BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE

31-1

21 JUNE 2018

Security

INTEGRATED DEFENSE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A4SP

Certified by: AF/A4S
(Brig Gen Andrea D. Tullos)

Supersedes: Air Force Policy Directive 31-1, 28 October 2011

Pages: 12

This Air Force Policy Directive (AFPD) establishes the framework for how the Air Force formulates and applies Integrated Defense. This Directive implements Department of Defense (DoD) Directive 3025.13, *Employment of DoD Capabilities in Support of the United States Secret Service, Department of Homeland Security;* DoD Instruction 3224.03, *Physical Security Equipment Research, Development, Test, and Evaluation*; DoD Instruction 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board;* DoD Instruction 5100.76, *Safeguarding Sensitive Conventional Arms, Ammunition, and Explosives;* DoD Directive 5200.31E, *DoD Military Working Dog Program;* DoD S-5210.41-M, *Nuclear Weapon Security Manual;* DoD Directive 5210.56, *Arming and the Use of Force; and* Directive Type Memorandum 09-012, *Interim Policy Guidance For DoD Physical Access Control.* This Directive interfaces with Air Force Doctrine, Annex 3-10, *Force Protection*, and Annex 3-27, *Homeland Operations*, and joint doctrine contained in the Joint Publication 3-10, *Joint Security Operations in Theater*. This Directive issues overarching policy on conducting integrated defense operations in order to sustain air, space, and cyberspace operations. Compliance with this directive is mandatory and applies to all military and civilian Air Force personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. The terms "must," "shall," and "will" denote mandatory actions. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System Records Disposition Schedule. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the AF Form

847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

This document updates the authorities transferred to the Air Force Installation and Mission Support Center as well as general updates throughout the document.

1. OVERVIEW.

1.1. Air, space and cyberspace power projection assets are critical enablers to the national security of the United States and contribute to the achievement of national strategy objectives. A central and fundamental component of the Air Force capability is the power projection platform from which we operate, our installations and, their most important critical enabler, our professional Airmen. Both require a deliberate and focused security strategy for protecting and defending air, space, and cyberspace power, one that considers mission accomplishment, threats, vulnerabilities, and the inherent risks associated with operation of a military installation. Within the Air Force, that strategy is integrated defense.

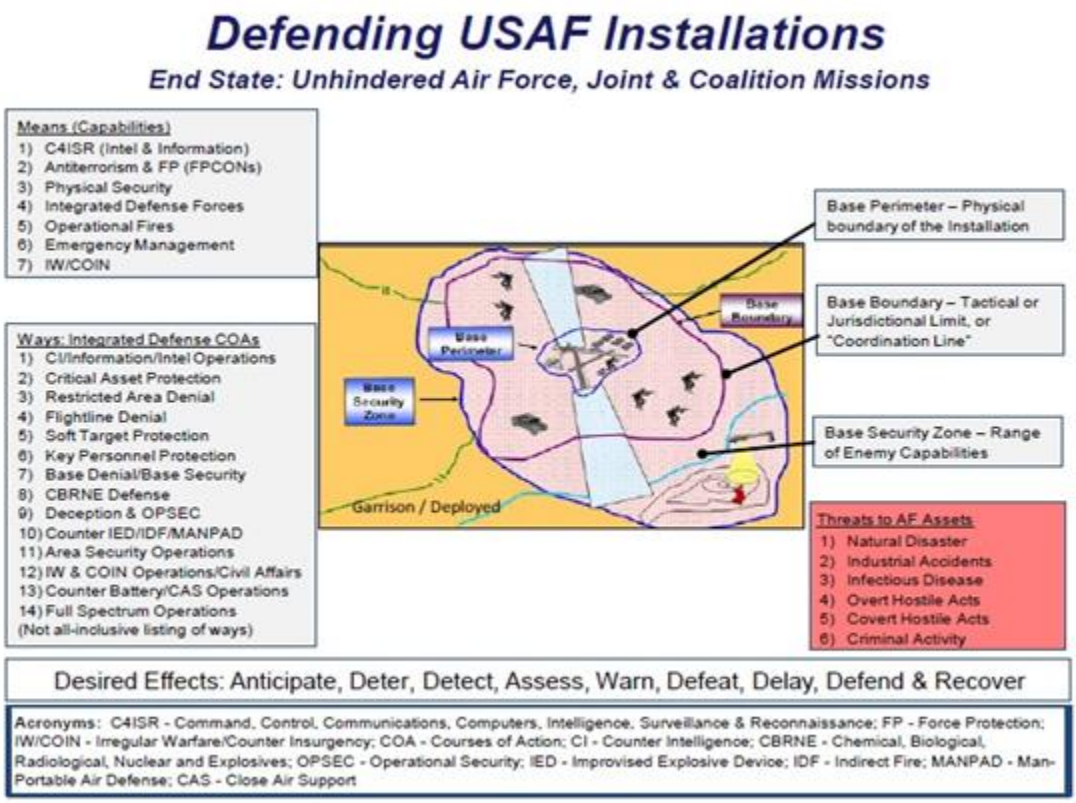
2. POLICY.

2.1. Protecting and defending Air Force Installations is a strategy; an ends, ways, and means construct, that employs a number of Air Force capabilities in a variety of ways to produce desired effects in the base defense battle space. This strategy, as depicted in **Figure 1.1.**, leverages assigned Air Force resources against adaptive threats to protect Air Force resources and personnel.

2.2. It is an installation commander's inherent responsibility to identify risks and develop risk management strategies to produce effects-based, integrated defense plans to ensure unhindered Air Force, Joint and Coalition missions.

2.3. Integrated defense is the incorporation of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations within the base boundary and the base security zone. These air and land threats include, but are not limited to, terrorists, insiders, foreign intelligence entities, criminals, and enemy forces. It is critical to incorporate integrated defense efforts with other Air Force, joint and combined capabilities to achieve synergistic effects using an all-hazards approach. Potential hazards to an installation include, but are not limited to, Chemical Biological, Radiological, Nuclear-High Yield Explosive attacks, natural and man-made disasters, major accidents, and accidental or deliberate release of hazardous materials, toxic industrial materials, or chemicals.

Figure 1.1. Integrated Defense Concept.



2.4. Installation commanders possess a wide variety of capabilities available to accomplish Integrated Defense. These capabilities (means) as shown in **Figure 1.1.** are not all encompassing and are critical to ensuring unhindered Air Force, Joint and Coalition operations in all environments from United States/outside United States to austere deployed locations.

2.5. The integration of multiple Air Force capabilities within the risk management process helps facilitate course of action development focused on achieving specific desired effects designed to protect and defend critical assets necessary to meet the commander's intent.

2.6. The nine Integrated Defense Desired Effects are: Anticipate, Deter, Detect, Assess, Warn, Defeat, Delay, Defend and Recover. Ideally, intelligence and threat information enable commanders to anticipate threats and hazards as the first step in protecting and defending an installation. Commanders identify additional integrated defense effects to enable planning and course of action development. Installation commanders publish the desired effects in a commander's intent and mission statement.

2.7. Integrated Defense Courses of Action (ways) comply with applicable laws and regulations. The laws, customs and culture, Status of Forces Agreements, Rules of Engagement and Law of Armed Conflict in some areas of operation may impose constraints and restrictions on integrated defense operations. Therefore, installations work to synchronize integrated defense efforts with friendly forces operating within the base security zone.

2.8. Commanders require timely and credible information and/or intelligence to protect their resources and make integrated defense operations decisions. The synchronization of information is executed through the information fusion cell in accordance with Air Force policy and guidance and tactics, techniques, and procedures.

2.9. Communications with and dispatch of integrated defense forces is conducted from the Base Defense Operations Center which is, typically, a part of the base Emergency Communications Center (deployed Base Defense Operations Centers could report to a Tactical Operations Center, Joint Operations Center, etc.). Command and control of integrated defense forces will be conducted in accordance with the Air Force Incident Management System which is explained in AF Manual 10-2502, *Air Force Incident Management System Standards and Procedures*.

2.10. Commanders of nuclear capable installations must plan and execute nuclear weapon security operations in accordance with DoD S-5210.41-M, *Nuclear Weapon Security Manual*, and AF Manual 31-108, Volumes 1-3, *Air Force Nuclear Weapons Security Manual* supplement.

3. ROLES AND RESPONSIBILITIES.

3.1. Commanders at all levels:

3.1.1. Are responsible for executing assigned missions in the installation's integrated defense plan.

3.1.2. Organize, train, and equip appropriate forces to conduct and sustain assigned integrated defense operations.

3.1.3. Align mission assurance-related activities with integrated defense.

3.2. AF/A1:

3.2.1. Provides guidance on roles and responsibilities for determining and validating Security Forces manpower.

3.2.2. Provides policy and guidance for integrating and vetting new/emerging institutional education and training requirements or learning outcomes into accessions, professional military education, and ancillary training.

3.3. AF/A2:

3.3.1. Provides operational, planning, programming and budgeting guidance for Air Force intelligence support to integrated defense operations.

3.3.2. Provides guidance supporting intelligence preparation of the operational environment, other threat information, and staff estimates to support installation commanders' integrated defense operations.

3.3.3. Provides collection management guidance for Intelligence, Surveillance and Reconnaissance assets to support integrated defense operations within the base security zone.

3.4. AF/A3:

3.4.1. Approves the Protection Level of Air Force assets.

3.4.2. Oversees development of homeland defense and civil support doctrine, policy, and operational standards, as outlined in AF Policy Directive 10-8, *Defense Support of Civil Authorities.*

3.5. AF/A4:

3.5.1. Establishes policy and guidance relating to training, organizing, and equipping of personnel for all facets of Logistics, Engineering and Force Protection for Integrated Defense.

3.5.2. Ensures Integrated Defense, including sustainment and readiness, through planning, programming, and budgeting.

3.5.3. Establishes implementation guidance for Integrated Defense.

3.5.4. Integrates Air Force policy pertaining to protection and defense against all threats and hazards to Air Force installations.

3.5.5. Develops and coordinates with AF/A1D approval to integrate institutional education and training requirements, e.g., ancillary training, Professional Military Education, and accessions into the appropriate venues in support of Integrated Defense operations prior to levying on the Total Force. **NOTE:** Career field specific requirements are coordinated with the respective career field manager and/or Functional Authority Force Development for integration into the Career Field Education Training Plan and Course Training Standard as appropriate.

3.5.6. Through the AF/A4S, retain the roles of strategy development, policy and guidance, resource advocacy, engagement with external agencies, and career field management.

3.5.7. Through the AF/A4S, develops and oversees, planning, training, integration, and guidance for effects-based integrated defense capabilities.

3.5.8. Through the AF/A4S, manages integration of integrated defense forces capabilities into Air Force, Joint and Coalition planning and operations.

3.5.9. Through the AF/A4S, manages integrated defense risk management methodology and approaches.

3.5.10. Through the AF/A4S, establishes policy for Air Force Law and Order programs.

3.5.11. Through the AF/A4S, provides the DoD Physical Security Review Board with incident information relating to conventional arms, ammunition, and explosives and provide support to the Undersecretary of Defense (Intelligence) for task groups related to safeguarding arms, ammunition, and explosives.

3.5.12. Through the AF/A4S, directs development of policy pertaining to arming of integrated defense forces.

3.5.13. Through the AF/A4S, designates a DoD program manager for all matters pertaining to training of DoD military working dogs.

3.5.14. Ensures the AF/A4S coordinates with Undersecretary of Defense (Intelligence) on development of policy for proper employment of explosive detection dog teams in support of the United States Secret Service.

3.5.15. Through the AF/A4S, designates an individual to represent the Department of the Air Force in the DoD Physical Security Enterprise and Analysis Group.

3.5.16. Through the AF/A4S, directs, creates and develops training based on emerging training requirements derived from policy or effects gaps.

3.5.17. Ensures the AF/A4S determines minimum system security standards. Advocates Major Command, Air Force Reserve Command, and Air National Guard manpower, facilities, and equipment requirements for conducting integrated defense operations.

3.5.18. Ensures the AF/A4S coordinates with the Undersecretary of Defense (Intelligence) on the physical security of DoD installations and resources.

3.5.19. Ensures the AF/A4S develops policy and provides oversight for Air Force integrated defense technology and equipment requirements.

3.5.20. Through the AF/A4C, provides field expertise, recommendations, support, and other input for structural, environmental, Fire Emergency Services, Explosive Ordnance Disposal, Emergency Management and other engineer areas of expertise.

3.5.21. Through the AF/A4C, implements non-medical Counter-Chemical, Biological, Radiological, and Nuclear passive defense and consequence management programs as part of the Emergency Management program.

3.5.22. Ensures the AF/A4C develops engineer-related force protection and integrated defense training standards and equipment requirements.

3.6. AF/A10:

3.6.1. Oversees development of Counter Chemical, Biological, Radiological, and Nuclear doctrine policy, and operational standards as outlined in AFPD 10-26, *Countering Weapons of Mass Destruction Enterprise.*

3.7. AF/SG:

3.7.1. Develops medical-related force protection and integrated defense training standards and equipment requirements.

3.7.2. Provides field expertise, recommendations, support, and other input for medical emergency management, medical Chemical, Biological, Radiological, and Nuclear operations, and other medical areas of expertise.

3.8. SAF/IG:

3.8.1. Ensures Air Force Office of Special Investigations provides installation commanders and Defense Force Commanders applicable counterintelligence information within the base security zone.

3.8.2. Ensures Air Force Office of Special Investigations establishes an effective liaison with host nation and civilian intelligence, security, and law enforcement agencies.

3.8.3. Ensures Air Force Office of Special Investigations maintains the capability to respond to criminal activities in support of law and order operations.

3.8.4. Ensures Air Force Office of Special Investigations provides immediate, worldwide, complementary support to the deployed area commanders by conducting specialized counterintelligence, counter-threat, and protective service operations.

3.9. Major Commands:

3.9.1. Provide direction for all integrated defense planning and operations through the range of military operations.

3.9.2. Develop guidance and procedures in support of installation integrated defense planning and operations.

3.9.3. Ensure fused force protection information is used to support commanders in executing Integrated Defense, Antiterrorism and Emergency Management responsibilities.

3.9.4. Define and/or validate, prioritize and advocate for requirements directly related to the integrated defense mission to inform the Major Command and Installation and Mission Support governance processes.

3.10. National Guard Bureau:

3.10.1. Develops guidance and procedures in support of Air National Guard installation integrated defense operations.

3.10.2. Programs and budgets resources to organize, train, and equip Air National Guard integrated defense forces in support of Air National Guard installation integrated defense operations.

3.11. Air Force Installation and Mission Support Center:

3.11.1. Serves as the single intermediate-level organization providing oversight of Installation and Mission Support capabilities to Major Commands/Direct Reporting Units and their subordinate organizations and installations.

3.11.2. Serves as the input source and submits options for programming actions with substantiating analysis in support of the integrated defense portfolio.

3.11.3. Programs and budgets resources to organize, train, and equip integrated defense forces in support of installation integrated defense operations.

3.11.4. Provides advocacy for Air Force requirements and cost and justification information to the DoD Physical Security Enterprise and Analysis Group in support of program budgeting and execution.

3.11.5. Provides tactical employment and program management of DoD Explosive Detection Dog teams to support the United States Secret Service.

3.11.6. Provides guidance and oversight of Security Forces units' equipment requirements. Coordinates research, procurement, and standardization for Major Command units' equipment. Provides management of Manpower and Equipment Force Packaging functions and subsequent Logistics Detail requirements for Security Forces applicable Unit Type Codes. Collects and prioritizes equipment requirements for consideration by the Security and Protection Category Council.

3.11.7. Executes organization training and equipping requirements (e.g., standardization and activity management). Provides development, access and sustainment support to authoritative databases/systems as required to achieve garrison and deployed integrated defense operations.

3.12. Installation Commanders:

3.12.1. Minimize mission degradation from threat activity within the base boundary and coordinate necessary support within the base security zone when the base security zone is not congruent with the base boundary; minimize loss of life and injury from threat activity and natural events; and protect government property and personnel from natural disasters, hostile and criminal acts.

3.12.2. Serve as the Integrated Defense risk acceptance authority for assigned, attached, or transient DoD personnel and assets.

3.12.3. Ensure an organic capability exists to continuously fuse all-source force protection information and deliver force protection intelligence in support of integrated defense.

3.12.4. Consider the potential effects produced by the threat/hazard, not just the nature of the threat/hazard.

3.12.5. Ensure installation commander's intent and risk tolerance level is known and incorporated into local plans and instructions.

3.12.6. Ensure the Defense Force Commander appropriately utilizes, coordinates, assigns and tasks the integrated defense force.

3.12.7. Ensure integrated defense operations are synchronized with the appropriate area of operations commander.

3.12.8. Establish and maintain appropriate support agreements with local, regional and state civil authorities, private sector organizations, and other federal facilities to address local support that either party might provide for immediate response to emergencies. When developing support agreements, commanders ensure that Air Force commitments are consistent with relevant regulatory and statutory requirements, including specific funding authority.

HEATHER WILSON
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD Directive 3020.40, *Mission Assurance,* 29 November 2016

DoD Directive 3025.13, *Employment of DoD Capabilities in Support of the United States Secret Service, Department of Homeland Security,* 8 October 2010

DoD Directive 5200.31E, *DoD Military Working Dog Program,* 10 August 2011

DoD Directive 5210.56, *Arming and the Use of Force,* 18 November 2016

DoD Instruction 2000.12, *DoD Antiterrorism Program,* 15 November 2016

DoD Instruction 2000.16 v1, *DoD Antiterrorism Standards,* 17 November 2016

DoD Instruction 3025.19, *Procedures for Sharing Information with and Providing Support to the United States Secret Service, Department of Homeland Security,* 29 November 2011

DoD Instruction 3025.21, *Defense Support of Civilian Law Enforcement Agencies*, 27 February 2013

DoD Instruction 3224.03, *Physical Security Equipment Research, Development, Test, and Evaluation,* 1 October 2007

DoD Instruction 5100.76, *Safeguarding Sensitive Conventional Arms, Ammunition, and Explosives,* 28 February 2014

DoD Instruction 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board,* 10 December 2005; IC3 20 November 2015

DoD Instruction O-5210.63, *DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials,* 21 November 2006

DoD Instruction 6055.17, *DoD Emergency Management Program,* 13 February 2017

DoD 5200.08-R, *Physical Security Program,* 27 May 2009

DoD S-5210.41-M, *Nuclear Weapon Security Manual,* 1 September 2015

Directive Type Memorandum 09-012, *Interim Policy Guidance for DoD Physical Access Control*, 8 December 2009; IC7 17 April 2017

Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms,* February 2017

Joint Publication 3-10, *Joint Security Operations in Theater,* 13 November 2014

Joint Publication 3-27, *Homeland Defense,* 29 July 2013

Air Force Doctrine Annex 3-10, *Force Protection,* 13 August 2014

Air Force Doctrine Annex 3-27, *Homeland Operations*, 26 April 2016

AF Policy Directive 10-25, Emergency Management, 28 April 2014

AF Policy Directive 10-26, Countering Weapons of Mass Destruction Enterprise, 17 June 2015

Headquarters United States Air Force Program Action Directive 14-04, *Implementation of the Air Force Installation and Mission Support Center*, 25 February 2015

AF Manual 10-2502, *Air Force Incident Management System Standards and Procedures*, 25 September 2009

AF Manual 31-108, *Air Force Nuclear Weapon Security Manual Volumes 1-3*, 15 June 2017

AF Manual 33-363, *Management of Records*, 1 March 2008; AFGM2017-01, 2 June 2017

Homeland Security Presidential Directive-5, *Management of Domestic Incidents*, 28 February 2003

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Terms

Air Force Incident Management System—A methodology designed to incorporate the requirements of Homeland Security Presidential Directive 5, the National Incident Management System, the National Response Framework, and Office of the Secretary of Defense guidance while preserving the unique military requirements of the expeditionary Air Force. The Air Force Incident Management System provides the Air Force with an incident management system that is consistent with the single, comprehensive approach to domestic incident management. The Air Force Incident Management System provides the Air Force with the coordinating structures, processes, and protocols required to integrate its specific authorities into the collective framework of Federal departments and agencies for action to include mitigation, preparedness, response, and recovery activities. It includes a core set of concepts, principles, terminology, and technologies covering the incident command system, emergency operations centers, incident command, training, identification, and management of resources, qualification and certification, and the collection, tracking and reporting of incident information and incident resources. The Air Force Incident Management System methodology is incorporated into current operating practices through revised instructions and manuals, training products, and exercise and evaluation tools.

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (Joint Publication 1-02)

Base Boundary—Joint Publication 3-10, *Joint Security Operations in Theater*, defines 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." Therefore, the base boundary is not necessarily the base perimeter; rather, it should be established based upon the factors of Mission, Enemy, Terrain and Weather, Time, Troops available, and Civil considerations, specifically balancing the need of the integrated defense forces to control key terrain with their ability to accomplish the mission. These measures decrease the likelihood of fratricide, prevent non-combatant casualties, and minimize damage to the property of friendly civilians. Boundaries may not necessarily coincide with the fenced

perimeter, property lines or legal boundaries. Nevertheless, while tactical considerations ideally determine integrated defense boundaries, the Defense Force Commander strictly adheres to legal, jurisdictional, host nation constraints, commander‘s intent, and higher echelon orders and directives when conducting operations within the base boundary.

Base Defense Operations Center—The Base Defense Operations Center is the command and control center for integrated defense operations during routine and emergency operations. The Base Defense Operations Center serves as the installation commander’s tactical operation center for the integrated defense effort and in that role should function as the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance integrator for integrated defense operations.

Base Perimeter—The physical boundary of the installation.

Base Security Zone—Planning term to describe the area of concern around an air base and to support the establishment and adjustment of the base boundary. The base security zone is the area outside the base perimeter from which the base may be vulnerable from standoff threats (e.g., mortars, rockets, man portable air defense systems). The installation commander should identify the base security zone and coordinate via their operational chain of command with local, state, federal agencies (inside the United States) or host nation or area commander (outside the United States) for the base security zone to be identified as the base boundary. If the base boundary does not include all of the terrain of the base security zone, the installation commander is still responsible for either mitigating (through coordination with local, state, federal agencies [inside the United States] or the area commander or host nation [outside the United States]) or accepting the risks of enemy attack from the terrain outside the base boundary.

Commander’s Critical Information Requirements—Include priority intelligence requirements and friendly force information requirements. Commander’s critical information requirements generate priority intelligence requirements and friendly force information requirements; the staff focuses on answering the commander’s critical information requirements to support the commander’s decision-making ability.

Emergency Communications Center—The nerve center of an installation’s emergency services response capability. Resources in the field communicate, often via radio, mobile data terminal, or mobile phone, with Emergency Communications Center controllers who then effectively manage the emergency resources for the area. These dispatch centers often use Computer Aided Dispatch software to assist in multiple incident dispatches to keep track of all the resources within their area of responsibility. The Emergency Communications Center includes a central dispatch capability or its interim equivalent for the installation. It should include the minimum functions of Fire Alarm Communications Center, Base Defense Operations Center, and Medical Dispatch (as applicable).

Force Protection—Preventive measures taken to mitigate hostile actions against DoD personnel (to include family members), resources, facilities, and critical information.

Force Protection Intelligence—Analyzed, all-source information concerning threats to DoD missions, people or resources and capabilities arising from terrorists/insurgents, insiders, criminal entities, foreign intelligence entities and opposing military forces and environmental/medical hazards. Force Protection Intelligence is proactive and drives force protection decisions and operations. Force Protection Intelligence is performed collaboratively

by Intelligence, Air Force Office of Special Investigations, and Security Forces personnel, with cooperation and support from several other entities (e.g., operations, weather, medical, communications). Intelligence supports unit deployments, readiness training, mission planning and other mission execution functions, to include, but not limited to integrated defense, critical asset risk management, and emergency management. Air Force intelligence activities are conducted on foreign adversaries or their agents, which generally means Air Force intelligence activities are conducted differently inside the United States as compared to outside the United States. Air Force Office of Special Investigations and other law enforcement entities are the lead for adversaries inside the United States, with intelligence providing support to their efforts, as appropriate.

Information Fusion Cell—Action cell where subject matter experts from the Intelligence, Air Force Office of Special Investigations, Antiterrorism and Security Forces collaborate and conduct Intelligence Preparation of the Operational Environment; the goal being to leverage information and intelligence to support the timely identification of indicators and warnings of emerging localized threats and threats within the area of interest. The Information Fusion Cell and its products are the primary information sources that directly support the installation commander, the Integrated Defense Working Group and the Threat Working Group in making proactive decisions for integrated defense planning. The Defense Force Commander ensures information gaps identified within the Integrated Defense Risk Management Process are properly identified. This is accomplished through the development of Priority Intelligence Requirements that are coordinated with the installation commander for inclusion into the Commander's Critical Information Requirements. Information Fusion Cell membership is determined by the installation/higher headquarters commander.

Integrated Defense—The integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to Air Force operations.

Law and Order Operations—Law and Order Operations are a core capability of Air Force Security Forces. These operations include active and passive defense measures, employed across the legally-defined operational environment, to mitigate potential risks and defeat adversary threats, to promote public order and efficient military operations. Law and Order Operations directly contribute to an installation's Integrated Defense. Law and Order Operations encompass many special disciplines. These include crime prevention, criminal investigations, corrections, traffic enforcement, access control and military working dogs. The specific authorities for Law and Order Operations may depend upon jurisdictional status of the installation which should be considered in planning for, and providing these Operations.

Operational Fires—Operational fires are the operational-level commander's application of nonlethal and lethal weapons effects to accomplish objectives during the conduct of a campaign or major operation.

Physical Security—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (Joint Publication 1-02)

Security—Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (Joint Publication 1-02)