AIR FORCE DOCTRINE PUBLICATION 3-10

FORCE PROTECTION

U.S. AIR FORCE

1 June 2023

Air Force Doctrine Publication 3-10, *Force Protection*

Table of Contents

"The Air Force organizes, trains, and equips forces to be an air component to a joint force commander (JFC). As part of the joint force's air component, our forces must be prepared to accomplish JFC objectives**.** The air component commander's administrative authorities are derived from Title 10, U.S. Code, and exercised as the Commander, Air Force Forces (COMAFFOR). The air component commander's operational authorities are delegated from the JFC and exercised as both the COMAFFOR, over Air Force Forces, and as the functional joint force air component commander (JFACC), over joint air forces made available for tasking. Thus, the air component commander leads Air Force Forces as the COMAFFOR and the JFC's joint air operations as the JFACC. This duality of authorities is expressed in the axiom: Airmen work for Airmen and the senior Airman works for the JFC."

-- Air Force Doctrine Publication (AFDP) 1, *The Air Force*

Since the COMAFFOR and JFACC are nearly always the same individual, this AFDP will use the term "air component commander" when referring to duties or functions that could be carried out by either or both, unless explicit use of the term "COMAFFOR" or "JFACC" is necessary for clarity.

CHAPTER 1: INTRODUCTION TO FORCE PROTECTION

The joint function of protection[1] is defined as all efforts to secure and defend the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area to maintain mission effectiveness. Force protection (FP)[2] is where protection places its focus.[3] FP is preventive measures taken to prevent or mitigate enemy and insider threat actions against Department of Defense (DOD) personnel (to include family members and certain contractor personnel), resources, facilities, and critical information. It is a fundamental principle of all military operations as a means to ensure the survivability of a commander's forces.

Due to the increased lethality of threats, including those from peer and near-peer competitors, it is imperative the United States Air Force (USAF) take strong measures to protect DOD personnel, resources, and installations around the world as part of a coordinated and integrated joint force. Doing so is critical to the Service's ability to perform its mission and conduct operations. An air expeditionary task force, poised to respond to global taskings, should be able to fully protect its forces. FP supports combat support and its supporting capability of "Protect the Force" and is an essential and primary responsibility of command. As such, commanders at all levels should establish an effective FP program.

THE AIRMAN'S PERSPECTIVE ON FORCE PROTECTION

FP is an essential responsibility of all personnel. All Airmen should understand the fundamental aspects of FP to safeguard their own lives, those of fellow Airmen and joint Service members, and valuable DOD resources. The key to the USAF's view of FP is the protection of its people, the Service's prime asset. Though this responsibility can stress available personnel and resources, commanders should balance mission accomplishment with FP and enlist all available forces to defend an air base. Typically, most FP responsibilities are carried out by installation security forces. However, in many instances, those forces may not be sufficient to cover the full range of force protection actions needed in a particular operational environment.

To support a commander's full range of force protection requirements, all military Airmen should be trained and equipped to defend the base against threats. Identified commanders should lead them in that effort. Training includes basic ground combat skills training (e.g., weapons familiarization, tactical combat casualty 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. Likewise, to counter the increasing threat of small unmanned aircraft systems, Airmen should understand the nature of these threats and the means to observe, report, and execute actions against them.

---

[1] See JP 3-0, *Joint Campaigns and Operations*.
[2] See JP 3-0.
[3] Protection also encompasses force health protection, which is addressed in Air Force Doctrine Publication (AFDP) 4-02, *Health Services*.

All Airmen contribute to FP. Security forces, augmentees, and resource owners or users (e.g., personnel working in maintenance and operations on and around a flightline) provide FP. Operations personnel may conduct missions to defend an installation or defeat immediate threats to it. Personnel involved in information fusion operations provide a threat picture by integrating all-source information through intelligence preparation of the operational environment to aid FP and support decision advantage. Civil engineers design physical security improvements; provide planning, training, and response capabilities to deal with FP-related infrastructure incidents; and provide explosive ordnance disposal capabilities. Fire department personnel conduct presumptive identification for the presence of CBRN hazards. Communications specialists integrate evacuation notification systems. These are only examples of the breadth of FP in the USAF.

FP is multi-dimensional and multi-layered. It covers actions at home station, in transit, and at deployed locations. It includes protection of military members and civilian employees, their families, contract employees, and visitors on an installation.[4] The functional expertise required to do so 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. Operations security (OPSEC) is also a key component of FP and is expected of all Airmen. Through this multi-layered approach, FP extends awareness and influence as far forward as possible, while simultaneously providing in-depth protection to DOD personnel and resources. This maximizes the ability to disrupt attacks and provide the earliest warning possible, while ensuring the best protection for Service forces through proper implementation of base defense. The end result is USAF forces able to conduct their missions with the best protection available, based on risk management (RM), wherever the mission is.

FP requires a global orientation. Threats occur across the competition continuum[5] and impact Airmen and Guardians ability, whether in garrison or deployed, to conduct operations. In a modern peer and near-peer environment, FP threats continue to evolve and challenge US personnel, facilities, and assets. Threats to the joint force are unpredictable and may be presented at any time. 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. Tactics may include conventional as well as asymmetrical methods.

FP practitioners use technology to enhance capabilities. Technology provides advantages in speed, range, and effectiveness to assist in meeting the demands of a changing operational environment. However, none of these technologies can perform FP alone. As technology evolves, so do the tactics of adversaries, necessitating changes in

[4] DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program*, establishes the responsibilities of geographic combatant commanders for force protection.
[5] See Joint Doctrine Note 1-19, *Competition Continuum*.

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.

Commanders should not only be concerned with the nature of these threats, but also with their intended effects. Even seemingly small or minor threats may have potential to inflict significant harm to personnel and resources and severely disrupt or impede operations. Understanding how threats function is the first step to developing an effective FP program. Effective intelligence, counterintelligence, and liaison efforts are critical to identifying, analyzing, and disseminating threat information. Airmen should be aware of assessed threats and FP factors in the operational environment at all times, whether in garrison or deployed.

FORCE PROTECTION MEANS

Because of how the USAF projects combat power, the Service views the joint function of protection with an airminded perspective. For the USAF, force protection provides an overarching structure that connects and incorporates various elements identified as tasks and activities included in the protection joint function. The tasks and activities Airmen employ to preserve the Service's fighting potential are:

- Protection against hostile air and ballistic missile threats through active and passive air and missile defense (AMD). AMD includes actions to counter small unmanned aircraft systems. Airmen work with US Army counterparts for air defense (AD) and ballistic missile defense (BMD) capabilities.[6]
- Protection of friendly information through cyberspace security, operations security, Department of Defense Information Network (DODIN) operations, defensive cyber operations, counterintelligence operations, and defensive use of electronic warfare.
- Base defense, physical security, antiterrorism programs, law enforcement, and insider threat protection to protect forces, bases, and infrastructure.
- Engineering/explosive ordnance disposal support and counter-improvised explosive device efforts.
- CBRN defense to minimize CBRN attacks and incidents.

Emergency management (EM) and response. EM and response, along with critical infrastructure protection programs are discussed in the appendix on additional FP lines of effort.

FORCE PROTECTION EFFECTS

FP efforts conserve fighting potential by safeguarding its forces and mission capability through the achievement of predetermined effects. Commanders should tailor resources and capabilities to achieve, at minimum, the following FP effects:

[6] See AFDP 3-01, *Counterair*.

- **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 USAF has the capability to conduct and sustain offensive and defensive operations. This is best achieved through the possession of forces properly organized, trained, and equipped to execute base security against unconventional, Levels I and II threats, and, if required, engage Level III threats and conduct a combat handover to a tactical combat force. Chapter 3 addresses threat levels.

- **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.

- **Delay**—Forces should use terrain, barriers, obstacles, and fires to delay adversaries, allowing time for the air base to take defensive measures and mass response forces at decisive points. Defense forces should intercept adversaries before they can reach positions to achieve their objective. The defensive nature of FP inherently surrenders the initiative to the adversary on the time and place of attack. FP forces play a critical role in delaying adversaries long enough to counterattack and regain the initiative.

- **Deny**—Denying means preventing adversary positioning to cause effects on forces. This may mean access to key terrain in the base security zone (BSZ) where direct or indirect fires can disrupt operations. It also means denying penetration attempts of installation perimeters and critical security areas and denying adversaries close proximity to resources to prevent sabotage, tampering, or intelligence collection on weapons systems. The effective application of barriers, obstacles, weapons systems, and technology aid in achieving denial.

- **Defeat**—Swiftly defeating an adversary is key to maintaining the initiative for a defending force. Any attack, regardless of effectiveness, can disrupt an air base's ability to generate airpower until ground defense forces regain the offensive. Ideally adversaries are defeated before they can cause significant damage or disruption to operational missions.

CHAPTER 2: COMMAND RESPONSIBILITIES FOR FORCE PROTECTION

FP is a task for every commander at every level. To ensure a comprehensive and integrated response, command responsibilities for FP should be clear. Integration of all aspects of FP should enable commanders to react quickly to threats. Commanders should understand the legal basis of their responsibilities and jurisdictions.

THE ROLE OF THE COMBATANT COMMANDER

Protection of assigned and attached forces is an inherent responsibility of all commanders. However, FP is not exclusively a Service responsibility. According to both the *Unified Command Plan* and JP 1, Volume 2, *The Joint Force,* **combatant commanders (CCDRs) with geographic responsibility have the overall requirement to establish and implement FP in their areas of responsibility (AORs).** CCDRs exercise authority for FP over all DOD personnel (including their dependents) assigned, attached, on temporary duty, transiting through, or training in the CCDR's AOR.

Department of State Chief of Mission. The exception to the statement above is for personnel for whom the Department of State (DOS) Chief of Mission (COM) retains security responsibility. Examples include air attachés and Marine Corps embassy security group personnel. CCDRs develop and maintain memoranda of agreement with COMs that delineate security responsibility for DOD personnel based on whether the COM or the CCDR 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 USAF personnel supporting military cargo aircraft at an international airport. Although the CCDR is ultimately responsible, the CCDR can work with the US Embassy to assume FP support duties to include intelligence sharing and threat warning.

Tactical Control for Force Protection. A CCDR's authority for FP over those forces in the CCDR's AOR that are not assigned or attached is exercised through tactical control (TACON). TACON for FP authorizes the CCDR 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 CCDR may also direct immediate FP 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 the CCDR's TACON for FP include regular and Reserve Component personnel (including National Guard personnel in a Title 10, U.S. Code, *Armed Forces,* status) in the AOR.[7]

Although CCDRs 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 applicable authorities, regulations, policies, and law.

[7] See DOD Instruction (DODI) 2000.12, *DOD Antiterrorism (AT) Program*.

TACON for FP: An Example

Airlift forces deployed to or transiting through a CCDR's AOR are subject to the TACON for FP standards established by the CCDR and the FP measures established by their Service chain of command. For example, Air Mobility Command (AMC) is the Air Force Service component to US Transportation Command, and has airlift assets forward deployed in the US Indo-Pacific Command AOR. Although the aircraft are staged in the Indo-Pacific region, the commander, AMC (AMC/CC), as the commander of Air Force forces, is responsible for securing these assets during mission execution. The AMC/CC 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. However, the protection of these aircraft and their personnel at their beddown location remains an installation commander responsibility.

FORCE PROTECTION IN US NORTHERN COMMAND

In most theaters, the senior DOD member serves as the CCDR 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 CCDR 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 support of USNORTHCOM's FP mission.

FORCE PROTECTION AND COMMAND RELATIONSHIPS IN A JOINT ENVIRONMENT

The CCDR or a subordinate joint task force commander can delineate the FP measures for all DOD personnel not under the responsibility of the DOS. If a joint force commander (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. When a USAF 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 AIR COMPONENT COMMANDER

Through the air expeditionary task force (AETF) structure, the air component commander presents the JFC a task-organized, integrated package with the proper balance of force sustainment and FP. Within this AETF structure, the air component commander and

commanders at appropriate subordinate echelons (such as wing, group, and squadron levels) are responsible 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 implement an effective FP program. These commanders have the added responsibility of accomplishing FP planning for the units identified to deploy to their location during contingency operations. Commanders face three major FP challenges: planning for FP integration and support as tasked in applicable operational plans, training for FP, and providing FP preventive measures for those personnel and resources within their purview. Commanders with FP responsibilities 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.

LEGAL CONSIDERATIONS DURING FORCE PROTECTION PLANNING AND EXECUTION

FP fundamentals are applied in many different operational environments and command structures. While planning, commanders should be aware 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 other policies (e.g., restrictions of movement, quarantine, rules of engagement, or rules for the use of force). Together, these laws and rules regulate the status and activities of forces. Below are some legal requirements a commander should consider, depending on where FP measures are being implemented.

TYPES OF JURISDICTION

Commanders should understand the degree of control they have over their installations and be familiar with the legal types of title and jurisdiction affecting them.[8] Depending on location, forces may be subject to various types of jurisdiction. For instances involving areas under US government control where the USAF does not exercise exclusive federal jurisdiction, commanders should work closely with the staff judge advocate and relevant authorities to establish protocols for handling civilians. For installations located in a foreign nation, jurisdiction may be governed by the terms of a status-of-forces agreement or other agreement with the host nation. In either case, commanders should coordinate FP requirements with local authorities and adjacent friendly forces. Likewise, in those areas where authority and jurisdiction constraints may prevent forces from patrolling or otherwise occupying areas outside the installation's recognized base boundary but within the base security zone, commanders should apply RM to minimize risk exposure to personnel and resources.

[8] Types of juFor 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; Title 40 U.S.C. §§3111 and 3112; and AFI 32-9001, *Acquisition of Real Property*.

LEGAL CONSIDERATIONS FOR HOMELAND OPERATIONS

In the US, commanders publish and enforce regulations to protect installation resources and personnel. To do so, force protection intelligence (FPI) is vital for providing an accurate picture for a commander to better anticipate and plan against threats. However, commanders should ensure units and organizations conducting intelligence activities do not infringe on or violate the rights of US persons. Commanders should implement an intelligence oversight program and associated safeguards to ensure FP operations do not violate intelligence oversight directives and that FP activities conform to US law, executive orders, and DOD directives.

When encountering FP issues in the US, commanders should consider the unique laws, challenges, and issues for homeland operations[9].

[9] See AFDP 3-27, Homeland Operations

CHAPTER 3: FORCE PROTECTION THREATS

Threats range from powerful state actors with the full range of conventional and CBRN weapons delivered by sophisticated means to non-state actors with inventive and asymmetric methods of harming forces. Such threats can inflict catastrophic damage with or without notice. Consequently, personnel, aircraft, spacecraft, equipment, installations, and operating locations—including the missions they perform or support—are vulnerable to a wide variety of threats. This daunting prospect demands FP awareness and education at all levels and effective FP measures implemented through a coherent and coordinated command structure.

SPECTRUM OF FORCE PROTECTION THREATS

Commanders are responsible for recognizing threats to a mission across the competition continuum. Threats may arise from terrorists or insurgents, insiders, criminal entities, foreign intelligence entities, opposing military forces, or violent extremist organizations. Though threats may be unique to a particular location, Airmen should maintain a wide perspective, mindful that not all threats will originate within their respective operational areas. Adversary tactics employed in one theater may manifest in other regions resulting in increased FP measures that may affect ongoing operations. Airmen should approach FP proactively and consider "what if" scenarios to anticipate potential threats and develop appropriate FP measures to counter them.

TYPES OF THREATS

In addition to 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.
- **Irregular Threat**—This threat encompasses a broad spectrum of military and paramilitary operations predominantly conducted by, with, or through 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 determine accurate indicators of future attacks. Aggressive and continuous liaison efforts are needed for timely information sharing and to encourage host nation cooperation.

- **Insider Threat**—This threat comes from civilian or military personnel, host-country nationals (military or civilian), third country nationals (contract employees) or other persons assigned to or transiting an operational area. Any of these groups of people may threaten USAF interests by disclosing sensitive or classified information, by actions that aid dissident groups, or by physical attack. They may target individuals, groups, facilities, weapons systems, or information systems.

- **Psychological Threat**—Enemy threats target the psychological and physical well-being of USAF personnel. The threat of attacks can hinder effective military operations as much as an actual attack. The enemy may also use deception to undermine operations. 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**—A CBRN attack or incident can occur via wartime action, terrorist attack, or as the result of a military or industrial accident. Different CBRN-related materials and agents are characterized by varying degrees of lethality, persistence, and destructive capability. Additionally, numerous other variables can affect a weapon's scope and the severity of its impact. CBRN agents may be combined and employed together or delivered via alternative methods. These variables may influence concentration levels, areas of contamination, and levels of physical destruction.

- **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 USAF information systems, information-based processes, and computer-based networks. The adversary and its supporters may attempt to impact military command and control; disrupt support activities (e.g., civil financial institutions), and interfere with systems used to control critical infrastructures.

THREAT LEVELS

Enemy threats take many forms and include any combination of types of threat. There are three levels of threat defined in JP 3-10, *Joint Security Operations in Theater*, that require security responses to counter them (shown in the figure below). These threat levels aid in performing risk assessments as well as conducting FP planning. Threats of any level, whether singular or a combination of threats at varying levels may exist in an operational area. They may also be related or independent of one another. Implementation of specific security measures may depend on the anticipated level of threat indicated by intelligence.

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

Level I Threats. Typical Level I threats include enemy agents and terrorists whose primary missions include espionage, sabotage, and subversion. Enemy activity may include random attacks, targeted attacks on specific personnel, kidnapping, and other aid or assistance to enable attacks on friendly, allied, or civil targets.

Countering Level I threats is a part of day-to-day FP measures implemented by all commanders. Level I threat tactics may also include hijacking air, land, maritime, and space vehicles for use in direct attacks or using improvised explosive devices (IEDs), vehicle-borne IEDs (VBIEDs), or individual grenades and rocket-propelled grenades in 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 force or network and their actions may be random and unpredictable. Operations to counter criminal activities and civil disturbance, including associated constraints and restraints, differ from those aimed at countering conventional forces, and normally require detailed coordination with external agencies. Further, activities that disrupt friendly operations may be viewed favorably or supported by many of the local populace for political, cultural, or other reasons, compounding the complexity of FP in such situations. Active support from some portion of the civilian population is key to countering Level I threats.

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. Level II threats may consist of well-coordinated, but small-scale, hit and run attacks, IED and VBIED attacks, ambushes, and may involve the

employment of indirect fire such as mortars and rockets. Level II threats may include special operations forces highly trained in irregular warfare whose operations are similar to those outlined in the Level I threat including air, land, and maritime vehicle hijacking. Such forces may seek to establish and activate espionage networks, collect intelligence, carry out specific sabotage missions, develop target lists, and conduct raids and ambushes.

Level III Threats. Level III threats may be encountered when an enemy has the capability to project combat power in one or more domain in an operational area. Specific examples include airborne, heliborne, and amphibious operations; large combined arms ground force operations; and infiltration operations involving significantly sized (company or larger) conventional forces. 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 may exceed the capability of base and base cluster security forces and air defenses, requiring additional forces, resources, fire support, or significant combat action to effectively counter the threat.

Commanders at all levels should use their own localized FP 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) 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.

FORCE PROTECTION CONDITIONS

FPCONs are arranged in a graduated order ranging from FPCON Normal to FPCON Delta. 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:[10]

- **FPCON Normal**—This condition applies at all times as a general threat of terrorist attacks, hostile acts, or other security threats always exists in the world.
- **FPCON Alpha**—This condition applies to a non-specific threat of a terrorist attack or hostile act directed against DOD elements and personnel. Commanders declare FPCON Alpha when a terrorist attack or hostile act is possible, but no specific information exists indicating a direct or indirect threat to DOD elements and personnel. Commanders must be able to sustain applicable FPCON Alpha measures indefinitely.
- **FPCON Bravo**—This condition applies when an increased or more predictable threat of a terrorist attack or hostile act exists and is directed against DOD elements and personnel. Commanders should be able to sustain all applicable FPCON Bravo

[10] DOD Instruction 2000.16, Volume 2, *DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System,* has a detailed discussion and listings of FPCONs and the mandatory measures for each.

measures indefinitely and understand FPCON Bravo will likely affect missions and base support operations during prolonged implementation.

- **FPCON Charlie**—This condition applies when a terrorist or hostile act incident occurs within the commander's area of interest, or intelligence is received indicating a hostile act or some form of terrorist action or targeting against DOD elements, personnel, or facilities is likely. FPCON Charlie measures will very likely affect missions and base support. Commanders should ensure they can sustain applicable FPCON Charlie measures throughout the entirety of the threat.

- **FPCON Delta**—This condition applies when a terrorist attack or hostile act has occurred or is anticipated against specific installations or operating areas. FPCON Delta should be maintained on a limited basis and only be declared so long as the necessary response capabilities are required.

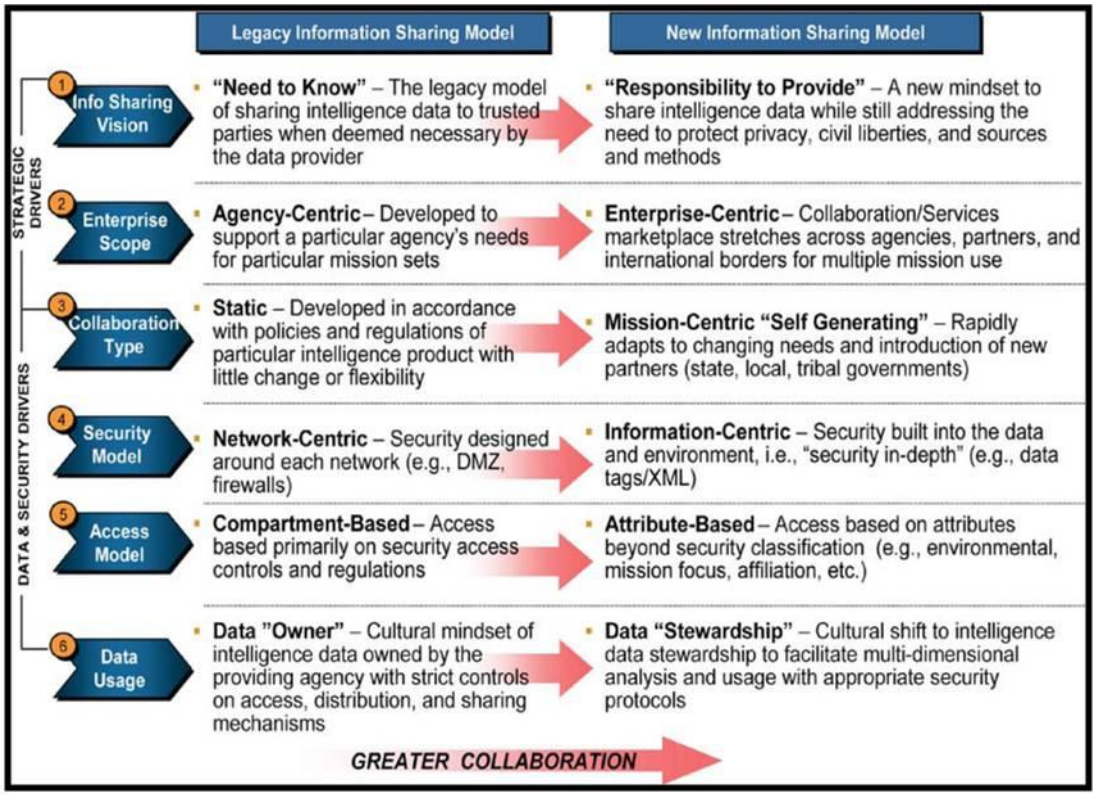
The persistence of threats reflects the number and intensity of conflicts around the world and the inherent difficulties of facing, assessing, and overcoming the objectives of threat perpetrators. All Airmen involved in FP benefit from a thorough understanding of these types of objectives. This understanding enhances planning to counter FP threats, thereby improving the FP status of organizations and personnel.

On March 2, 2011, a 21-year-old Kosovan male conducted a "lone wolf" attack on a bus containing US Air Force personnel from RAF Lakenheath at Frankfurt Airport, Frankfurt, Germany. The attacker spoke with an Airman smoking outside the bus. Upon learning the bus contained Service members on their way to Afghanistan, he shot and killed the Airman. The gunman then entered the bus, killed the driver and wounded two other Airmen. He held his pistol to the head of a fifth Airman, but the weapon jammed and the attacker fled the scene. He was quickly subdued and later admitted to being motivated by online extremist propaganda. Unpredictable attacks like this highlight the inherent difficulty of assessing and overcoming every objective of threat perpetrators. Force protection planners should consider the gamut of risks and hazards and strive to mitigate their effects.

CHAPTER 4: FORCE PROTECTION INTELLIGENCE AND COUNTERINTELLIGENCE SUPPORT TO FORCE PROTECTION

Intelligence is a collaborative effort between intelligence, counterintelligence, security forces, the medical and preventive medicine communities, EM, weather, and communications. However, the roles of each differ depending on location (within our outside the US) due to executive orders and other policies. Through collaboration, commanders at all levels are provided a more accurate threat picture, enhancing the protection of personnel, resources, and information. All-source intelligence should be provided on threats to 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.[11]

The figure, "United States Intelligence Community Information Sharing Strategy," portrays an information sharing strategy used in the intelligence community, illustrating the importance of this cooperation necessary for intelligence to support FP.



United States Intelligence Community Information Sharing Strategy

[11] FPI deals specifically with intelligence efforts to counter enemy threats. For additional information on incident awareness and assessment, see AFDP 2-0, *Intelligence,* and AFI 71-101V4, *Counterintelligence*. For additional information on intelligence oversight, see DOD Directive 5240.01, *DOD Intelligence Activities*.

FORCE PROTECTION INTELLIGENCE

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. In concert with OPSEC requirements, commanders should develop critical information requirements to guide FPI work supporting their decision-making and operations. 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 and preventive medicine communities, 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 Department of the Air Force (DAF) guidance. Constant liaison with local counterparts and host nation forces also enhances cooperation and willingness to share information, especially in crisis situations.

COUNTERINTELLIGENCE SUPPORT TO FORCE PROTECTION

Counterintelligence support to force protection (CIFP) is the employment of AFOSI capabilities to find, fix, track, and neutralize enemy threats to create a sustained permissive environment for operations. CIFP is essential in detecting, assessing, denying, and responding to threats affecting operations. CIFP are intelligence-driven operations using information derived from multiple intelligence and counterintelligence sources providing tactical situational awareness to forewarn or preempt adversary attack. CIFP activities include counterintelligence collection, analysis, and investigation; surveillance; and countersurveillance. These activities provide valuable intelligence that assists FP operations, enabling base defense forces to identify, monitor, and eliminate threats.

Though adversaries have the advantage of choosing the time and place for their attacks, they typically require extensive pre-attack planning and preparation to maximize chances for success. To do so, enemy forces collect intelligence and conduct physical surveillance and other activities, providing a critical window within which vigilant CIFP activities stand the greatest chance of detecting threats before they occur. By compiling and analyzing suspicious activity reports, indications and warnings of pre-attack activity may be discovered, enabling an effective response to thwart or defeat an impending threat. Such activities are a high priority task for the intelligence community, law enforcement, security elements, and local community authorities.

CHAPTER 5: FORCE PROTECTION PLANNING

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 area designated as a base boundary.

BASE DEFENSE ZONE IDENTIFICATION AND COORDINATION

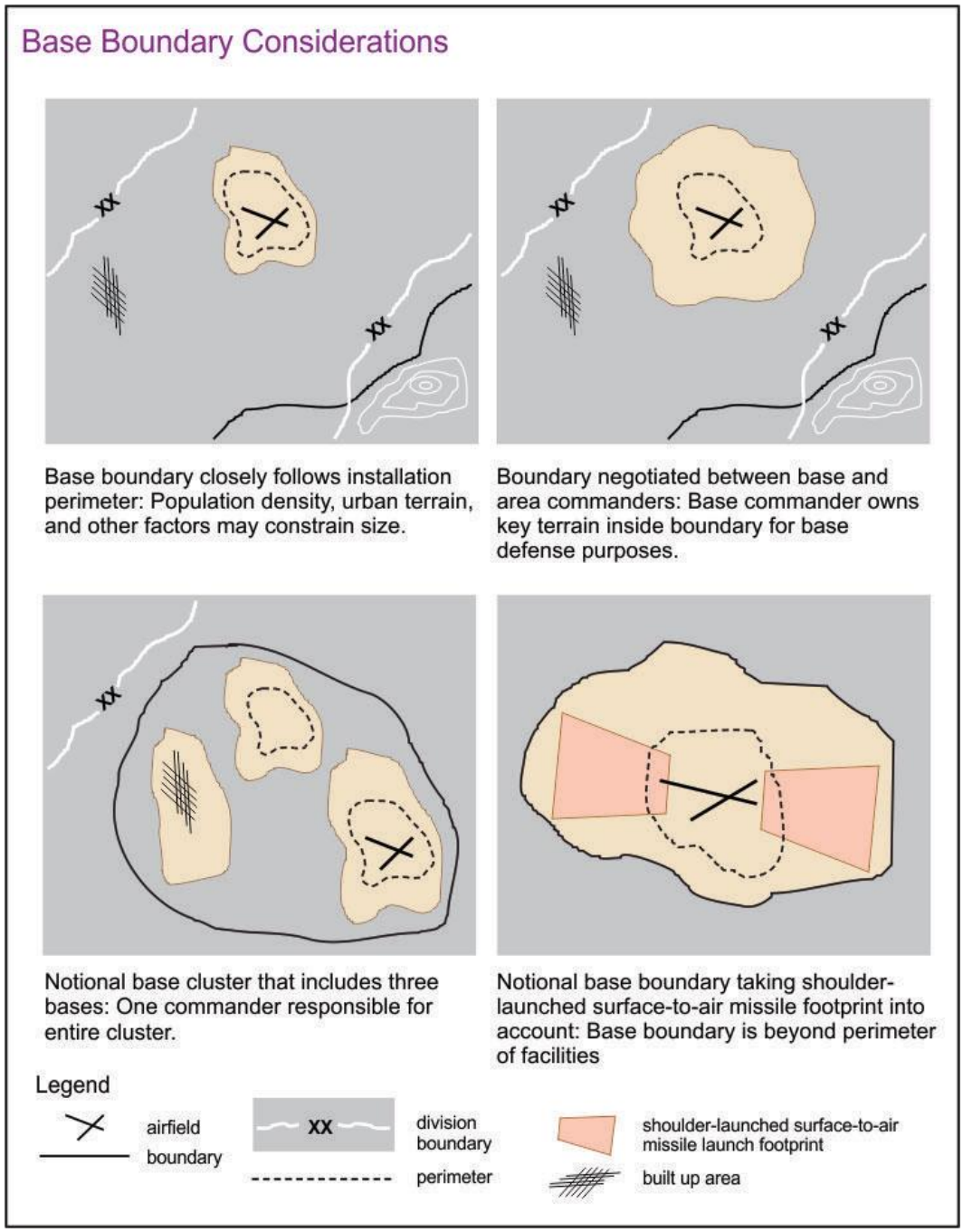
To ensure FP planners identify the areas that may be under threat, they should recognize the locations that may be affected by forces posing a threat. For planning purposes, the relationship of the base perimeter and the base boundary should be understood, and planners should use the planning construct of the base security zone (BSZ) to ensure proper planning considerations are taken into account.

BASE PERIMETER

The base perimeter is the physical and logical base boundary. The base perimeter is not the first line of defense from which all efforts to deter, detect, delay, deny, and defeat an enemy begin. Rather, in the context of protecting a system of systems, it is the last line of defense against a determined enemy. If an enemy penetrates the base perimeter, personnel should mobilize to delay adversary progress and deny them opportunities to achieve their objective. This enables base defense forces to defeat the enemy by maneuvering, regaining the initiative, and culminating offensively.

BASE BOUNDARY

JP 3-10 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 on the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations. It should balance the need of base defense forces to control key terrain with their ability to accomplish the mission. Whenever a USAF or US Space 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 senior USAF or US Space Force commander is not the base commander and the base boundary does not include all the terrain of concern, as identified by the BSZ, the air component commander's staff should support subordinate commanders in their efforts to mitigate risks of enemy attack. The figure, "Base Boundary Considerations," illustrates these considerations. Where the base boundary and BSZ are not congruent, commanders should understand the vulnerability and risk to airpower in takeoff and landing patterns and the threat of standoff weaponry ranges that exceed the base boundary. Commanders should work with the host nation and sister Services to mitigate these vulnerabilities to the extent possible.



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

BASE SECURITY ZONE

The USAF uses the planning construct of the BSZ to ensure threats that could impact operations are considered and planned for. 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. Focused intelligence preparation of the battlespace

(IPB) efforts and base defense operations should operate in unison to support BSZ establishment. FP planners should first establish this planning construct through IPB, and then seek to align it with the negotiated base boundary—the area allocated to the base commander for protection. If the BSZ does not align with the base boundary, then USAF security planners should coordinate with battlespace owners to ensure the protection of airpower resources.

RISK MANAGEMENT PROCESS

Commanders, with input from appropriate staff, determine how best to manage risks. FP should be based on risk management, not risk elimination. This requires a balance between risk mitigation and mission accomplishment, resulting in risk acceptance. The USAF defines RM as the "systematic process of identifying hazards, assessing risk, analyzing risk control options and measures, making control decisions, implementing control decisions, accepting residual risks, and supervising/reviewing the activity for effectiveness."[12] In all cases, the assessments include threats as well as hazards. An RM process supporting FP can consist of the following elements:

- Prioritizing assets and resources through a **criticality assessment**. The criticality assessment identifies the relative criticality of assets based on mission criticality, impact on national defense, replaceability, and monetary value. The primary objectives in an effective 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.

- Identifying potential threats with a **threat assessment**. 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. 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.

- Analyzing resource and asset vulnerabilities through a **vulnerability assessment**. This assessment should address the broad range of medical and physical threats to the security of the commander's personnel and resources based on the criticality assessment. It then considers the identified and projected threats against personnel, facilities, or other assets to identify those areas where resources are susceptible to actions that may reduce or diminish operational effectiveness.

- Determining the risks acceptable for a given operation by conducting a **risk assessment**. This assessment compares the relative impact of any loss or damage

[12] This Air Force definition, found in AFPD 90-8, *Environmental, Safety and Occupational Health Management and Risk Management*, is in accord with 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" (JP 3-0, *Joint Campaigns and Operations*; common access card required).

to an asset (criticality) with the relative probability of an unwanted event. Risks to the most critical USAF 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.

- **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. OPSEC should be considered during the RM process as well.

Safety, as applied via RM, is a major element of FP planning and should be used in the risk assessment phase of the RM process when planning to counter a threat. The RM process established in USAF safety channels ideally lends itself to planning for FP efforts.[13] Safety has a strong impact on FP's overall effectiveness.

[13] See AFI 90-802, *Risk Management,* and Air Force Policy Directive (AFPD) 10-24, *Mission Assurance.*

APPENDIX: ADDITIONAL FORCE PROTECTION LINES OF EFFORT

FP covers a diverse range of measures and capabilities. These additional lines of effort are incorporated throughout Service and joint doctrine, as well as policy that delineates programs and activities in support of the overall FP effort for the joint force:

- Provide air, space, and missile defense. For guidance on countering theater air and missile threats, refer to AFDP 3-01, *Counterair Operations*.
- Provide CBRN defense and minimize the effects of CBRN incidents. For guidance on CBRN defense, refer to AFDP 3-40, *Counter-Weapons of Mass Destruction Operations.*
- Conduct defensive countermeasure operations, including military deception in support of OPSEC, counter deception, and counterpropaganda operations. For guidance on defensive countermeasure operations, refer to JP 3-13.4, *Military Deception*.
- Conduct OPSEC, cyberspace defense, cyberspace security, and electronic protection activities. For guidance on OPSEC, refer to CJCSI 3213.01, *Joint Operations Security*, and JP 3-13.3, *Operations Security*. For guidance on cybersecurity, refer to DOD Instruction 8500.01, *Cybersecurity*. For guidance on electromagnetic warfare, refer to AFDP 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations.* For guidance on cyberspace operations, refer to AFDP 3-12, *Cyberspace Operations*.
- Conduct personnel recovery operations. For guidance on personnel recovery, refer to AFDP 3-50, *Personnel Recovery.*
- Perform mission assurance, a process to protect or ensure the continued function and resilience of critical capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DOD mission-essential functions in any operating environment or condition. Guidance on mission assurance is provided in DOD Directive 3020.40, *Mission Assurance*, and AFPD 10-24, *Mission Assurance*.
- Provide EM and response capabilities and services. EM 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 USAF incident management system. EM 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 AFPD 10-25, *Air Force Emergency Management Program,* and DOD Instruction 6055.17, *DOD Emergency Management (EM) Program*, for more information on the installation EM and installation EM response program.

REFERENCES

All websites accessed 8 February 2023.

Doctrine can be accessed through links provided at: https://www.doctrine.af.mil/

US AIR FORCE DOCTRINE: https://www.doctrine.af.mil/

- AFDP 1, *The Air Force*
- AFDP 2-0, *Global Integrated Intelligence, Surveillance, and Reconnaissance*
- AFDP 3-01, *Counterair Operations*
- AFDP 3-12, *Cyberspace Operations*
- AFDP 3-27, *Homeland Operations*
- AFDP 3-40, *Counter-Weapons of Mass Destruction Operations*
- AFDP 3-50, *Personnel Recovery*
- AFDP 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*
- AFDP 4-02, *Health Services*

JOINT DOCTRINE

Joint Electronic Library (JEL): https://www.jcs.mil/Doctrine/

JEL+: https://jdeis.js.mil/jdeis/index.jsp?pindex=2

- JP 1, Volume 2, *The Joint Force*
- JP 3-0, *Joint Operations*
- JP 3-10, *Joint Security Operations in Theater*
- JP 3-12, *Cyberspace Operations*
- JP 3-13.3, *Operations Security*
- JP 3-13.4, *Military Deception*
- Joint Doctrine Note 1-19, *Competition Continuum*

MISCELLANEOUS PUBLICATIONS

- AFI 32-9001, *Acquisition of Real Property*
- AFI 71-101V4, *Counterintelligence*
- AFI 90-802, *Risk Management*
- AFPD 10-24, *Mission Assurance*
- AFPD 10-25, *Air Force Emergency Management Program*
- AFPD 10-26, *Countering Weapons of Mass Destruction*
- AFPD 90-8, *Environmental, Safety and Occupational Health Management and Risk Management*
- CJCSI 3213.01, *Joint Operations Security*
- Department of the Air Force Instruction 10-2602, *Countering Weapons of Mass Destruction Enterprise*
- DOD Directive 3020.40, *Mission Assurance*
- DOD Directive 5240.01, *DOD Intelligence Activities*
- DOD Instruction 2000.12, *DOD Antiterrorism (AT) Program*
- DOD Instruction 6055.17, *DOD Emergency Management (EM) Program*

- DOD Instruction 8500.01, *Cybersecurity*
- Homeland Security Presidential Directive 5
- National Response Framework
- Presidential Executive Order 12333, *United States Intelligence Activities*
- *The Military Commander and the Law*
- Title 10, U.S. Code, *Armed Forces*
- Title 40, U.S. Code, §§3111 and 3112
- US Constitution
- US Northern Command