AIR FORCE DOCTRINE PUBLICATION 3-10

FORCE PROTECTION

U.S. AIR FORCE

19 November 2019

CURTIS E. LEMAY CENTER
FOR DOCTRINE DEVELOPMENT AND EDUCATION

AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-10 FORCE PROTECTION

CATALOG OF DOCTRINE TOPICS

Introduction to Force Protection
Force Protection (FP) Fundamentals
The Airman's Perspective on Force Protection

Command Responsibilities for Force Protection
Force Protection and Command Relationships in a Joint Environment
Legal and Law Enforcement Considerations during Force Protection Planning and Execution

Threats to the Air Force Mission (FP)
DOD Terrorism Threat Levels
Threat Objectives
Risk Management Process

Force Protection Planning

Force Protection Intelligence

Counterintelligence Support to Force Protection

The Force Protection Community

AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-10 FORCE PROTECTION

INTRODUCTION TO FORCE PROTECTION

Last Updated: 19 November 2019

Force protection (FP) doctrine is constantly evolving. It should guide us to effectively organize and employ through the complexities of counterinsurgency and steady-state operations, and help us re-learn the lessons of large-scale peer and near-peer conflict and competition in contested environments. As we continuously improve our airpower capabilities and capacities in air, space, and cyberspace, our ability to revolutionize force protection and incorporate new concepts and technologies will identify the new best practices that shape future force protection doctrine. The competition continuum that encompasses the range of military operations, from peacetime through large-scale combat, is always a consideration when determining the best practices for our Air Force. Consideration of peer and near-peer competition is a continuing necessity for doctrine as the Air Force supports the joint fight. Every Airman is an innovator and is integral to this continuous development process–we should all connect, share, and learn together to succeed. Force protection in a contested environment against a peer adversary requires the air component to be more adaptive, resilient, and agile in its deployment and employment plans and leadership philosophies.

The 21st Century has, thus far, been characterized by a significant shift in Air Force responsibilities and an increased exposure of its resources to worldwide threats. This point is underscored by the terrorist attacks of 11 September 2001 and ongoing operations worldwide. Today, potential opponents are less predictable, leveraging the increased availability of both high and low technology weapons, including weapons of mass destruction. The Air Force's ability to project US airpower requires protection from these threats at home, in transit, and abroad.

Due to the increased lethality of international and domestic threats, it is imperative the Air Force take strong measures to protect personnel and installations around the world, as part of a coordinated and integrated joint force. How the Air Force protects forces is critical to global engagement. An air expeditionary task force poised to respond to global taskings within hours should establish the capability to fully protect its forces.

Commanders at all levels should have an effective force protection program. Commanders are responsible for protecting their people and the warfighting resources necessary to perform any military operation. We are obligated by the moral necessity of protecting our Airmen to ensure FP is a part of Air Force culture.

Understanding and using FP doctrine will help ensure the successful protection of people and resources.

FP supports combat support and its supporting capability of "Protect the Force." Protecting Department of Defense (DOD) personnel and resources is critical to the Service's ability to perform its mission.

FORCE PROTECTION DEFINED

Joint doctrine defines FP as "[p]reventive measures taken to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information" (Joint Publication 3-0, *Joint Operations*). FP is a fundamental principle of all military operations as a way to ensure the survivability of a commander's forces.

A comparison of the joint definition with the North Atlantic Treaty Organization (NATO), definition is instructive. NATO doctrine explains that "[t]he operational environment may have no discernable 'front-lines' or 'rear area' and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities."[1] Consequently, NATO defines FP as "[m]easures and means to minimize the vulnerability of personnel, facilities, materiel, operations, and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success."[2]

---

[1] Allied Joint Publication 3.14, *Allied Joint Doctrine for Force Protection*.
[2] Ibid.

AIR FORCE DOCTRINE PUBLICATION (AFDP) 3-10 FORCE PROTECTION

FORCE PROTECTION FUNDAMENTALS

Last Updated: 19 November 2019

All Airmen should know the fundamental aspects of force protection (FP) to safeguard their own lives, those of fellow Airmen and joint Service members, and valuable Department of Defense resources. Key to the Air Force view of FP is the protection of its people, the prime asset of the Service. Further, every Airman is expected to contribute to FP as both a sensor and as a warrior, prepared to protect and defend operations and assets.[3]

Effective FP is more than just a law enforcement function. Prior to the 1996 bombing of Khobar Towers in Saudi Arabia, the closest term to "force protection" used with any frequency was "antiterrorism" (AT), which was often viewed as a law enforcement-only function with some focus on individual protective measures.[4] Some have even confused FP as being synonymous with antiterrorism, hence the erroneous term "AT/FP." FP is much broader in scope, serving as the overarching ends integrating all programs and efforts relating to defense against hostile actors. FP includes force health protection, which supports FP and includes all measures to provide for the health and safety of Service members. Security Forces, augmentees, and owner or user personnel (e.g., personnel working in maintenance and operations on and around a flightline) provide FP. Personnel involved in information fusion operations provide a threat picture by integrating all-source information. This shapes decision-making through intelligence preparation of the operational environment. Civil engineers design physical security improvements; provide planning, training, and response capabilities to deal with force protection-related incidents; and provide explosive ordnance disposal capabilities. Medical and emergency management personnel conduct presumptive identification for the presence of chemical, biological, radiological, and nuclear agents. Communications specialists integrate evacuation notification systems.[5] Operations

[3] While this publication refers to all Airmen as "warriors", military Airmen and Air Force civilian employees have distinct duties and obligations under the law of war. Further, Air Force chaplains and Air Force medical personnel must also act in a manner consistent with their noncombatant status. While integrated defense relies on the ability of all Airmen to contribute to the defense of their installation, each individual must do so in a manner consistent with any applicable limitations required by Department of Defense (DOD) policy, US law, and the law of war.

[4] DOD Instruction 2000.12, *DOD Antiterrorism Program*.

[5] AFDP 4-0, *Combat Support*.

security (OPSEC) is also a key component of FP. These are only examples of the breadth of FP in the Air Force.

Every Airman is a sensor, and protecting the force is everyone's duty.[6] All Airmen are responsible for FP at all times. This responsibility can stress available personnel and resources. In the end, commanders should balance mission accomplishment with FP and embrace the "every Airman is a warrior" culture, enlisting the whole force in protecting or defending an air base. All military Airmen should be trained and equipped to protect and defend the base against threats, and commanders should be identified to lead them in the effort. This includes basic ground combat skills training (e.g., weapons familiarization, self-aid / buddy care), and other relevant training required to prepare Airmen to better protect themselves and the base. Additionally, all Airmen should be trained to recognize and report chemical, biological, radiological, and nuclear (CBRN) hazards, which can be difficult to detect and may not always be preceded by a recognizable hostile incident. To counter the increasing threat of small unmanned aircraft systems (SUAS), Airmen should understand the need to direct attention, report an incident, observe, notice, and execute actions against SUAS.

FP is multi-dimensional, providing multi-layered protection of forces and resources. It covers actions at home station, in transit, and at deployed locations. It includes not only protecting military members and civilian employees, but also their families, contract employees, and visitors while on an installation.[7] This functional expertise includes intelligence collection; awareness and reporting by all Airmen, on and off duty; detection of and protection from CBRN threats; physical security enhancements; armed defense; law enforcement liaison; and numerous other areas of expertise.[8] This multi-layered protection extends awareness and influence as far forward as possible, while simultaneously providing in-depth protection to Department of Defense personnel and resources. This maximizes the ability to disrupt attacks and provide the earliest warning possible, while ensuring the best protection for the Service's most valuable assets, its people, through close-in security, with proper implementation of integrated defense. The end result is Air Force forces able to conduct their missions with the best protection available, based on risk management, wherever the mission is.

FP requires a global orientation because of the joint force's worldwide presence and the Air Force's ability to move quickly across great distances in the pursuit of theater and national objectives. Deploying personnel and those traveling for other reasons should focus on their changing environments. For example, they should be aware of the assessed threat at their home station and at each location they will transit, examine the vulnerabilities associated with their travel, and develop a personal protection plan.

---

[6] Quotation of James G. Roche, Secretary of the Air Force, 2001-05.

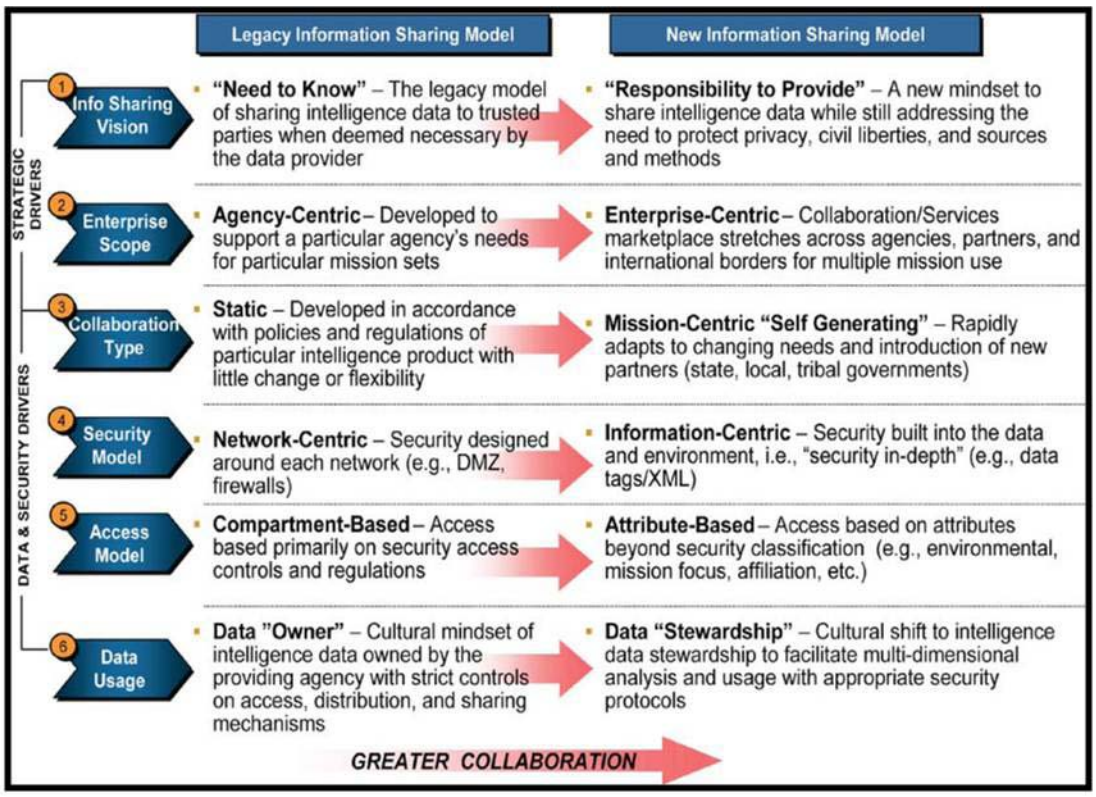
[7] DOD Instruction 2000.12, *DoD Antiterrorism (AT) Program*, establishes the responsibilities of geographic combatant commanders for force protection.

[8] See AFDP 3-40, *Counter Weapons of Mass Destruction (WMD) Operations*.

Effective intelligence, surveillance, and reconnaissance (ISR); counterintelligence; and liaison efforts are critical to identifying, analyzing, and disseminating threat information to commanders and ensuring FP. Threats may include conventional military units, special forces, foreign intelligence agents and services, terrorist groups, aggressive civil populations, criminal elements, extremist groups, or insider threats operating in, through, and across multiple domains. The enemy may use weapons such as improvised explosive devices (IEDs) or vehicle borne IEDs, mortars, rockets, man-portable air defense systems, computer viruses, CBRN material and agents, explosive ordnance, and small arms. Tactics may include conventional as well as asymmetrical methods. In concert with OPSEC requirements, commanders should develop critical information requirements to guide force protection intelligence (FPI) work supporting their decision-making and operations. FPI is analyzed, all-source intelligence information that, when integrated or fused with other FP information, provides an assessment of the threats to DOD missions, people, or resources. FPI is proactive and drives FP decisions in support of commander's intent. Personnel at all levels should coordinate with cross-functional counterparts (e.g., intelligence, Air Force Office of Special Investigations [AFOSI], security forces, installation emergency managers, medical health community, weather, etc., as well as the counterparts to these entities in other Services in theater and local or host nation forces) to share information and ensure FPI requirements are satisfied in accordance with DOD and Air Force guidance. Constant liaison with local counterparts and host nation forces also enhances cooperation and willingness to share information, especially in crisis situations.

The figure, "United States Intelligence Community Information Sharing Strategy," portrays an information sharing strategy used in the ISR community, illustrating the importance of this cooperation necessary for intelligence to support FP. **FP practitioners use new technology to enhance capabilities.** Technology offers force protectors advantages in speed, range, and effectiveness to assist them in meeting the demands of a changing operational environment. For example, use of motion sensors, thermal imaging cameras, and night vision devices can enhance tactical situational awareness for base defense. However, none of these technologies can perform FP alone. As technology evolves, so do the tactics of adversaries, necessitating changes in the response to threats. FP requires continued vigilance by the members of the force being protected, with technology acting to enhance their capabilities, not to replace them.

FP is both an individual and a command responsibility. Individuals should know the assessed threat against them and the vulnerabilities at their current location, along their route of travel, and at their destination. They should also know and implement individual protective measures. In addition, individuals should immediately report suspicious activities or occurrences to the nearest security forces, AFOSI or joint equivelant, or local law enforcement officer. Immediate reporting increases the chance that information collected is analyzed and turned into intelligence to support the commander.



United States Intelligence Community Information Sharing Strategy

---

THE AIRMAN'S PERSPECTIVE ON FORCE PROTECTION

Last Updated: 19 November 2019

"AIRMINDED" FORCE PROTECTION (FP)

Airmen normally think of airpower and the application of force from a functional rather than geographical perspective. Airmen do not divide up the battlefield into areas of operation as do surface forces.[9] Airmen typically approach battle in terms of the effects they create on the adversary, rather than on the nature and location of specific targets.[10] This approach normally leads to inclusive and comprehensive perspectives that favor strategic solutions over tactical ones. These perspectives extend to the Service's views on FP and its application to the joint fight.

How Air Force forces are commanded and organized to execute FP responsibilities is influenced by this Airman's perspective. Because of the strategic nature of airpower operations in support of the joint fight, Airmen have developed a distinct perspective. General Henry "Hap" Arnold referred to this *Airman's perspective* as "air-mindedness."[11] This airmindedness reflects the range, speed, and capabilities of air, space, and cyberspace forces, as well as threats and survival imperative to supporting joint forces. The Airman's perspective is an approach that shapes the conduct of operations and training to maximize operational effectiveness. Airmen should use their Airmen's perspective to drive how FP is applied in support of joint operations.

---

[9] Dr. Dale L. Hayden, "Air-Mindedness," *Air & Space Power Journal*, Winter 2008.
[10] AFDP 3-0, *Operations and Planning*.
[11] Gen Henry H. "Hap" Arnold, *Third Report of the Commanding General of the Army Air Forces to the Secretary of War* (Baltimore, Md: Schneidereith, 12 November 1945), 70.

COMMAND RESPONSIBILITIES FOR FORCE PROTECTION

Last Updated: 19 November 2019

Centralized control and decentralized execution of force protection (FP) measures and resources are essential to protect forces against threats worldwide. FP is a task for every commander at every level. Clarity of command responsibilities for FP is essential for a comprehensive, unambiguous, and integrated response. Integration of all aspects of FP, including interoperability with civilian command and control systems, should enable commanders to react quickly to threats. FP commanders should understand the legal basis of their responsibilities and jurisdictions. Discussion of FP command responsibilities begins above the Air Force organizations in a joint force because of the top-down guidance that permeates the military in support of FP.

THE ROLE OF THE GEOGRAPHIC COMBATANT COMMANDER

FP is not exclusively a Service responsibility. According to both the Unified Command Plan and Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, **geographic combatant commanders (GCC) have the overall requirement to establish and implement FP in their areas of responsibility (AORs).** GCCs exercise authority for force protection over all Department of Defense (DOD) personnel (including their dependents) assigned, attached, transiting through, or training in the GCC's AOR, except for those for whom the Department of State (DOS) Chief of Mission (COM) retains security responsibility.[12] Examples of the latter include air attachés and Marine Corps embassy security group personnel. Additionally, GCCs develop and maintain memoranda of agreement with COMs that delineate security responsibility for DOD personnel based on whether the COM or the GCC is in the best position to provide FP. This is referred to as "proximity." Examples of this include US military personnel attending a foreign nation's defense college or Air Force personnel supporting military cargo aircraft at an international airport. Although the GCC is ultimately responsible, the GCC can work with the US Embassy to assume FP support duties to include intelligence sharing and threat warning.

[12] DOD Instruction 2000.12, *DoD Antiterrorism (AT) Program*.

Tactical Control Authority for Force Protection

GCCs have the authority to enforce appropriate FP measures to ensure the protection of all DOD elements and personnel subject to their control within their geographic AORs. This includes personnel on temporary duty, with the exception of DOD personnel for whom the COMs have security responsibility. This authority includes tactical control (TACON) for FP over military personnel within a GCC's AOR.

Further, TACON for FP authorizes the GCC to change, modify, prescribe, and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements, and submit budget requests to parent organizations to fund identified corrections. The GCC may also direct immediate force protection condition measures (including temporary relocation and departure) when in his or her judgment such measures must be accomplished without delay to ensure the safety of the DOD personnel involved. Persons subject to TACON for FP of a GCC include regular and Reserve Component personnel (including National Guard personnel in a Title 10, US Code, *Armed Forces,* status) in the AOR.

There are two similar terms that affect air mobility forces: TACON for FP and protection. TACON for FP is an explicit authority and responsibility of a GCC for all US forces physically present within the assigned AOR (except for those for whom the DOS COM retains security responsibility). Simultaneously, protection of assigned and attached forces is an inherent responsibility of all commanders. Airlift forces deployed to or transiting through a GCC's AOR are subject to the TACON for FP standards established by the GCC and the force protection measures established by their Service chain of command. For example, Air Mobility Command (AMC) is the the Air Force Service component to US Transportation Command (USTRANSCOM), and has airlift assets forward deployed in the US Central Command AOR. Although the aircraft are staged in the Middle East, the commander, AMC (AMC/CC), as the commander of Air Force forces, is responsible for securing these assets during mission execution. The AMC/CC, per Joint Publication 3-36, *Joint Air Mobility and Sealift Operations*, has determined that Phoenix Ravens, specially trained Security Forces who travel with the aircraft, are required to support these missions. Therefore, Phoenix Ravens are forward deployed with these assets to secure the aircraft on missions. The protection of these aircraft and their personnel at their beddown location, however, remains an installation commander responsibility.

Although GCCs may delegate authority to conduct the FP mission, they may not absolve themselves of their responsibility for its accomplishment. Authority to conduct the FP mission may be limited by the establishing authority and applicable regulations and law.

Force Protection in US Northern Command

In most theaters, the senior DOD member serves as the combatant commander and assumes FP responsibilities. In US Northern Command's (USNORTHCOM's) AOR,

where the Secretary of Defense and other senior DOD officials outrank the USNORTHCOM commander, the combatant commander maintains responsibility for FP. While this is a unique situation for USNORTHCOM, the principle is the same–there must be a commander responsible for the protection of DOD assets in the USNORTHCOM AOR to ensure unity of effort, and that commander is the commander, USNORTHCOM. The statutory requirements of the military departments to support USNORTHCOM are the same as in any other theater, including supporting the USNORTHCOM FP mission.

USNORTHCOM executes a comprehensive all-hazards approach to provide an appropriate level of safety and security for the DOD elements (to include the Reserve components, DOD civilians, family members, and contractors supporting DOD at DOD facilities or installations), resources, infrastructure, information, and equipment from the threat spectrum to assure mission success. The authorities of commanders in the USNORTHCOM AOR are similar to those of commanders in other AORs.

FORCE PROTECTION AND COMMAND RELATIONSHIPS IN A JOINT ENVIRONMENT

Last Updated: 19 November 2019

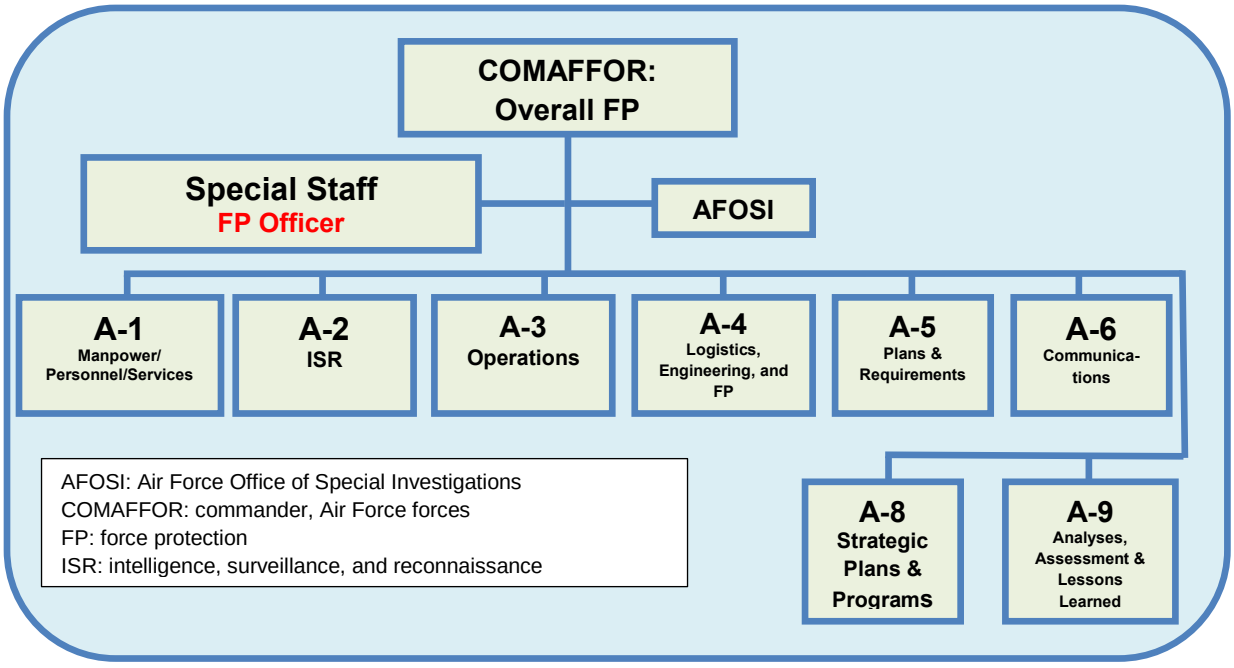
Since protecting the force is an overarching mission responsibility inherent in the command of all military operations, joint force commanders (JFCs) should consider force protection (FP) in the same fashion they consider other aspects of military operations, such as movement and maneuver; intelligence, surveillance, and reconnaissance; employing firepower; sustaining operations in a chemical, biological, radiological, and nuclear environment; environmental conditions; and providing command and control during the execution of operations across the competition continuum. The geographic combatant commander (GCC) or a subordinate joint task force commander can delineate the force protection measures for all Department of Defense (DOD) personnel not under the responsibility of the Department of State. If a JFC designates command of an installation to a specific Service component commander, that commander has FP responsibility over all personnel on that installation, regardless of Service or status. For instance, if an Air Force commander is given FP responsibility for an installation, it is his or her responsibility to coordinate FP operations with commanders in adjoining or surrounding geographic areas; this includes intelligence sharing and deconfliction of operations that span the seams between operational areas.

The Service authority of administrative control (ADCON) is used to support various measures of FP, but is not the appropriate term to describe where the responsibility for implementation lies. For example, each Service may have ADCON responsibility to equip its personnel deploying to a hostile environment with appropriate body armor, but the requirement to wear that armor, and under what circumstances, is the responsibility of the commander on the ground at the deployed location, as these are operational, not administrative, decisions. As the JFC normally delegates operational control to the commander, Air Force forces (COMAFFOR) for all Air Force forces assigned or attached, the COMAFFOR normally exercises tactical control (TACON) for FP over those forces. TACON for FP over Air Force forces also resides with the joint commander of another Service who has Air Force forces attached with specification of TACON for a given responsibility.

COMMANDER, AIR FORCE FORCES

In any operation in which the Air Force presents forces to a JFC, there will be a designated COMAFFOR who serves as the commander of US Air Force forces assigned or attached to the US Air Force component. The COMAFFOR, with the air expeditionary task force, presents the JFC a task-organized, integrated package with the proper balance of force sustainment and force protection elements. This applies on installations when the JFC has designated an Air Force officer as the base commander, i.e., when the Air Force is the primary occupant of a base.[13]

Commanders at appropriate subordinate echelons (such as wing, group, and squadron level) retain ultimate responsibility for protecting people and property subject to their control and have the authority to enforce security measures. To this end, those commanders should ensure FP standards are met and make it an imperative to have an effective force protection program. These commanders face three major FP challenges: planning for FP integration and support as tasked in applicable operational plans, training for FP, and providing FP for those interests within their influence. These commanders have the added responsibility of accomplishing FP planning for the units identified to deploy to their location during contingency operations. Commanders should designate a member of their staffs as the integrator of FP subject matter experts to establish guidance for, program for, and manage FP requirements for their organizations. The figure, **"**COMAFFOR Staff with FP Officer Location Identified," illustrates a notional COMAFFOR staff with the FP officer location identified.



COMAFFOR Staff with Force Protection Officer Location Identified

[13] Joint Publication 3-10, *Joint Security Operations in Theater*, Chapter II, para 3.b.(8).

LEGAL AND LAW ENFORCEMENT CONSIDERATIONS DURING FORCE PROTECTION PLANNING AND EXECUTION

Last Updated: 19 November 2019

Force protection (FP) fundamentals are applied in many different operational environments and organization command structures. In the course of planning, commanders should maintain an awareness of legal constraints that may affect operations. Information relevant to the use of force is contained in international law, US law, host nation law, the law of war, and established restrictions of movement, quarantine, and the rules of engagement or rules for the use of force. Together, these laws and rules regulate the status and activities of forces across the competition continuum. Below are some legal requirements a commander should consider, depending on where force protection measures are being implemented.

TYPES OF JURISDICTION

Depending upon where an incident occurs on a continental US installation or within the base boundary, jurisdiction may differ as installations may have more than one type of civilian criminal jurisdiction. For instances involving areas under government control where the Air Force does not exercise exclusive federal jurisdiction, commanders should work closely with the staff judge advocate and relevant authorities to establish protocols for handling civilians. When an installation is located within a foreign nation, jurisdiction may be governed by the terms of a status-of-forces agreement or other agreement with the particular host nation. Likewise, in these areas where authority and jurisdiction constraints prevent organic security forces from patrolling or otherwise occupying areas outside the installation's recognized base boundary but within the base security zone, commanders should apply risk management to minimize risk exposure to assets and personnel. They should also coordinate FP requirements with local authorities and adjacent friendly forces.

LEGAL CONSIDERATIONS FOR HOMELAND OPERATIONS

In the US, commanders publish and enforce regulations to protect installation resources and force protection intelligence (FPI) is vital to painting an accurate picture for a commander to better anticipate and plan against threats. However, due diligence should

be given to intelligence oversight issues when carrying out the FPI process. The duties and obligations placed on Department of Defense (DOD) intelligence organizations to protect the rights of individuals stem from the US Constitution, Presidential Executive Order 12333, *United States Intelligence Activities*, and DOD Manual 5240.01, *Procedures Governing the Conduct of DOD Intelligence Activities*, which spells out how the Presidential Executive Order applies to defense intelligence activities. In a similar manner, DOD members not part of the intelligence community have obligations stemming from the US Constitution, Title 5 of the US Code, *Government Organization and Employees* (the "Privacy Act"), and DOD Directive 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*. Specific Air Force guidance is contained in Air Force Instruction (AFI) 14-404, *Intelligence Oversight*.[14]

Domestic use of unmanned aircraft systems for force protection raises unique legal and policy issues and requires approval from appropriate authority. Before using unmanned aircraft systems for domestic FP, commanders should consult with their legal advisors to ensure they have permission to do so. The primary objective of a commander's intelligence oversight program is to ensure units and staff organizations conducting intelligence activities do not infringe on or violate the rights of US persons. Commanders should implement safeguards to ensure the conduct of force protection activities conform to US law, executive orders, and DOD directives. These tools ensure that FP operations do not violate intelligence oversight directives. Likewise, commanders should understand the degree of control they have over their installations, and be familiar with the concepts of title and jurisdiction.[15]

In the US, commanders are responsible for protecting installation resources, especially personnel. Force health protection measures such as restriction of movement (ROM) are an important aspect to this protection. Due diligence should be given to planning for ROM in regard to legal and law enforcement implications on an installation when carrying out quarantine or isolation measures.[16] ROM is used to prevent the introduction, transmission, and spread of communicable diseases or any other hazardous substances that pose a threat to public health and safety. These references also authorize the Director of the Centers for Disease Control and Prevention (CDC), through delegated authority of the Secretary of the U.S. Department of Health and Human Services, to take public health measures the Director deems necessary

---

[14] Air Force oversight of intelligence activities not only applies to intelligence organizations but also extends to non-intelligence units and staffs when they are assigned an intelligence mission and to personnel doing intelligence work as an additional duty, even if those personnel are not assigned or attached to an intelligence unit or staff. See AFI 14-404, *Intelligence Oversight*.

[15] For a more detailed discussion of the types of jurisdiction in the homeland, see *The Military Commander and the Law*. Sources for the DOD intelligence oversight program and the types of jurisdiction come from multiple sources: Presidential Executive Order 12333, DOD Manual 5240.01; US Constitution, Art. I, §8, cl. 17; US Constitution, Art. VI, cl.2; 40 U.S.C. §§3111 and 3112; *Greer v. Spock*, 424 US 828 (1976); and AFI 32-9001, Acquisition of Real Property.

[16] Quarantine and isolation are types of restriction of movement that can in certain circumstances be imposed by a military commander for individuals within the scope of the authority of the commander.

regarding facilities owned by the Federal Government within the US.[17] The Director of the CDC is also empowered to provide further guidance on public health measures that may include oral authorization for military commanders to quarantine individuals not within their scope of authority until a formal written order is issued by the CDC. Commanders should implement safeguards and guidance to address law enforcement and legal requirements to protect personal rights and at the same time protect installation resources. Specific Air Force guidance is contained in AFI 10-2519, *Public Health Emergencies and Incidents of Public Health Concern*.

When encountering FP issues in the US, commanders should consider the unique laws, challenges and issues for homeland operations.

---

[17] Presidential Executive Order 13295.

THREATS TO THE AIR FORCE MISSION (FORCE PROTECTION)

Last Updated: 19 November 2019

The threats facing the Air Force are broad and extensive. They range from powerful state actors with the full range of conventional and chemical, biological, radiological, and nuclear (CBRN) weapons delivered by sophisticated means to dangerous and ingenious non-state actors with inventive and asymmetric methods of delivering scalable harm to our forces. Such threats can create an unpredictable environment capable of inflicting catastrophic damage with or without notice. Consequently, Air Force personnel, aircraft, satellites, equipment, installations, operating locations, and, by extension, the Air Force mission are vulnerable to a wide variety of threats. This potentially daunting prospect demands force protection (FP) awareness and education at all levels and effective FP measures that are implemented through a coherent and coordinated FP command structure.

FORCE PROTECTION THREAT SPECTRUM

Prior to the attack on Khobar Towers in June 1996, the largest terrorist strike against US forces occurred on 23 October 1983 when two large vehicle-borne improvised explosive devices (VBIEDs) struck separate buildings housing US and French military forces in Beirut, Lebanon, killing 241 US military personnel. The VBIEDs were estimated at 15,000 to 21,000 pounds of TNT equivalent. In the Khobar Towers attack, a truck laden with 20,000 pounds of TNT was detonated, destroying the building and killing 19 Americans. In another scenario in 2003, three housing complexes were simultaneously attacked in Riyadh. In this case, trucks loaded with explosives were driven behind vehicles designed to penetrate the compound defenses. In each case, the attackers appeared to have placed little priority on their own survival.

It is the commander's responsibility to recognize threats to the Air Force and its mission across the competition continuum that encompasses the competition continuum and therefore consider the intentional objectives of threat actors. There are a variety of

threats facing the Air Force. Threats may arise from terrorists or insurgents, insiders, criminal entities, foreign intelligence entities, opposing military forces, or violent activist organizations.

US forces should consider the potential of an attack from an insider threat. On 27 April 2011, an Afghan air force pilot used his pistol to kill eight Airmen and one American contractor at Kabul International Airport. After a gun battle with two US officers, the attacker was killed by Afghan quick reaction force (QRF) members. This type of insider attack, known as a green-on-blue attack, began as an adversary tactic in 2008, and hit a peak in 2012, with 44 incidents. To mitigate risk of additional green-on-blue attacks, military leaders in Afghanistan instituted the Guardian Angel program, which provides a specially trained and dedicated armed overwatch to protect military advisors and personnel from insider threats and attacks. The US casualties were supporting the Afghan government as part of a North Atlantic Treaty Organization-led International Security Assistance Force in Afghanistan.

The examples in this section demonstrate that, in addition to addressing the threats below, Airmen should continually consider “what if” scenarios to counter potential future threats. Tactics and procedures introduced in one theater could be seen again in other regions and may result in increased FP measures due to the threat of attack which could affect ongoing operations.

At approximately 2200L on 14 September 2012, 15 heavily-armed Taliban insurgents dressed in US Army uniforms breached the eastern perimeter of Camps Bastion, Leatherneck, and Shorabak in Afghanistan undetected. They split into three teams of five men each, and commenced a coordinated attack on the Camp Bastion airfield. US and coalition personnel present on the airfield responded immediately, and the US and United Kingdom (UK) QRF made contact with the enemy shortly thereafter, beginning an engagement lasting into the early hours of 15 September 2012. The resulting friendly casualties and damage included two US personnel killed in action, eight US personnel wounded in action (WIA), eight UK personnel WIA, one civilian contractor WIA, six aircraft destroyed, eight aircraft damaged, and multiple other facilities and resources damaged. The QRFs, supported by US and UK personnel and helicopters, killed 14 of the Taliban attackers and wounded the remaining attacker, who was detained and interrogated. Only heroic action by US and UK forces on the scene prevented greater loss of life and equipment.

Types of Threats

In addition to those known threats, there is the paradox of countering unknown threats. The types of threats listed below provide general categories; this list is not exhaustive, but can be used as a guide.

- **Conventional Threat**—Regular military forces supported by a recognized government including air, land, maritime, and space forces.

- **Unconventional Threat**—This threat encompasses a broad spectrum of military and paramilitary operations predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape networks.

- **Terrorism Threat**—This threat involves the calculated use of violence or threat of violence to instill fear and is intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Acts of terrorism are often planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists, and erode public confidence in the ability of a government to protect and govern the people.

- **Criminal Threat**—Criminal activity may help predict future actions or provide advanced indications and warnings of attack. For example, theft of vehicles, military identification cards, passports, or installation entry passes are potential indicators of pending hostile action. Synthesized analysis of law enforcement and counterintelligence information is necessary to identify indicators of future attacks. Aggressive and continuous liaison efforts are needed for timely information sharing and willing cooperation from host forces.

- **Insider Threat**—This 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 an area of responsibility. Any of these groups of people may threaten Air Force interests by disclosing sensitive or classified information, by making decisions that favor dissident groups, or by irregular attack. They may target individuals, groups, facilities, weapon systems, or information systems. Host country forces may not provide the degree of FP anticipated or agreed to under treaty or coalition arrangements.

- **Psychological Threat**—Enemy threats target the psychological and physical well-being of Air Force personnel. The threat of CBRN attacks can hinder effective military operations as much as an actual attack. The enemy may also use deception (such as releasing harmless powder) to undermine the mission. Enemy propaganda and potentially biased media sources may also undermine coalition and public

support, create civil unrest, and dangerously weaken military morale. Commanders should recognize the importance of effective communication to minimize FP risks.

- **CBRN Threats**—The CBRN threats are chemical, biological, radiological, and nuclear weapons or hazards that pose or could pose a threat to individuals. These threats may result from the deliberate employment of weapons of mass destruction by enemy forces.

- **Civil Unrest Threat**—This threat reflects country-specific concerns of violence by the population related to friendly force operations. The threat can manifest itself during protests, demonstrations, refugee and humanitarian operations, or any other local tensions that may escalate into a direct threat to US forces.

- **Information/Data Threat**—This threat results from attempts to adversely affect Air Force information systems, information-based processes, and computer-based networks. The enemy and its unconventional supporters may attempt to impact military command and control; disrupt support activities such as local, military, and civil financial institutions; and interfere with supervisory control and data acquisition systems used to control critical infrastructures.

Threat Levels

Threat Levels	Examples
Level I	**Agents, saboteurs, sympathizers, terrorists, civil disturbances**
Level II	**Small tactical units, unconventional warfare forces, guerrillas, may include significant stand-off weapon threats**
Level III	**Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air and space operations**

Threat Levels

Enemy threats to Air Force assets take many forms and include any combination of types of threat. There are three levels of threat, depicted in the figure, "Threat Levels," and defined in JP 3-10, *Joint Security Operations in Theater*, which require security responses to counter them. These threat levels aid in performing risk assessments as well as conducting force protection planning. Each level or any combination of levels may exist in an operational area either independently or simultaneously. Emphasis on specific base or lines of communication security measures may depend on the anticipated level of threat supported by intelligence. This

does not imply that threat activities will occur in a specific sequence or that there is a necessary interrelationship among the levels.

Level I Threats. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion. Enemy activity and individual attacks may include random or directed killing of military and civilian personnel, kidnapping, and guiding special-purpose individuals or teams to targets.

Level I threat tactics may also include hijacking air, land, maritime and space vehicles for use in direct attacks; the use of improvised explosive devices (IEDs); vehicle borne IEDs (VBIEDs); or individual grenade and rocket-propelled grenade attacks. Civilians sympathetic to the enemy may become significant threats to US and multinational operations. They may be the most difficult to counter because they are normally not part of an established enemy agent network and their actions may be random and unpredictable. Countering criminal activities and civil disturbance requires doctrine and guidelines that differ from those used to counter conventional forces, and normally requires detailed coordination with external agencies. More significantly, based on political, cultural, or other perspectives, activities that disrupt friendly operations may be perceived as legitimate by a large number of the local populace. Countering Level I threats is a part of the day-to-day FP measures implemented by all commanders. Key to countering these threats is the active support of some portion of the civilian population, normally those sympathetic to US or multinational goals.

Level II Threats. Level II threats include small scale forces conducting irregular warfare that can pose serious threats to military forces and civilians. These attacks can cause significant disruptions to military operations as well as to the orderly conduct of local governments and services. These forces are capable of conducting well-coordinated, but small-scale, hit and run attacks, IED and VBIED attacks, and ambushes, and may include significant standoff weapons threats such as mortars, rockets, rocket-propelled grenades, and surface-to-air missiles.

Level II threats may include special operations forces highly trained in irregular warfare. These activities may also include operations typically associated with attacks outlined in the Level I threat including air, land, maritime and space vehicle hijacking. These forces establish and activate espionage networks, collect intelligence, carry out specific sabotage missions, develop target lists, and conduct damage assessments of targets struck. They are capable of conducting raids and ambushes.

Level III 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. Specific examples include airborne, heliborne, and amphibious operations; large combined arms ground force operations; and 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,[18] 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.

US Air Force Airmen successfully conducted base perimeter force protection operations 17 July 2014 to defend their operating locations when insurgents attacked an Afghanistan Air Force (AAF) air base using rocket-propelled grenades, machine guns, small arms fire, and VBIEDs. US Air Force Security Forces from the 438th Air Expeditionary Advisory Wing (AEW) took immediate action, establishing defenses and returning fire to defend the 438 AEW compound. Nearby, a USAF Special Operations Forces (SOF) Combat Aviation Advisor (CAA) team from the 6th Special Operations Squadron, assigned to a joint US SOF Advisory Group embedded with the AAF, was also taking fire. CAAs manned firing positions using their personal firearms and operating M-240 machine guns to lay down counter fire against the attackers. During the attack, the CAA Airmen also set up an initial medical aid station. The Airmen's "airmindedness" played a role in the defense, as the CAAs, working with their AAF counterparts, coordinated a combined AAF and US Air Force airpower show of force over the base. The Airmen's role in defending the base highlights the effectiveness of their FP preparation and training. The base sustained only minor damage with no friendly forces' loss of life.

[18] For information on base cluster defense operations, see Joint Publication 3-10, *Joint Security Operations in Theater*.

DOD TERRORISM THREAT LEVELS

Last Updated: 19 November 2019

The Department of Defense (DOD) uses a standardized set of terms to describe the terrorism threat level in each country: low, moderate, significant, and high. The Defense Intelligence Agency (DIA) sets the terrorism threat level for each country based on analysis of all available information. The levels are defined by the DIA as follows:

TERRORISM THREAT LEVELS

LOW: No terrorist group is detected or the group activity is non-threatening.

MODERATE: Terrorists are present, but there are no indications of anti-US activity. The operating environment favors the host nation and the US.

SIGNIFICANT: Anti-US terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as its preferred method, but has limited operational activity. The operating environment is neutral.

HIGH: Anti-US terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DOD presence and the operating environment favors the terrorist.

Commanders at all levels should use the DIA terrorism threat level plus their own localized force protection intelligence threat analyses as a basis for developing plans and programs to protect Service members, civilian employees, family members, facilities, and equipment within their operational areas. Force protection conditions (FPCONs)[19] are specific security measures promulgated by the commander after considering a variety of factors including the threat level, current events that might increase the risk, observed suspicious activities, etc.

[19] See DOD Instruction 2000.16, Volume 2, *DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System* (controlled access) for a more detailed discussion and listings of FPCONs and their measures.

FORCE PROTECTION CONDITIONS

There is 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. The FPCONs are:

- **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.

THREAT OBJECTIVES

Last Updated: 19 November 2019

For Airmen to fully understand threats and hazards, it is important to discuss possible intended threat objectives.

THREAT OBJECTIVES

Threat incidents over the years have been increasing in numbers and sophistication. Terrorism makes up the most prominent type of threat. Terrorism methods include threats, bombing, kidnapping, hostage taking, hijacking, assassination, sabotage, arson, armed raids or attacks, and other measures to disrupt daily activities. Such actions occur almost routinely in some parts of the world, and anyone can be a potential victim. In 2016, a small terrorist cell consisting of gunmen and suicide bombers attacked a concert hall, a major stadium, restaurants, and bars almost simultaneously in Paris, France, leaving 130 people dead and several hundred injured. In June 2016, suicide bombers killed over 40 and injured more than 200 people in an attack at an Istanbul airport. The 2016 Orlando nightclub shooting by a self-radicalized lone gunman who killed 49 people and left another 53 people injured shows that these attacks can occur within the US as well. DOD installations and personnel remain targets for terrorist organizations, as demonstrated by attacks against the Washington Navy Yard in 2013 and the Navy Reserve station and recruiting offices in Chattanooga, Tennessee, in 2015.

The persistence of threats reflects the number and intensity of conflicts around the world and the inherent difficulties of facing, assessing, and overcoming the threat objectives. There are multiple methods of attack with threat objectives designed to cause one or more of the following harmful results:

- ✪ Injure or kill personnel to create a tactical, operational, or strategic event.
- ✪ Destroy warfighting or war-supporting capabilities.
- ✪ Deny use of warfighting or war-supporting capabilities through damage or contamination.
- ✪ Deny or disrupt military operations through the threat of attack.

- ✪ Influence public opinion or governmental policies to comply with competing ideologies.
- ✪ Force nations deployed on foreign soil to end operations and depart the deployed location.
- ✪ Thrust a nation into civil unrest resulting in civil war.
- ✪ Force a government agency or corporation to alter its policies.
- ✪ Reduce military advantage through theft, destruction, or fraud involving military information or technology.
- ✪ Increase criminal activity such as kidnapping, robbery, and extortion, likely to be used to finance enemy operations.
- ✪ Isolate and exploit real or perceived weaknesses to demonstrate a group's capability and reduce US credibility.
- ✪ Bring favorable attention to a terrorist organization and serve as a recruiting tool.

All Airmen involved in force protection (FP) benefit from a thorough understanding of these types of threat objectives. This understanding enhances planning to counter FP threats, thereby improving the FP status of organizations and personnel.

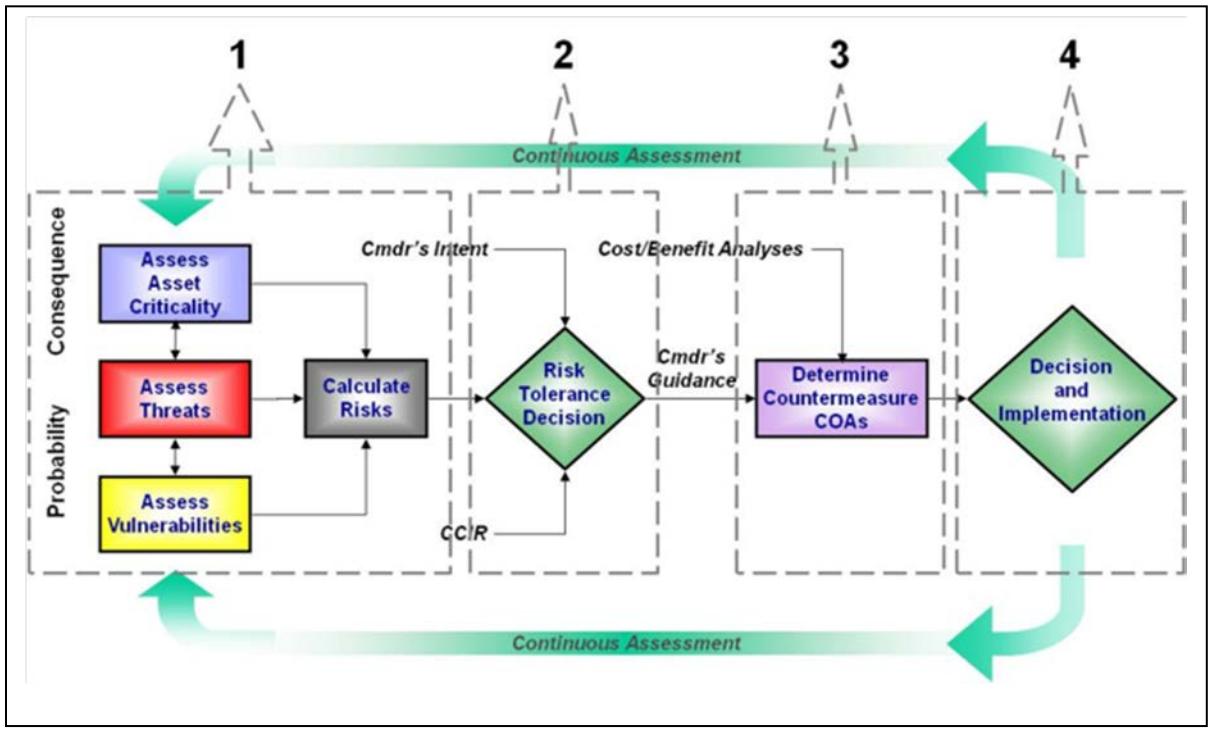
RISK MANAGEMENT PROCESS

Last Updated: 19 November 2019

Commanders, with input from appropriate staff, determine how best to manage risks. The Air Force defines risk management (RM) as **the process of identifying critical assets; understanding the threat; understanding Air Force vulnerabilities to the threat; determining risk to personnel, assets, and information; and assuming risk or applying countermeasures to correct or mitigate the risk.**[20] In all cases, as part of the installation all-hazards emergency management program, the assessments include hazards as well as threats. This RM process consists of the following elements: prioritizing assets and resources through a **criticality assessment**, identifying potential threats with a **threat assessment**, analyzing resource and asset vulnerabilities through a **vulnerability assessment**, determining the risks acceptable to them for a given operation by conducting a **risk assessment**, then supervising and reviewing the effort to eliminate or mitigate the risks that are not acceptable. A safety and RM focus ensures maximum protection of people and physical resources. This kind of risk-based focus may be critical to warfighting success. Operations security should be considered during the risk management process as well.

Safety, as applied via RM, is a major element of force protection (FP) planning and should be used in the risk assessment phase of the RM process when planning to counter a threat. The risk management process established in Air Force safety channels ideally lends itself to planning for FP efforts.[21] Safety has a strong impact on FP's overall effectiveness.[22] The figure, "The Risk Management Process," is an illustration of the RM process for FP focusing on threats.

[20] See Air Force Instruction (AFI) 31-101, *Integrated Defense*. This Air Force definition accords with and supports the joint definition of risk management: "The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits." (Joint Publication 3-0, *Joint Operations*)
[21] See AFI 90-802, *Risk Management,* and Air Force Policy Directive (AFPD) 10-24, *Air Force Critical Infrastructure Program (CIP)*.
[22] See the 91-series of Air Force instructions for information on Air Force safety programs.



The Risk Management Process
(Derived from AFI 31-101, *Integrated Defense*)

CRITICALITY ASSESSMENT

A commander should understand and identify those assets critical to mission execution. A criticality assessment is a systematic effort to identify key assets and infrastructure and evaluate the effect of temporary or permanent loss of the same on an installation's or a unit's ability to perform its mission. This assessment should examine costs of recovery and reconstitution including time, funds, capability, and infrastructure support. Assessments of non-mission essential assets should also be considered, such as high-population facilities; mass gathering activities; and other facilities, equipment, services, or resources deemed important by the commander to ensure continued effective operation. This assessment also assists the commander in identifying assets that are priorities for FP resource allocation.

The criticality assessment identifies the relative criticality of assets based on mission criticality, impact on national defense, replaceability, and monetary value. An asset is anything of value, including people, information, equipment, facilities, and infrastructure. Assets can also extend to more general or intangible items such as operations, systems, strategic advantage, morale, and reputation. The primary objectives in the effective asset criticality assessment are to identify key assets, determine if critical functions can be duplicated, identify the resources required for duplication, and determine the priority of response.

Assessing criticality requires judgment and analysis. For example, the enemy's destruction of an asset not considered essential to mission success or necessary for continued efficient operations may still be critical, if the enemy perceives it to be symbolic. Such an asset may warrant protection because its loss may give an enemy the media coverage they seek or cause personnel to doubt a commander's ability to keep them safe. Complete protection of every asset is not possible, but the more difficult it is for the enemy to attack an asset, the less likely they are to attack. The critical asset risk management program enhances the risk management decision-making capability at all levels to ensure that Air Force critical assets are available when required to support mission requirements in an all-threats and hazards environment. This risk management approach supports the prioritization of scarce resources across the Air Force, focusing priorities on the greatest risk based on assessed criticality, threat, vulnerability, and risk.

THREAT ASSESSMENT

A commander should know what threat is anticipated in order to devise an effective means to counter or mitigate it. Without this knowledge, the commander is acting blindly. A thorough threat assessment reviews the factors of a threat's existence, capability, intention, history, and targeting, as well as the operating environment within which friendly forces operate. Analyzing and synthesizing this information are essential precursor steps in identifying the probability of attack. Air Force Office of Special Investigations (AFOSI) and other Service counterparts produce a local threat assessment that should be used as a baseline product for adversary threats in the FP effort. At the installation level, the threat working group or other intelligence fusion and analysis cell (e.g., a joint intelligence support element) should assist in producing a localized threat assessment and recommend courses of action to the commander to mitigate or counter threats.

In the complex environment of irregular warfare (IW), intelligence, surveillance, and reconnaissance (ISR) forces should use information collected from a variety of sources to provide or collect information to fill intelligence gaps. ISR personnel should validate the credibility of these various sources to overcome adversary denial, deception, and information operations. Though rules of engagement and operational objectives drive operations, analysts should craft their intelligence requirements to help protect the population against both lethal and nonlethal capabilities. Analysts should recognize an increased need to make correlations between various development projects and levels of cooperation with the local nationals. Additionally, ISR forces should be aware that one of the basic underpinnings of successful IW operations is the capability to train partners to conduct independent operations and participate in coalition operations.

Threat assessments fuse information and intelligence from open source, law enforcement, government intelligence, medical intelligence, and counterintelligence information, along with local, state, and federal information to create a cohesive threat picture for FP decision-makers. By synthesizing law enforcement, intelligence, medical intelligence, and counterintelligence information, analysts can identify indicators of

future attacks. The more common sources are described in the figure, “Sources of Intelligence and Counterintelligence.”

OPEN SOURCE INFORMATION: —News media, hearings, publications, reference services, publicly available internet sites/data
LAW ENFORCEMENT INFORMATION: —Collection, retention, and dissemination regulated by law enforcement channels —Law enforcement information
GOVERNMENT INTELLIGENCE AND COUNTERINTELLIGENCE INFORMATION: —Products and reporting from the US intelligence community
LOCAL, STATE, AND FEDERAL INFORMATION (including host nation)**:** —Service member, civil servant, individuals with regional knowledge —Counterintelligence force protection operations—information gleaned from the streets

Sources of Intelligence and Counterintelligence.

Considering the wide range of possible threats, FP personnel should focus on developing a robust force protection intelligence (FPI) threat picture to support unit deployments, readiness training, mission planning, and other mission execution functions such as integrated defense, the critical infrastructure program, and emergency management.[23] Commanders should develop priority intelligence requirements to guide FPI work supporting their decision-making and operations. FP personnel should coordinate with their cross-functional counterparts to ensure information requirements are satisfied. Once FP information has been fused, the end product should be provided to the commander to guide intelligence-driven and risk-based measures or operations, such as counterintelligence support to FP, to preempt, deter, mitigate, or negate threats. FPI provides support to all phases of FP operations.

The AFOSI’s local threat assessment is a good starting point for general information on the security threats facing an installation. However, when more specific local threat information is required, it can be obtained from multiple sources through AFOSI’s liaison with federal, state, local, and foreign national law enforcement, counterintelligence, and security agencies.[24]

[23] See AFI 31-101; AFPD 10-24; and AFI 10-2501, *Air Force Emergency Management Program,* for more information on these functions.
[24] AFPD 71-1, *Criminal Investigations and Counterintelligence*.

VULNERABILITY ASSESSMENT

Once the threat assessment is complete, commanders should prepare a vulnerability assessment of their personnel, equipment, facilities, installations, and operating areas. This assessment should address the broad range of medical and physical threats to the security of the commander's personnel and assets. The vulnerability assessment then considers the identified and projected threats against personnel, facilities, or other assets to identify those areas where resources are susceptible to actions which may reduce or diminish operational effectiveness. This includes the local populace and infrastructure due to association or proximity with Air Force operations.

Airmen should consider both the threat and existing vulnerabilities, but should not rely exclusively on the assessed threat. For example, terrorists successfully attacked military targets, such as Khobar Towers, the USS Cole, and three residential compounds in Riyadh, Saudi Arabia, even though those locations were in force protection condition Bravo. Non-military targets, such as the US embassies in Tanzania and Kenya or the World Trade Center, have been attacked when the country terrorist threat assessments for those locations were moderate, low, or negligible. History shows that the assessed threat is not necessarily an accurate reflection of the actual threat. As a result, identifying vulnerabilities is critical. Once identified, steps to mitigate the vulnerabilities should be undertaken to increase survivability for Air Force personnel and assets.

RISK ASSESSMENT

The risk assessment compares the relative impact of any loss or damage to an asset (criticality) with the relative probability of an unwanted event. When combined in a quantified fashion, these elements analyze and measure the risks associated with an unwanted event. Upon completion of the criticality, threat, and vulnerability assessments, commanders should have the information they need to make decisions regarding what level of risk they are willing to accept. However, risks to the most critical Air Force assets should be mitigated or eliminated whenever possible. If risks cannot be eliminated, commanders should implement measures to mitigate them to the greatest extent possible.

FORCE PROTECTION PLANNING

Last Updated: 19 November 2019

The essential goal of force protection (FP) is to counter threats against Air Force operations and assets. It is intended to conserve the force's fighting potential so it can be applied at the decisive time and place and incorporates the integrated and synchronized offensive and defensive measures to enable the effective employment of the force while degrading opportunities for the adversary.[25] Air Force personnel should identify threats, then determine ways to counter them to protect personnel and resources in order to enable mission accomplishment. The FP tools below are available for commanders to consider when preparing to counter threats. This begins with the risk management process and proceeds to FP countermeasure planning considerations.

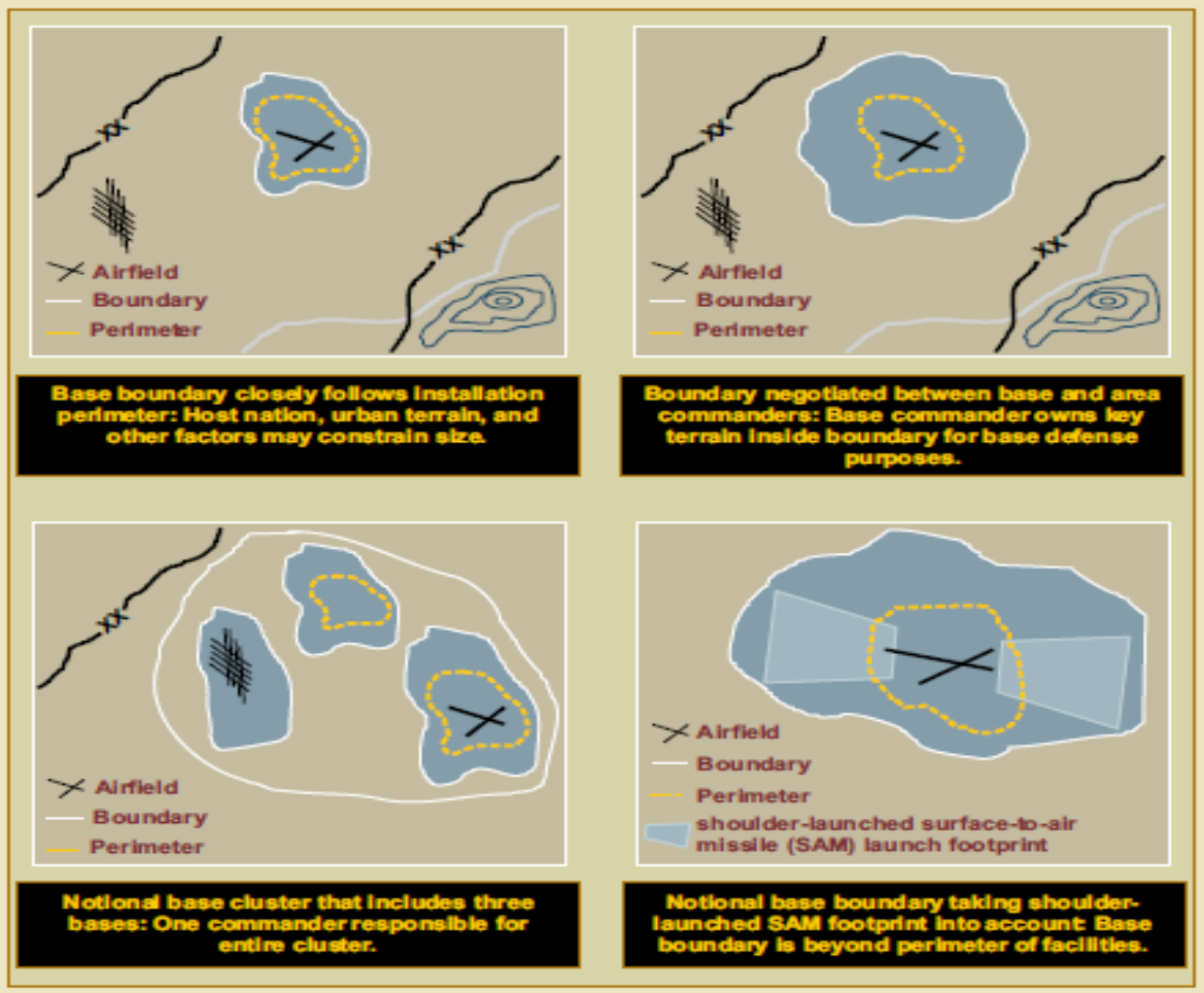
Because threats to operations can come from a wide range of sources, the Airman's Perspective requires Airmen to plan for FP in broad terms. For example, the threats to an active airfield may extend far beyond the surface area designated as a base boundary. To address these threats, the Air Force uses the planning construct of the base security zone (BSZ) to ensure those ground threats that could impact operations are considered and planned for.

BASE SECURITY ZONE

The multi-dimensional space around the base from which the enemy might impact air operations by launching an attack against approaching or departing aircraft or personnel and resources located on the base is critical to air base defense planning. To secure airpower assets and protect personnel and resources in this area, the Air Force uses a unique planning construct, referred to as the BSZ.[26] Focused intelligence preparation of the battlespace (IPB) efforts and integrated defense operations should operate in unison to support BSZ establishment. Security planners should first establish this planning construct through IPB and commander's estimate, and then seek to align it with the negotiated base boundary—the area allocated to the base commander for protection. Should the derived area extend beyond the base boundary into the BSZ, and alignment with the base boundary is not possible, then Air Force security planners

[25] Information derived from Joint Publication (JP) 3-0, *Joint Operations*.
[26] See AFPD 31-1, *Integrated Defense*, and AFI 31-101, *Integrated Defense*, for information that establishes the BSZ as an Air Force construct.

should coordinate with battlespace owners to ensure the protection of airpower resources.



Base Boundary Considerations

(Information from JP 3-10, *Joint Security Operations in Theater)*

BASE BOUNDARY

JP 3-10, *Joint Security Operations in Theater*, identifies the base boundary as, “a line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas.” The base boundary, which is not necessarily the base perimeter, is negotiated on a case-by-case basis between the base commander and the area commander or host-nation authority. The base boundary should be established based upon the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations, specifically balancing the need of the base defense forces to control key terrain with their ability to accomplish the mission. Whenever an Air Force commander

is designated the base commander of a joint use base, he or she should use the base boundary construct in establishing base defense plans as it most readily translates to effective plans for the other Services present on the base. If the base boundary does not include all of the terrain of concern to the senior Air Force commander (if not the base commander), as identified by the BSZ, he or she should advise the base commander of the responsibility to either mitigate (through coordination with the area commander or the host nation) or accept the risks of enemy attack from the area outside the base boundary. The figure, “Base Boundary Considerations,” illustrates these considerations.

FORCE PROTECTION INTELLIGENCE

Last Updated: 19 November 2019

Airmen are subject to threats whether in the continental US (CONUS) or outside the CONUS (OCONUS). These threats are continually evolving and will increasingly challenge US personnel, facilities, and assets. Understanding how these threat elements function is the first step to developing an effective force protection (FP) program that will help commanders assess their ability to respond to an attack.

As such, tailored force protection intelligence (FPI) is fundamental to the prosecution of an effective FP program. It is a mission set used to identify intelligence support to FP. All-source intelligence should be provided on threats to Department of Defense (DOD) missions, people, or resources stemming from terrorists, criminal entities, foreign intelligence entities, and opposing military forces as appropriate under Presidential Executive Order 12333, *United States Intelligence Activities*; the US Constitution; applicable law; and DOD and Service policies and regulations.[27]

Intelligence is a major enabler that supports FP decisions and operations. It is a collaborative effort between intelligence, counterintelligence, Security Forces, the medical health community, emergency management, weather, and communications. However, the roles of each differ depending on location (CONUS or OCONUS) due to executive orders and other policies. The end result of this vital function is a more accurate picture for commanders at all organizational levels, enhancing the protection of personnel, resources, and information.

[27] FPI deals specifically with intelligence efforts to counter enemy threats. Those intelligence efforts that address hazards are referred to as incident awareness and assessment. For additional information on incident awareness and assessment, see AFDP 2-0, *Global Integrated Intelligence, Surveillance, and Reconnaissance*, and Air Force Instruction 71-101V4, *Counterintelligence*. For additional information on intelligence oversight, see DOD Directive 5240.01, *DoD Intelligence Activities.*

COUNTERINTELLIGENCE SUPPORT TO FORCE PROTECTION

Last Updated: 19 November 2019

Counterintelligence support to force protection (CISFP) is the employment of Air Force Office of Special Investigations capabilities to find, fix, track, and neutralize enemy threats in order to create a sustained permissive environment for air, space, and cyberspace operations.[28] CISFP is essential in detecting, assessing, denying, and responding to threats affecting Air Force operations. CISFP are intelligence, surveillance, and reconnaissance (ISR)-driven operations using information derived from multiple intelligence and counterintelligence sources providing tactical situational awareness to forewarn or preempt adversarial attack. CISFP activities include counterintelligence collection, analysis, and investigation; surveillance; and countersurveillance. These activities provide excellent sources of intelligence that assist force protection operations. The base defense forces should use ISR to identify and monitor threats, enabling their elimination. The ability to acquire and analyze suspicious activity reports for indications and warning of possible terrorist pre-attack activities is a critical component of counterintelligence support to the force protection mission. Terrorists have the advantage of choosing the time and venue for their attacks, but normally have to conduct extensive pre-attack preparations to maximize their chances of success. The pre-attack phase of a terrorist operation, however, is the period of greatest vulnerability to the terrorist group, since it must surface to collect intelligence and conduct physical surveillance and other activities of the target. Therefore, an effective system, such as CISFP, for detecting terrorist pre-attack activities is a high priority task for the intelligence community, law enforcement, security elements, and local community authorities.

[28] See Air Force Tactics, Techniques, and Procedures 3-10.3, *Integrated Defense Counterthreat Operations*, for more information on CISFP.

THE FORCE PROTECTION COMMUNITY

Last Updated: 19 November 2019

Force protection (FP) is achieved through the successful execution of three related but distinct lines of effort: integrated defense, emergency management (EM), and the critical infrastructure program. These lines of effort are supported by programs and activities contributing to FP through integration of multifunctional capabilities and activities. The purpose is to integrate these capabilities to achieve the desired FP effects of detect, deter, preempt, negate, and mitigate. Integration of all the programs and activities is the means to achieve successful FP.

INTEGRATED DEFENSE

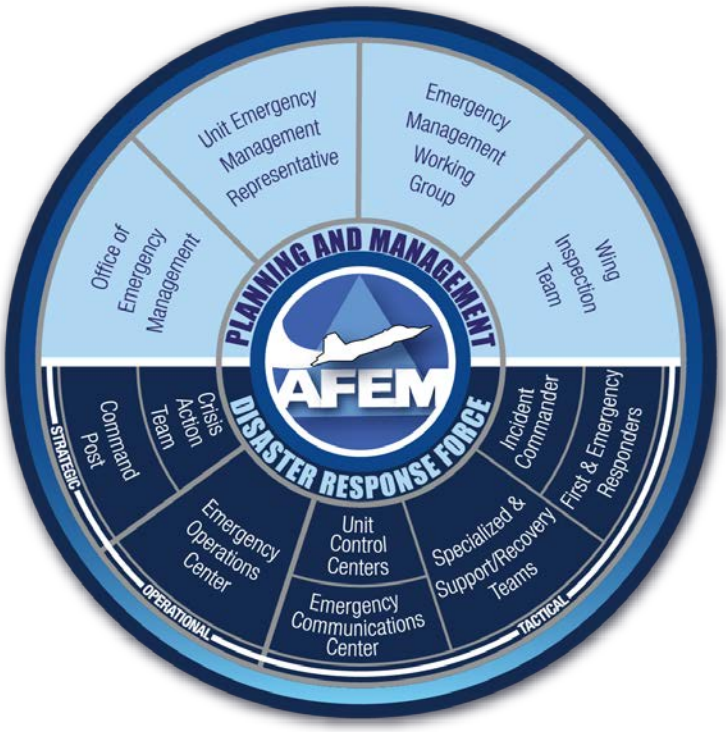
Effective integrated defense helps ensure effective FP. While integrated defense is an Air Force-wide responsibility, Air Force Security Forces are the Service enterprise lead for integrated defense operations, synchronizing Air Force policy pertaining to protection and defense against all threats and hazards to Air Force installations. The defense force commander (DFC) employs Air Force Security Forces and other multidisciplinary resources and personnel to execute this operation. The DFC integrates operations with emergency management activities. Integrated defense operations protect and defend Air Force personnel, installations, activities, infrastructure, resources, and information. Integrated defense requires timely force protection intelligence (FPI). Commanders should use FPI to support decision-making for operations. Integrated defense relies on the ability of all Airmen to contribute to the defense of their installation while still fulfilling their primary functions.

Integrated defense is conducted worldwide, from mature theaters to austere regions. Air Force leadership should adapt to a variety of operational requirements. Some Air Force resources may be geographically separated from the main base. For example, communications facilities are often isolated and sited on high ground to maximize their effectiveness. Regardless of location, forces conducting integrated defense employ the basic tactics, techniques, and procedures as those employed at home station during day-to-day operations. As specific threats to base personnel and resources increase, integrated defense forces adjust tactics to counter the threat. Adjustments to operating procedures should be based on the specific threat to operations, the dynamics of operating in an international environment or the way integrated defense efforts collaborate with joint, combined, civilian, and host nation forces. Integrated defense

forces should be prepared to operate at a variety of locations and may deploy to sites without existing Air Force or host nation facilities.

EMERGENCY MANAGEMENT

The protection of Air Force personnel and resources on Air Force installations is essential to ensure successful Air Force operations. The Air Force emergency management (EM) program addresses activities across the all-hazards physical threat environment at home station or expeditionary locations to support overall FP. The figure, “Air Force Emergency Management Construct,” illustrates the Air Force‘s emergency management construct.



Air Force Emergency Management Program Construct

The primary mission of the Air Force EM Program is to save lives; minimize the loss or degradation of resources; and continue, sustain, and restore operational capability in an all-hazards physical threat environment at Air Force installations worldwide. The ancillary missions are to support homeland defense and defense support of civil authorities operations and to provide support to civil and host nation authorities according to DOD directives and through the appropriate combatant command. The Air Force EM program contributes to mission assurance and the continuation of mission essential functions necessary to perform the operations of the installation in support of the *National Defense Strategy*.

These physical threats may occur at any time, with or without prior warning. Emergency management supports protection of personnel and resources through integration of installation preparedness, response, and recovery programs aimed toward reducing the impact of these events on the installation; prepares for risks that cannot be eliminated; and prescribes actions required to deal with consequences of actual events and to recover from those events using the Air Force incident management system. Emergency management planning and response is based on National Incident Management System methodology to align with the National Response Framework as directed by Homeland Security Presidential Directive 5. See Air Force Policy Directive 10-25, *Air Force Emergency Management Program,* and Department of Defense (DOD) Instruction 6055.17, *DOD Emergency Management (EM) Program*, for more information on the installation emergency management program.

CRITICAL ASSET RISK MANAGEMENT PROGRAM

Operations in support of the *National Defense Strategy* are dependent on globally linked physical and cyber infrastructures (US and foreign, public and private sector). These interconnected infrastructures, while improving capabilities and mission effectiveness, also increase vulnerability to potential failures due to human error, natural disasters, or intentional attack. Consequently, it is important to identify and protect those infrastructures critical to mission accomplishment.

FORCE PROTECTION EFFECTS

Threats to Air Force interests occur across the competition continuum from peacetime through wartime. Commanders should recognize that any given threat may be present at any time. Commanders should also consider the effects intended to be produced by the threat, not just the nature of the threat itself. In this manner, a threat can be small in execution with large-scale effects as the outcome; threats can undermine mission capability as severely as sabotage or engagement with enemy forces. FP efforts conserve the Air Force's fighting potential by safeguarding its forces and mission capability through the achievement of predetermined effects. In all circumstances, commanders should tailor resources and capabilities to achieve, at minimum, the following FP effects:

- **Deter**—Measures should be developed to discourage adversarial actions. Vital to the effectiveness of these measures is the existence of a credible threat of unacceptable counteraction. Potential adversaries should perceive the Air Force has the capability to conduct and sustain offensive and defensive operations. This is best achieved through the possession of forces properly trained, organized, and equipped to execute base security against unconventional, Level I and II threats, and, if required, engage Level III threats and conduct a combat handover to a tactical combat force.

- **Detect**—Measures should be developed to identify the presence of an object or an event of possible military interest, whether a threat or hazard. Detection may arise

through observation of the operational area or through deductions made following an analysis of the operational area.

- **Preempt**—Once conclusive evidence indicating an imminent enemy attack is determined, actions should be initiated to rapidly respond and establish or gain a position of advantage to eliminate the threat. Essential to effective preemptive operations is an accurate estimate of the adversary's capabilities and vulnerabilities. Every intelligence and counterintelligence resource available should be used to determine enemy capabilities, intentions, and probable courses of action.

- **Negate**—Measures should be taken to render a threat or hazard incapable of interfering with Air Force operations. This includes the effective employment of coordinated and synchronized offensive and defensive measures and measures to counteract hazards.

- **Mitigate**—If actions to negate are unsuccessful, measures should be taken to minimize enemy success and lessen the consequence or severity of the adversary's actions. Likewise, measures should be taken to reduce the consequences of any hazard affecting operations.
