted entry also applies to personnel visiting restricted/controlled areas for non-official business.

ESCORTED ENTRY PROCEDURES

Escort officials assume responsibility for the safe and secure conduct of their visitors and are required to maintain constant surveillance and control of their visitors at all times while in the restricted/controlled area. MAJCOMs may require departure inspections and prescribe search policies for visitor's hand-carried possessions. ECs and escort officials are responsible for accomplishing the following actions when allowing entry:

- Escorts will positively identify individuals being escorted before allowing entry, inspect their vehicles and hand-carried items and certify to the EC that an inspection was conducted
- Escorts will perform escort briefings to the individuals they are escorting that covers security and safety requirements
- Escorts will sign all visitors they are escorting on the AF 1109, Visitor Register Log and ensure at no time they are without escort

EXCHANGE BADGE SYSTEM

The exchange badge system is the most secure method of limiting entry into a restricted area. Installations will develop local procedures to control the badge manufacturing process to prevent exploitation by a single individual. Exchange badges are not required for unescorted entry into non-nuclear restricted areas. However, if used, follow these procedures:

- Issue two badges for each person authorized unescorted entry
- Issue the first badge (maintained by the individual authorized entry) the second exchange badge (maintained at the restricted area entry control points) with information identical to that on the basic badge but on a different color AF Form 1199 card stock
- Mark only the number of the restricted area where entry is authorized on the exchange badge. Exchange badges at the entry control points may be marked or numbered to help personnel track them during exchange and inventory

Note: *Do not mark or number the basic badge. If the badge is lost or stolen, such a mark or number could compromise the system.*

SINGLE BADGE SYSTEM

Another entry control technique which requires only one badge for each person authorized unescorted entry into a restricted area. The EC compares the photograph and identification data on the badge with the bearer's physical characteristics. In order to enter a restricted area unescorted, the individual requesting entry must have one of the following:

- An AF Form 1199 with appropriate area open for access
- An authenticated EAL matching a RAB from another installation or government issued photo ID
- Air Crew Orders with associated CAC

The single badge technique is relatively easy to defeat. Use one of the following supporting techniques to reinforce its effectiveness.

PERSONAL RECOGNITION- Used after the EC has initially verified the individual's authority to enter the restricted area. It can be defined as the ability to match a person's identification to their facial features.

SIGNATURE AND CREDENTIAL CHECK- Ask the bearer to produce a personal ID credential with a picture and signature which can be verified against the RAB signature.

EALs- Compare entry credentials with information contained on an EAL. Ensure accuracy between the two documents.

TELEPHONE OR RADIO VERIFICATION- Designated unit dispatching agencies or similar authorities notify BDOC when a person needs to enter an area.

- BDOC uses a call back procedure to verify the notification and ensure entry is authorized
- BDOC informs the area EC of the impending entry

16I. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT STOP-CHECK-PASS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

STOP-CHECK-PASS

Utilized when there is an immediate need to locate individuals who might be entering or exiting the installation. Local operating instructions will clarify SF requirements and actions upon incident.

Prior to initiating Stop-Check-Pass procedures the Entry Controller needs the following information:

- The physical description of the individual(s) to be located
- The description of the vehicle
- In which lane the procedures need to be implemented
- If the individual(s) is on base then the Stop, Check and Pass procedure will be initiated on the out bound lane, traffic will be halted on the unaffected inbound lane while these procedures are being conducted on the out bound lane
- If the individual(s) is coming from off base then the Stop, Check and Pass procedures will be initiated on the inbound lane, all traffic will be halted on the unaffected outbound lane while these procedures are being conducted on the inbound lane

WHAT IS THE CONCEPT?

Entry controllers can initiate a Stop-Check-Pass – Initiate during AA&E or higher priority Alarm Activation, Anti-Robbery, Duress, Gate Runner and/or when directed by the Flight Sergeant or higher authority.

After initial stop- Entry controller will determine status of the vehicle and passengers and instruct the first vehicle's operator to stand-by until released. The lead vehicle may proceed as soon as another vehicle arrives to replace them (Stop-Check-Pass). This ensures proper lane blockage. Once a suspect has been identified and description obtained, IECPs may initiate a (Stop-Check-Pass) on outbound vehicle lanes. Each occupant in the outbound vehicle must be verified before being allowed to depart.

Use two personnel- Inspect the first vehicle in the outbound lane, then inspect the second vehicle in line before the first is allowed to leave.

Continue cycling through vehicles- Always ensuring there is a vehicle with verified occupants blocking the outbound lane until terminated. Due to the high probability the individual(s) who is being located is trying to flee, it is imperative those conducting Stop, Check, and Pass practice good situational awareness.

UNIT 17 INSTALLATION ACCESS

17a. CAN IDENTIFY THE RELATIONSHIP OF BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT CONDUCT INSTALLATION BREACH PROCEDURES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Conduct Installation Breach Procedures

Physical security encompasses measures designed to protect personnel, equipment, installations, material, and documents. Procedures in local Integrated Defense Plans (IDPs) are established to deter unauthorized personnel from entering an installation and to protect installation resources. To restrict unauthorized access, the perimeter of the installation should have appropriate fencing, lighting and signage that clearly delineates the legal boundary of the installation. Military personnel who enter or re-enter an installation illegally may be apprehended under the UCMJ. Civilian personnel who enter or reenter an installation.

Defense Biometric Identification System (DBIDS)

DBIDS provides positive identification of individuals requesting access to the installation through the electronic interrogation of access credentials. The use of DBIDS is mandatory. Daily DBIDS installation access use aids the prevention of unauthorized access to the installation by providing the capability to detect forged, invalid, or unauthorized access documents/credentials.

Base Debarment Listing

SF will maintain a list of personnel barred from the installation. Will be used to ensure unauthorized personnel are not allowed access, and if applicable, issued a citation for trespassing when entry is illegally gained. May be combined and maintained in the same manner as lists documenting revoked base driving privileges or other privileges.

Active Vehicle Barriers (AVB)

Provides capability to physically impede and prevent a threat vehicle from unlawful or unwanted entry to DOD Installations. Most effective measure to stop a gate runner and are essential to preventing unauthorized access to the installation.

Gate Runner Procedures

1. Announce Gate Runner utilizing local SOP's
2. Activate an Emergency Fast Operate (EFO) button if applicable illegally may be prosecuted under 18 U.S.C 1382

3. Sound the alarm and notify BDOC
4. Provide vehicle description, registration number (LP #), number and description of occupants, direction of travel, any actions taken by vehicle, any other identifiers
5. Challenge/engage and/or detain the perpetrator/s
6. Secure evidence and crime scenes
7. Recover (return entry point to normal operations)
8. Report (process appropriate documents/personnel/evidence)

If suspect vehicle is not stopped by the barrier system, responding patrols will intercept the vehicle. BDOC will coordinate with local law enforcement agencies, as needed. BDOC will direct Restricted Area ECP's to close all vehicle gates (Alert crews and launch personnel will be granted vehicle entry without delay.)

NOTE: CHASE VEHICLES MAY BE PLACED AT ACCESS CONTROL POINTS
NOTE: AN ASSISTANT ENTRY CONTROLLER (OVERWATCH) WILL ALSO BE POSTED TO ASSIST THE ENTRY CONTROLLER

17b. CAN IDENTIFY RELATIONSHIP OF BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT CONDUCT INSTALLATION ENTRY/EXIT POINT CHECKS(IACP) AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Installation Entry/Exit Vehicle Checks (IEVC)

Installation commanders determine when, where and how to implement random checks of vehicles or pedestrians based on the results from the IDRMP (Integrated Defense Risk Management Process) and thorough crime trend analysis. May be delegated to the deputy installation commander or applicable group commander. If delegated, it must be identified in the IDP. The intent is to protect the security of the command and to protect personnel and government property.

Checks are not conducted merely to establish probable cause of suspected criminal activity. A locally devised computer program approved by the installation commander and the SJA is used to randomly select entry/exit point checks. The installation commander or their designee approves the list of entry/exit vehicle check timelines, which is sent to SF for implementation.

Entry/Exit Point Checks

The main purpose of an entry/exit examination is to prevent the introduction of weapons, illegal drugs, drug paraphernalia or other contraband and prevent the loss of classified information and government property. SF will utilize locally established procedures to conduct the inspection. Entry/Exit point checks will be recorded in the daily blotter. The inspection will be consensual. If an examination is declined, you must make a walk around check of the vehicle to look for any probable cause in plain view. If evidence is discovered in plain view, you now have probable cause. This evidence establishes the foundation for a search authorization

from the proper authorities (normally the installation commander or designee.) If no probable cause for a search is found, hold the individual and contact the SJA office for further advise. Vehicle operators' information should be documented for further processing.

17c. CAN IDENTIFYRELATIONSHIP OF BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT CONDUCT ALARMED RESPONSE AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Alarmed Response

SF are the enterprise leader for delivering armed response capabilities and must be able to respond appropriately to routine and emergency situations. Security Response Teams (SRT) are required at PL-1, PL-2 and PL3 resources (e) SRT's are response elements made up of two properly trained, armed, and equipped SF personnel.

Response to Alarms

Response time limits for patrols vary according to the type of patrol and resources being protected. Response times will be clearly defined in the Integrated Defense Plan (IDP). The speed of emergency vehicles should be reasonable and proper with due regard for actual and potential hazards. SF will be held responsible for any reckless disregard for the safety and wellbeing of others while responding to alarms.

Response Considerations Upon Arrival (OPEN FACILITY) **Procedures may vary based on local SOPs**

Notify BDOC upon arrival. Establish a 360-degree perimeter (control area.) Assess the situation and determine whether it is hostile or non-hostile. Make contact with alarm custodian and have them authenticate with BDOC. Confirm the reason for the alarm and notify BDOC. Conduct a joint sweep with the alarm custodian. Keep BDOC and other patrols informed of the status of the situation. Ensure the alarm is reset and confirm with BDOC.

Response Considerations Upon Arrival (CLOSED FACILITY) **Procedures may vary based on local SOPs**

Notify BDOC upon arrival. Establish a 360-degree perimeter (control area.) Assess the situation and determine whether it is hostile or non-hostile. A patrol will conduct a physical check of the facility looking for signs of forced entry. If forced entry is found, SF will conduct an interior search of the facility for suspects (Use MWD if available.) Once facility is cleared/safe, SF will conduct a walkthrough of the facility with the building custodian. If no signs of forced entry are found during the physical check of the facility, the building custodian will be contacted, and the alarm reset.

Alarm Response Building Positions

Point 1- To left of main entrance to facility
Point 2- Directly behind Point 1 *Large or odd shaped buildings may have additional points*
Point 3- Directly to right of point 2
Point 4- To right of main entrance to facility

Response to Protection Level (PL) Resources Considerations **Procedures may vary based on local SOPs**

- PL-1 At least one SF member dedicated for immediate internal response to the resource. At least one other SF member dedicated to the restricted area capable of responding immediately. An external two person SRT capable of responding immediately. An area supervisor
- PL-2 An internal two-person response team for immediate internal response. An external two-person response team capable of responding immediately. An area supervisor
- PL-3 At least two trained and equipped SF personnel dedicated for immediate internal response. An external two-person response

team capable of responding immediately

- PL-4 Owner/User will maintain primary security and entry control to PL-4 Aircraft and Resources. SF will provide armed response to incidents and alarms

17d. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT CONDUCT UNAUTHORIZED ENTRY PROCEDURES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Access Control

Designed to prevent unauthorized entry into protected areas such as Restricted Areas and Controlled Areas

Designed to prevent incidents such as:
Unlawful entry to aircraft
Sabotage or attempted sabotage to AF aircraft
A breach of aircraft security
Acts of vandalism directed at AF priority resources
Hijacking or attempts
Unauthorized entry into a launch facility
Damage to aircraft
Robberies involving weapons/munitions

Circulation control procedures are designed to detect hostile actions within areas, prevent unauthorized removal of material, and provide for safe movement of personnel and resources.

For owner/user integrations is control over resources and assets (LRS owns/uses base armory, OG owns/uses the flight line). Commanders at all levels are responsible to secure unit assets with organic resources. Typically, owner/user personnel provide detection and security as part of daily operations. Owner/user personnel, while performing security, are not considered sentries or security guards.

Security Forces Actions
Contact BDOC upon observing suspicious personnel/activity within a restricted area. Initiate contact with suspect to investigate further (may initiate a challenge.) Take action to block the suspect from contacting or observing the resource being protected. Obtain status of suspects restricted area badge and reason for being in the restricted area. If member is not authorized to be in the area, detain, apprehend, or escort as needed. Update BDOC and move suspect to an alternative location in order to conduct a full search if applicable. A sweep/purge will be conducted of the restricted area for any signs of tampering or hostility.

Nuclear Resources
All possible actions, including the use of deadly force may be used to stop unauthorized entry to or seizure of nuclear weapons storage areas, nuclear weapons transport vehicles or a nuclear weapon system. All necessary actions must be taken to ensure immediate reoccupation and securing of any close in security area penetrated. SF will not be deterred by bystanders.

17e. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT UTILIZE DURESS PROCEDURES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Duress- Threats, violence, constraints, or other action brought to bear on someone to do something against their will.

Duress Codes -Word or words used during normal conversation to indicate duress. Provide a means for authorized owner/user personnel to pass a pre-designated word to the alarm monitor to indicate duress. All personnel who work in or who are authorized to enter restricted areas must know the duress codes. SF will have a locally devised duress code system to communicate between posts, patrols and the BDOC controller to ensure assistance, should the need arise. The BDOC controller must remain alert at all times, should a duress situation arise it will be handled expeditiously and effectively.

Duress Alarms- Used when duty personnel are forced to yield protected items to unauthorized persons. Configured to allow on duty personnel to activate it without arousing the intruders suspicion. Must be located to permit hidden activation by on duty personnel. Ensure alarms are reset after termination of the duress incident.

Two Types of Duress Indicators:

Active Duress -When an individual uses an existing system to indicate duress. Such as passing the duress word in a restricted area or pressing a duress button in the armory.

Passive Duress- When an individual does not follow established procedures. Such as mis-authenticating twice or failing to use established ECPs on the flightline.

For duress response the local guidance and instructions will cover how to perform duress procedures. Most involve establishing 360 security, challenging individuals, separating individuals, and acquiring reason for duress.

17f. CAN IDENTIFY RELATIONSHIP OF BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT UTILIZE SIGN, COUNTERSIGN AND EMERGENCY RESPONSE CODES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Sign/Countersign

Signs that personnel must give in response to other corresponding signs. Used to facilitate entry into restricted areas during security responses and emergencies or validate security status. Examples are code words, challenge/password, number combination, running password, recognition signals (near-far and day-night). If using number combinations, odd numbers work best because person receiving the sign cannot return the same number and be correct. If wrong countersign is passed back, challenge individual/s.

Code Words

Used in the same manner and under the same circumstances as the sign countersign.
The word counterword could be "Square" and "Baseball."

The Entry Controller says "Square" and the individual replies with "Baseball."

A one-word code word could be "Fireball"

The Entry Controller asks, "What is the code word?" and the individual replies with "Fireball."
ENSURE CODE WORDS ARE NOT DISCLOSED TO UNAUTHORIZED PERSONNEL

Emergency Response Codes

SF utilize response codes to rapidly and efficiently communicate status between BDOC and on duty personnel. Response codes pertain to various SF functions and duties (Incidents, meal breaks, latrine breaks, Driving, Status, etc.)

Dispatch Response Codes

Code 1
(Non-Emergency) **a.** Respond in compliance with all traffic regulations **b.** Do not utilize lights or siren **c.** Use most direct route

Code 2
(Urgent) **a.** Requires an immediate response to a non-life-threatening emergency **b.** Utilize lights only

Code 3
(Emergency) **a.** Requires an immediate response to a life-threatening emergency or emergency involving AF priority resources **b.** Utilize lights and siren. If the emergency lights and siren put SF, victims, or bystanders in peril, turn them off at a safe distance from the scene

Code 4 (Wants and Warrants)
If a person or a vehicle comes back "Code 4" that means that they have outstanding wants and warrants. BDOC will direct the SF member to "secure their mic" prior to relaying the positive "Code 4." BDOC will also dispatch additional patrols to the location to assist **d.** If the entering agency does not request extradition, SF will accomplish an AF Form 3907 and deny access/escort off the installation. If the entering agency will extradite, detain, complete AF Form 3907 and transport to holding cell. Once civilian LE takes custody, accomplish DD Form 2708 and AFJIS report.

17g. CAN IDENTIFY RELATIONSHIP OF BASIC FACTS AND STATE GENERAL PRINCIPLES ABOUT CONDUCT BUILDING AND REPOSITORY CHECKS AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

Conduct Building and Repository Checks

One of the Security Forces responsibilities under the Installation Security Program is to make security checks of buildings, repositories, and other areas. Building checks must be performed to ensure security for high value assets and a proactive crime prevention measure is in Place. These checks offer Defenders an opportunity to learn building layouts, vulnerabilities, likely avenues of approach/escape, and safe efficient response routes. Building checks should be conducted both during duty and nonduty hours to provide opportunities for Defenders to meet and interact with building occupants.

Building Check Procedures

Each installation normally has a locally produced building check sheet that list the facilities to be checked along with the frequency of the check (ex. twice a shift.) The check sheet normally includes an area to annotate the date, time, status of building, and the Defenders name who checked the facility. Defenders may check the same buildings/areas each day/each shift, so it is important not to set a predictable pattern. Vary the routes and approaches to each building as well as the times the facility is checked and be alert for suspicious vehicles and activity. Notify BDOC upon arrival before the start of the building check and upon completion of the building check (include status of building). During

hours of darkness try to stay out of well-lit areas while approaching the building. Physically check all doors and windows (also look inside) while looking for signs of forced entry (broken door/window, pry marks, open door/window.) For areas not within reach, look closely for signs of forced entry.

Forced Entry/Unsecure Building Procedures

If a Defender finds a building with signs of forced entry, they will take up a covered position and observe the building. BDOC will then be contacted and given the facts of the situation.)

BDOC will then dispatch back up patrols to set up a 360-degree cordon. Once cordon is established Defenders will search and clear the building (Utilize MWD if available.) If perpetrators are located, challenge and apprehend/detain them. Once building has been cleared, Defenders will conduct a walk through with the building custodian to see if theft or vandalism has taken place. If a Defender finds a building unsecure without signs of forced entry, follow the same procedures as above.

Restricted Area supervisors must conduct daily visual checks of all physical security facilities, boundary barrier systems, gates, and structures. All discrepancies will immediately be reported to BDOC.

UNIT 18 RESOURCE CONTROL DUTIES

18d. CAN IDENTIFY BASIC FACTS AND TERMS ABOUT PERFORM OR LEAD ABGD AND RESOURCE SECURITY DUTIES AND RECEIVE A MINIMUM PASSING SCORE OF 70% ON THE WRITTEN TEST

SF COMPOSITION AND RESPONSIBILITIES

ID forces protect resources that directly support the global DAF mission. SF are the enterprise leader for delivering ID armed response capability. On-duty SF response elements are required for restricted and controlled areas containing PL resources. They form a major part of the total capability for detecting, responding to, and neutralizing hostile actions under normal and emergency conditions. SF flights may vary in size based on the mission(s) they are required to execute. Personnel on each flight must know their individual responsibilities and must also have a working knowledge of all positions within the flight.

FLIGHT COMMANDERS

When authorized, an officer oversees supervision of each flight. They are responsible for all the flight does or fails to do. They ensure proper individual and collective training, equipping, conduct, and the welfare of the flight both on and off duty.

FLIGHT CHIEF

Normally senior noncommissioned officers (SNCOs), or civilian defender equivalent. Oversees the management of the flight, is directly responsible for leading, coaching and mentoring the Defenders assigned. Guide and supervise the flight sergeants, oversee flight operations during normal and emergency conditions. Responsible for the training, basic operation, and administrative functions of the flight.

FLIGHT SERGEANT

Tactical leaders who are responsible for flight operations during normal and emergency conditions. Responsible for the operation and training functions of the flight. Responsible for preparing and posting duty schedules and scheduling leaves.

Note: *Flight Sergeants, Flight Chiefs and Flight Commanders are responsible for ensuring posted forces understand their role in ID operations. Also responsible for executing ID operations and knowing the threats and any security gaps or vulnerabilities. At least one should check each post at least once during their shift.*

BASE DEFENSE OPERATION CENTER (BDOC)

The command and control (C2) center for ID operations during normal and emergency operations. Personnel assigned as a BDOC controller should be of the highest caliber because of its demanding nature and critical duties.

SQUAD LEADERS

Supervise and are responsible for conducting collective training of the squad and individual training. Training includes on-the-job and proficiency training requirements. Squad leaders supervise squads based upon site specific METT-TC factors and the ID force's ability to anticipate, deter, detect, assess, warn, defeat, delay, defend and recover.

AREA SUPERVISORS

Senior ID force personnel assigned to a specific Area of Operation (AO). They direct and manage the area security operation in support of PL resources and monitor the well-being of forces posted in the area. They must check every posted ID force member as frequently as possible.

ENTRY CONTROLLERS (EC)

ECs control entry to specific locations (e.g., installations, restricted areas, cordoned areas). ECs apply controls ensuring only authorized personnel are admitted to the areas for which they are responsible. **Assistant ECs** may be posted to conduct vehicle and personnel searches and assist ECs, as necessary.

FIRE TEAM (FT) LEADERS

They directly supervise team personnel. FT leaders are responsible for the collective training of the FT and individual training of FT personnel.

FIRE TEAMS

FTs consist of four ID force personnel on one team, or any combination of internal and external SRTs, and security patrols who come together to form a FT. FTs respond to threat situations and may work in smaller teams.

SECURITY RESPONSE TEAMS (SRT)

SRTs are required at all installations supporting PL-1, 2, or 3 resources. SRTs are response elements consisting of two properly trained, armed, and equipped ID force personnel. SRTs observe assigned resources and provide immediate response to alarms generated from IDS or personnel and incidents. SRTs must be capable of responding immediately, as defined in the IDP, to defeat the adversary before any negative effect against the resource occurs. If approved by the installation commander, two-person SRTs may be separated and work as single-person security patrols within their assigned area in order to facilitate area coverage and response to alarms. If separated, the two security patrols must join together as a two-person response element to respond to alarms within their assigned area.

Internal SRTs (ISRT)- are two-person teams dedicated to the interior of a restricted area. May be located external to the restricted area when located inside a facility (e.g., operational Ground Communication System within a Sensitive Compartmented Information Facility) or small geographic footprint (e.g., small fenced area).

External SRTs (ESRTs)- are two-person teams which may operate inside or outside of the restricted areas to which they are assigned.

Close-in-Sentry (CIS)- maintains surveillance over assigned areas of responsibility and alert the BDOC of any unusual situation in their area. Prevent unauthorized entry to or near their areas of responsibility and detect and apprehend unauthorized personnel and equipment.

Close Boundary Sentry (CBS)- is posted to provide security surveillance over the boundary of restricted areas or individual resources. IDS performs this function when available.

IMMEDIATE VISUAL ASSESSMENT SENTRIES

Provide surveillance over IDS sectors or zones when closed circuit television systems fail. Provide surveillance when an alarm monitor cannot see because of poor visibility or blind zones.

ALARM MONITORS

Alarm monitors are required to monitor IDS, may dispatch SF to alarms and make initial notifications. They may control entry to alarmed storage structures, alert aircraft shelters, and other facilities protected by IDS.

MILITARY WORKING DOG (MWD) TEAMS

Security of PL resources is one of the most important uses of MWD teams. Key players in a proactive security environment and should be used on a recurring basis to enhance detection and deterrence capabilities. MWD teams can operate independently or integrate with IDS and posted sentries, while providing search, initial response, and force multiplier capabilities. Unless performing explosive or narcotic detection, observation or listening post duties, MWDs should not be placed on static posts as this seriously degrades the dog's detection capability. Military Working Dogs should be used in installation security operations in the following ways: Sweeps of exterior and interior areas of observation and concealment, and avenues of approach to installations and restricted or controlled areas. Exterior sweeps should be conducted randomly, so as not to establish a pattern and extend beyond the immediate area of resources, possibly as far out as 1000 meters. Interior sweeps should be conducted on a random basis. Also, by conducting random vehicle inspections at installation, restricted area, or controlled area entry control points (ECP). To clear an area after an emergency response, ensuring all personnel have departed.

INSTALLATION SF PATROLS

Primary functions of installation SF patrols are to deter threats, serve as a means of detection and defeat adversaries to the installation. Limit patrol response to only that necessary to maintain good order and discipline.

Commercial Vehicle Inspector- performs inspections of commercial vehicles entering the installation and complete paperwork associated with the inspections.

Installation Access Control Overwatch Posts- prevents the ingress of vehicles attempting to enter the installation without proper authorization.

Town Patrol (Off-Installation Patrol)- is used to patrol areas frequented by military personnel and alert BDOC of any unusual situation in their area. Apprehend and transport military offenders from civil police to proper military control.

UNIT - 14 USE OF FORCE

14a. PLACED IN A TRAINING ENVIRONMENT, CAN IDENTIFY WHY AND WHEN THE TASK MUST BE DONE AND WHY EACH STEP IS NEEDED FOR APPLY CONCEPTS AND PRINCIPLES OF USE OF FORCE IAW PC II-14a

KEY TERMS

Objective Reasonableness-" The reasonableness" of a particular use of force must encompass the totality of circumstances and be judged from the perspective of a reasonable officer with the same training and experience. Judgment must be made with what we know at the time (not 20/20 hindsight).

Totality of Circumstances- Refers to any and all circumstances related to the scene, understanding that scenes are tense, uncertain, and rapidly evolving.

Imminent Threat- A dangerous or threatening situation which is about to occur or take place and is perceived to be unfolding.

Immediate Threat- One that can be delivered without delay and requires an instant response by a Defender to stop the threat or control the situation.

Force- An effort by a Defender to compel compliance, gain control or overcome resistance.

Less-lethal Force- Any use of force other than that which is considered deadly force and that involves physical effort to control, restrain, or overcome the resistance of another.

Justified Force- Defender demonstrates through articulation that the intensity, duration, and magnitude of force utilized was objectively reasonable given the totality of the circumstances.

Excessive Force- When the intensity, duration and magnitude of the force utilized is not deemed to have been objectively reasonable given the totality of the circumstances confronting the Defender at the time force was used.

Deadly Force- Any use of force that creates a substantial risk of causing death or serious bodily injury.

Escalation- The intensification of force in a situation meant to gain control.

De-escalation- Tactics and techniques used by Defenders to minimize the force needed or utilized during an incident in an effort to increase the likelihood of cooperation, collaboration, and compliance.

Stabilization- Evaluating the entirety of the situation and implementing the best tools and tactics in order to generate the advantage and restore compliance.

Note: *The goal for the use of force, as opposed to any other context (combat is to gain control of the situation or individual/s encountered when reasonable.*

GRAHAM V. CONNOR (1989)

This case (U.S. Supreme Court established the standard of "objective reasonableness" pursuant to the U.S. constitution (4th Amendment as the appropriate standard for assessing the use of force. The Court explained "the reasonableness" of a particular use of force must be judged from the perspective of a reasonable officer on the scene.

In Graham v. Connor the Supreme Court emphasized three factors affecting the use of force:

- The severity of the crime
- Whether the person poses an immediate threat to the safety of the officer or others
- Whether the person is actively resisting, or attempting to evade detention by flight

Graham v. Connor Story

Petitioner Graham, a diabetic, asked his friend, Berry, to drive him to a convenience store to purchase orange juice to counteract the onset of an insulin reaction. Upon entering the store and seeing the number of people ahead of him, Graham hurried out and asked Berry to drive him to a friend's house instead. Respondent Connor, a city police officer, became suspicious after seeing Graham hastily enter and leave the store, followed Berry's car, and made an investigative stop, ordering the pair to wait while he found out what had happened in the store. Respondent backup police officers arrived on the scene, handcuffed Graham, and ignored or rebuffed attempts to explain and treat Graham's condition. During the encounter, Graham sustained multiple injuries. He was released when Connor learned that nothing had happened in the store. Graham filed suit in the District Court under 42 U.S.C. 1983 against respondents, alleging that they had used excessive force in making the stop, in violation of "rights secured to him under the Fourteenth Amendment to the United States Constitution and 42 U.S.C. 1983."

USING FORCE

Defenders do not need to select the least intrusive or minimum force available, only a reasonable one. At times Defenders try to work within the belief that force is to be used only as a last resort rather than allowing their ability to utilize force which is reasonable and necessary to control the situation. If action is not taken or delayed the potential to utilize a higher level of force may become necessary.

On duty SF members draw from a reservoir of use of force options including:

- Displays of authority, verbal, and nonverbal communication.
- Various levels of non-Lethal force, and ultimately the use of deadly force.

Application of force encompasses three main elements of action and assessment:

- Tools
- Tactics
- Timing

THREAT ASSESSMENT (PRE-ASSAULT INDICATORS)

- Verbal threats, noncompliance, clenching, fist, constantly scanning
- Rubbing face or neck, stalling or hesitation, target glancing
- Rapid eye blinking, rolling up sleeves, stretching, squaring up

SECURITY FORCES PERCEPTION

SF use of force response is based off of the subject's action and the Defenders perception (Subject's action/Defenders perception/Defenders response).

SF may use the three elements listed below as guidelines in determining whether to use force (they are not defined in law):

Intent- The apparent or perceived mental state of the subject initiating an overt act (words or deeds).
Ability/Capability- The ability/capability of the subject to carry out a threatened action.
Opportunity- Is the action or threat SF perceive imminent but not necessarily instantaneous. ***Note:*** *The subject must be in a position where they can carry out the act or threat.*

SUBJECT BEHAVIORAL CATEGORIES

Compliant/Cooperative- Subject complies with SFs objective.

Resistant Passive- Exhibits the preliminary level of noncompliance and requires some degree of physical contact to obtain compliance.

Resistant Active- Subject exhibits physical defiance to SF control.

Assaultive Bodily Harm- Subject exhibits intent, capability, and opportunity of physical aggression that the Defender perceives is not lethal to him or others.

Assaultive Grievous Bodily Harm/Death- Subject exhibits intent, capability, and opportunity to inflict death or serious bodily harm to SF or others displaying the intent to use a weapon or taking a Defenders weapon.

SF RESPONSE TO SUBJECT BEHAVIOR

Compliant/Cooperative- SF utilize professional appearance, nonverbal actions and verbal requests and commands, handcuffing and control holds.

Resistant Passive- SF utilize strength to take physical control, including lifting, carrying, pain compliance control holds, take-downs and techniques to direct movement or immobilize a subject.

Resistant Active- SF utilize control holds and techniques to control the subject and situation, use of personal body weapons to gain advantage over subject.

Assaultive Bodily Harm- SF utilize devices or techniques to secure compliance and gain control of the situation, use of personal body weapons in self-defense and to gain an advantage over subject.

Assaultive Grievous Bodily Harm/Death- SF utilize firearms or any other available weapon or action in defense of self and others to stop the threat.

USE OF DEADLY FORCE

As with non-lethal force, the use of deadly force must meet the "objectively reasonable " standard. SF must be able to articulate why it was objectively reasonable based on their perception of the threat and the totality of the circumstances.

Standing Rules for The Use of Force (CJCSI 3121.01B, Enclosure L) authorizes deadly force for the following circumstances:

- Inherent right of self defense
- Defense of others
- Assets vital to national security
- Dangerous property
- National critical infrastructure
- Serious offense against persons
- Prevent escape of prisoner (if has committed or attempted to commit a serious offense)
- Arrest or apprehension

SPECIAL CONSIDERATIONS FOR THE USE OF FIREARMS AND DEADLY FORCE

When feasible, give an order to "HALT or STOP" before discharging a firearm. If subject is armed, and if feasible, give the order to "DROP THE WEAPON" before discharging a Firearm.

CBRN AND HIGH YIELD EXPLOSIVE OPERATIONS

The safety of innocent bystanders or hostages may be a relevant consideration in determining whether the use of deadly force is excessive or objectively reasonable.

LOCAL, HOST NATION LAWS, AND STATUS OF FORCES AGREEMENTS (SOFA)

Commanders may impose further restrictions on the use of deadly force to comply with local or host nation laws and status of forces agreements. Such restrictions must not unduly compromise U.S. national security interests and must be published in local installation instructions.

POST USE OF FORCE CONSIDERATIONS

Determine whether any person was injured by the use of force and render aid if needed (medical attention). Immediately tend to and request medical attention for the following use of force tools or techniques regardless of visible injury or complaint of injury.

Baton

OC spray

Electronic Control Device

Use of MWD

Use of force with a vehicle

Firearm

Ensure photographs are taken, providing a detailed account of the incident from the Defenders perspective including the following:

- Reason for initial contact, specific description surrounding the totality of circumstances, subject's actions to include statements made.
- Duration of subject's action, number of subject's involved, size and age, condition of subject as well as Defender, did force applied result in injury.

END OF BLOCK II