BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-119

6 JANUARY 2004

Intelligence

INTELLIGENCE SUPPORT TO FORCE PROTECTION (FP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/XOIA
(Lt Col Gregory Kimbrell)

Certified by: HQ USAF/XOI
(Maj Gen Ronald Sams)

Pages: 12
Distribution: F

This instruction implements DoDD 2000.12, *DoD Antiterrorism Program*, DoDI 2000.16, *DoD Antiterrorism Standards*, AFPD 10-2, *Readiness*, AFPD 14-1, *Intelligence Applications and Requirements Planning*, AFPD 14-3, *Control, Protection and Dissemination of Intelligence Information*, AFPD 71-1, *Criminal Investigations and Counterintelligence*, AFMND 39, *Air Force Office of Special Investigations,* AFI 10-245, *Air Force Antiterrorism Standards,* AFI 14-105, *Unit Intelligence Mission and Responsibilities*, AFI 71-101 Vol 4, *Counterintelligence, and* CSAF message (DTG 060928Z Feb 01)*, Policy Guidance for Intelligence Support to Antiterrorism/Force Protection.* This instruction is to be used in conjunction with higher headquarters (HHQ) directives and local guidance. It establishes responsibilities and guidance for intelligence support to the Air Force FP Program. This Air Force Instruction (AFI) applies to Air Force Reserve Command and Air National Guard units. Records Disposition. Ensure that all records created by this AFI are maintained and disposed of IAW AFMAN 37-139, *Records Disposition Schedule*.

1. Mission and Responsibilities

1.1. Mission. Intelligence will provide timely, all-source threat analysis and prepare threat briefings to support planning and execution of Air Force operations. Intelligence support to force protection is a vital function that ensures commanders have the needed intelligence to make critical force protection and operational decisions. Through participation in Threat Working Groups (TWGs), development of various threat assessments and dissemination of actionable intelligence, intelligence personnel will ensure commanders, their staffs, air crews, AF Office of Special Investigations (AFOSI), Security Forces (SF) and other customers (e.g., Civil Engineers {CE}, Systems Communications and Information {SC}, Surgeon General {SG}, Tanker Airlift Control Center {TACC}) are provided current all-source threat information.

2. AJCOM Intelligence Responsibilities:

2.1. **Planning and Direction:**

2.1.1. Coordinate on all MAJCOM and HHQ policies affecting intelligence support to FP.

2.1.2. Designate in writing an intelligence professional(s) (officer, NCO, or civilian counterpart) to provide intelligence support to FP.

2.1.2.1. Individual(s) should have appropriate clearance and access to Top Secret (TS), Sensitive Compartmented Information (SCI), HUMINT Control System (HCS) and Gamma (G) data. MAJCOMs will ensure all intelligence professionals performing FP functions receive appropriate training.

2.1.2.2. For installations within the MAJCOM's chain of command that do not have intelligence professionals permanently assigned, establish procedures to ensure threat information is available to the installation commander (e.g., assigning non-intelligence personnel to fulfill the FP responsibilities listed in this instruction, establishing a Memorandum of Agreement {MOA}/Memorandum of Understanding {MOU} with local AFOSI detachments, BLUE DART, Operations Report-3 {OPREP-3} message or other products for immediate/rapid transmission of terrorist threat information).

2.1.3. Ensure Air Reserve Component (ARC) elements and assigned Individual Mobilization Augmentees (IMAs) are knowledgeable of FP intelligence support requirements and procedures. ARC elements and IMAs assigned to conduct specific FP duties or to support FP intelligence efforts should possess TS/SCI/HCS/G clearances.

2.1.4. Develop actions and implement a comprehensive intelligence support to FP program in compliance with HHQ standards and guidance. Processes and procedures must be documented in the form of a Concept of Operations (CONOPS), Operating Instructions (OIs) or Tactics, Techniques and Procedures (TTP).

2.1.4.1. Establish procedures to identify intelligence FP requirements and program for resources to meet requirements, including identifying intelligence manpower, training, security clearance, systems, facilities and information/production requirements.

2.1.4.1.1. Incorporate FP requirements into intelligence architecture and contingency planning, including 24/7 connectivity and requirement for access to TS, SCI, HCS and G information.

2.1.4.1.2. Individuals requiring clearances will work through their unit and MAJCOM Director of Personnel to get their Unit Manning Document (UMD) position(s) changed to reflect the need for an SCI clearance.

2.1.4.2. Establish processes/procedures for MAJCOM and subordinate wings/bases/centers to receive, evaluate, analyze and disseminate all relevant data on terrorist activities, trends and indicators of imminent attack, IAW the servicing Joint Intelligence Center (JIC)/Joint Analysis Center (JAC).

2.1.4.2.1. Analyze all-source intelligence and fuse it with Counterintelligence (CI) and Law Enforcement (LE) information provided by AFOSI.

2.1.4.2.2. In coordination with the MAJCOM TWG, assess the terrorist threat for the Area

of Interest (AOI) and provide threat information to subordinate units and commanders.

2.1.4.2.3. Coordinate, as required, with local, theater, national and other (e.g., Department of State {DoS}, coalition) intelligence agencies regarding threats.

2.1.4.2.4. Establish procedures to track active defense terrorism warnings and Intelligence Community terrorist threat alerts and advisories.

2.1.4.2.5. Incorporate threat information in FP planning and programming.

2.1.4.2.6. Utilize all-source threat information in support of vulnerability assessments and the installation threat assessment.

2.1.4.2.7. Support the development of risk assessments using threat and vulnerability assessment data.

2.1.4.3. Participate in the MAJCOM TWG IAW AFI 10-245.

2.1.4.4. IAW DoD Directive 2000.12, Geographic Combatant Commanders (GCC) have overall Antiterrorism (AT) responsibility within their Area of Responsibility (AOR). The GCC's force protection policies take precedence over all force protection policies or programs of any DoD Component, Element and personnel assigned, deployed, transiting through, performing exercises or training in the GCC's AOR.

2.1.5. In conjunction with the TWG and Force Protection Working Group (FPWG), participate in installation and HHQ vulnerability assessments IAW AFI 10-245 and DTRA/USAF Vulnerability Assessment Program Guidelines.

2.1.6. Oversee, inspect, exercise, assess, and report to AF/XOI (via AF/XOIA) NLT 10 October of each year on intelligence support to FP programs within the command, based on the standards set forth in this document. Reports should summarize the MAJCOM FP Intelligence Program and identify discrepancies, best practices and items for HHQ consideration.

2.1.7. Develop procedures for identifying and tracking all assigned MAJCOM intelligence professionals with FP background and experience.

2.2. **Collection and Requirements Management:**

2.2.1. Develop MAJCOM FP-related Priority Intelligence Requirements (PIRs) in cooperation with AFOSI and update them at least annually or IAW HHQ directives.

2.2.2. Coordinate with local, theater and national collection organizations, to include AFOSI Regional offices, to satisfy MAJCOM FP PIRs.

2.2.3. Monitor and evaluate reporting against FP intelligence collection requirements. Ensure evaluations are completed regularly to guide FP collection efforts.

2.2.4. Champion enhanced production requirements of sanitized and tearline reporting with Unified Command JICs/JAC for widest possible dissemination of threat information.

2.2.5. Annually assess how well FP PIRs are being satisfied in cooperation with AFOSI. Include findings of collection reviews in the annual report on intelligence support to FP (see paragraph **2.1.6.**).

2.3. **Employment and Deployment:**

2.3.1. MAJCOM Senior Intelligence Officers (SIO) will serve as the single point of contact (POC) responsible for ensuring intelligence support to FP is provided.

2.3.1.1. NLT 60 days prior to a deployment/exercise, prepare and submit pre-deployment message to servicing JIC/JAC identifying FP intelligence requirements (info copy to AF/XOIA). If deployment is short notice, a pre-deployment message will be submitted NLT 48 hours after deployment notification was received.

2.3.1.2. Ensure any unit deploying as part of an exercise, training or operational mission has their intelligence personnel cleared for TS, SCI, HCS and G intelligence material. This includes appropriate IMA and ARC personnel assigned to support FP. Those units that do not have access to TS, SCI, HCS and G at home station will arrange to have their personnel read into these programs either prior to deployment departure or upon arrival at the deployed location. These actions must be coordinated with the deployed Special Security Office (SSO) as soon as possible following official notification of the deployment. The deployed SSO will establish and maintain the "need to know" for personnel who are not already read into TS, SCI, HCS and G. Units that have access to these programs at home station must take care of the applicable requirements prior to deployment.

2.3.1.3. Ensure coordination with communications and SSO staff so that deploying intelligence personnel (including IMA and ARC personnel) have appropriate intelligence communications connectivity to access TS, SCI, HCS and G information and intelligence.

2.3.1.4. Ensure deployed units have an intelligence professional(s) (officer, NCO or civilian counterpart) designated in writing to provide intelligence support to FP.

2.3.1.5. Develop CONOPS/TTPs/OIs to establish intelligence dissemination processes, to include Foreign Disclosure, for various threat data. Ensure procedures are in place (e.g., TWG) to expeditiously coordinate with AFOSI and rapidly pass threat data to commanders, SF, Ops, etc. Additionally, ensure procedures are developed to expeditiously coordinate with AFOSI to pass terrorist threat data to coalition partners and host nation personnel.

2.3.1.6. Ensure procedures are in place for deployed units to transmit locally-derived threat information to HHQ and theater JIC/JAC. Terrorist threat information must be immediately provided to AFOSI for appropriate dissemination. Intelligence from post-deployment debriefings should reach HHQ and theater JIC/JAC within 48 hours and any "lessons learned" should reach HHQ, theater JIC/JAC and AF/XOIA within 7 days.

2.3.1.7. Support AFOSI in the development of annual installation threat assessments for all MAJCOM installations IAW AFI 10-245. MAJCOM and NAF INs will review all subordinate unit installation threat assessments, threat assessment findings, observations and recommendations.

2.3.1.8. Contact and exchange intelligence information with national-level agencies, AFOSI, law enforcement and CI organizations (via AFOSI), JICs/JAC, sister services, US embassies and country teams, to include US Defense Attaché Office (USDAO) and Regional Security Officer (RSO), as appropriate.

2.3.1.9. Ensure procedures, systems and/or databases are in place to incorporate real-world and exercise lessons learned and best practices into FP policies and procedures (i.e., FPWG, USAF Center for Knowledge and Sharing Lessons Learned Database, etc.).

2.3.1.10. Ensure continuity books are developed and maintained for FP functions.

2.4. **Training and Systems Support:**

2.4.1. Provide guidance for unit-level FP-related intelligence external training, Initial Qualification Training (IQT), Mission Qualification Training (MQT) and Continuation (internal) Training, including assigned or attached IMAs.

2.4.2. MAJCOM and locally established internal FP intelligence training programs should include the following:

2.4.2.1. Understanding terrorist TTPs

2.4.2.2. Conducting FP focused predictive analysis (e.g., IPB)

2.4.2.3. Developing threat assessments

2.4.2.4. Understanding terrorism threat methodologies (e.g., DoD, DoS, DHS)

2.4.2.5. Developing tailored threat assessments and assessing terrorist threat levels

2.4.2.6. Supporting FP planning

2.4.2.7. Supporting Vulnerability Assessments

2.4.2.8. Locating sources of FP intelligence, CI and LE information including the various threat levels and warning conditions

2.4.2.9. FP legal considerations (e.g., Intelligence Oversight policy)

2.4.3. Identify FP training requirements to AF/XOIA that should be incorporated into entry-level intelligence course and advanced skills courses (e.g., Intelligence Master Skills Course {IMSC}) curricula to enhance understanding of terrorist threats and the role intelligence plays in combating the threat.

2.4.4. Establish policy for updating individual training records to reflect FP training.

3. Wing/Base/Center/OSS Intelligence Responsibilities: Responsible for providing intelligence professionals to support FP for in-garrison, in-transit and deployed units.

3.1. **Collection and Requirements Management:** Identify and submit FP production requirements (PRs) IAW HHQ directives.

3.2. **Employment/Deployment:**

3.2.1. Provide FP intelligence support to commanders and their staffs through current, all-source intelligence products and briefings, focusing on terrorist capabilities, tactics, trends, courses of action and ongoing threat situation in the unit's AOI.

3.2.1.1. Ensure deploying intelligence personnel assigned to support FP (to include IMAs and ARC personnel) have TS, SCI, HCS and G security clearances. Those units that do not have access to TS, SCI, HCS and G at home station will arrange to have their FP personnel read into these programs either prior to deployment departure or upon arrival at the deployed location.

These actions must be coordinated with the deployed SSO as soon as possible following official notification of the deployment. The deployed SSO will establish and maintain the "need to know" for FP personnel who are not already read into TS, SCI, HCS and G. Units that have access to these programs at home station must take care of the applicable requirements prior to deployment.

3.2.1.2. Ensure coordination with communications and SSO staff so that deploying intelligence personnel (including IMAs and ARC personnel) have appropriate intelligence communications connectivity to receive Near Real Time (NRT), all-source threat updates.

3.2.2. Provide FP intelligence support and terrorist threat advisories to base organizations such as the TWG, FPWG, battle staff, air base operability/defense and tenant organizations as needed.

3.2.3. Analyze incoming intelligence for FP value and impact on unit mission, current and planned operations, exercises, air shows, significant Morale, Welfare and Recreation (MWR) events, etc. and rapidly disseminate significant FP threat information and intelligence to the TWG, battle staff, SF, aircrews, mission-planners, subordinate and lateral units, higher headquarters, other agencies and sister services as needed.

3.2.3.1. In coordination with the TWG, fuse all-source intelligence with CI and LE information provided by the AFOSI to analyze terrorist group patterns of behavior and identify evolving threats within the AOI.

3.2.3.2. Ensure FP is addressed in current intelligence briefings, pre-mission and pre-deployment briefings.

3.2.3.3. Ensure intelligence is incorporated in the FPWG, Vulnerability Assessment Teams (VATs), TWG and installation threat assessment.

3.2.3.4. Designate in writing an intelligence professional(s) (officer, NCO, or civilian counterpart) for intelligence support to FP.

3.2.3.4.1. Individual(s) should have appropriate clearance and access to TS, SCI, HCS and G data. Wing/base/center/OSS INs will ensure all intelligence professionals performing FP functions receive appropriate training. MAJCOMs can levy training requirements to satisfy unique or specialized mission areas.

3.2.3.4.2. For installations within the MAJCOM's chain of command that do not have intelligence professionals permanently assigned, ensure procedures are established to ensure threat information is available to the installation commander (e.g., assigning non-intelligence personnel to fulfill the FP responsibilities listed in this instruction, establishing MOA/MOU with local AFOSI detachments, BLUE DART, OPREP-3 message or other products for immediate/rapid transmission of terrorist threat information).

3.2.4. Ensure continuity books are developed and maintained for FP functions.

3.2.5. Establish formal procedures (i.e., CONOPS, OIs, TTPs, checklists) for providing FP intelligence to the local commander and providing such intelligence and/or coordinating with the TWG, FPWG, AFOSI, SF, SSO and other organizations, as appropriate.

3.2.5.1. Ensure Essential Elements of Information (EEIs) are included in debrief checklists.

3.2.5.2. After debriefing, threat information must be reported IAW tasking authority require-

ments. Terrorist threat information must be immediately provided to AFOSI for dissemination.

3.2.6. Document FP lessons learned and forward to TWG, FPWG and MAJCOM for action (as required) and entry into lessons learned databases.

3.2.7. Establish procedures to track operational, training and exercise wing deployments and coordinate with theater and national intelligence centers to ensure receipt of latest threat information, intelligence and deployment orders, particularly for in-transit units.

3.2.8. Identify all wing pre-deployment FP intelligence requirements NLT 60 days prior to deployment and forward to MAJCOM. If deployment is short notice, a pre-deployment message will be submitted NLT 48 hours after deployment notification was received.

3.2.9. In coordination with the TWG, develop realistic terrorist threat scenarios for installation exercises.

3.2.10. Participate in installation vulnerability assessments IAW AFI 10-245 and DTRA/USAF Vulnerability Assessment Program Guidelines.

3.2.11. Participate in the installation-level TWG IAW AFI 10-245.

3.2.12. Support AFOSI in the development of the installation threat assessment IAW AFI 10-245.

3.3. **Training and Systems Support:**

3.3.1. The wing/base/center FP Intelligence training program should be crafted with input from Operations Support Squadron, SF and AFOSI personnel.

3.3.2. Establish an internal FP intelligence-training program and develop an OI detailing how the program will be conducted. This program will follow MAJCOM guidance and standards for FP training at the unit level. Establish qualifications for intelligence personnel to certify as FP intelligence trainers prior to conducting training. Wing/base/center/OSS INs will ensure all intelligence professionals performing FP functions receive appropriate training.

3.3.2.1. Program must prepare all assigned intelligence personnel to perform FP responsibilities.

3.3.2.2. FP intelligence training should be included as part of the unit's IQT, MQT and Continuation Training (internal training) programs.

3.3.2.3. To the maximum extent possible, identify inbound personnel who will perform FP duties and arrange for them to attend appropriate FP training enroute to their new duty station.

3.3.2.4. Individual training records shall be updated to reflect FP training IAW MAJCOM policy.

3.3.2.5. Locally established internal FP training programs should address the following:

3.3.2.5.1. Understanding terrorist TTPs

3.3.2.5.2. Conducting FP focused predictive analysis (e.g., IPB)

3.3.2.5.3. Understanding terrorism threat methodologies (e.g., DoD, DoS, DHS)

3.3.2.5.4. Developing tailored threat assessments and assessing terrorist threat levels

3.3.2.5.5. Supporting FP planning and programming

3.3.2.5.6. Supporting Vulnerability Assessments

3.3.2.5.7. Locating sources of FP intelligence, CI and LE information including the various threat levels and warning conditions

3.3.2.5.8. FP legal considerations (e.g., Intelligence Oversight policy)

3.3.2.6. Coordinate with AFOSI and SF to identify training requirements and develop an appropriate external FP intelligence awareness program for SF personnel (similar to traditional aircrew external training programs). External training programs should address the following:

3.3.2.6.1. Terrorist TTPs, operational capabilities, intentions and developing potential courses of action (COAs)

3.3.2.6.2. Current terrorism threat

3.3.2.6.3. Terrorism threat levels

3.3.2.6.4. Postulated threat to nuclear weapons facilities (as appropriate) and nonnuclear threat to USAF installations, personnel, and resources

3.3.2.6.5. Man-portable air defenses (MANPADS), rocket propelled grenades (RPGs), mortars and small arms threats, tactics and mitigation measures

3.3.2.6.6. Locating sources of FP intelligence

RONALD E. KEYS, Lt Gen, USAF
DCS/Air and Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 2000.12, *DoD Antiterrorism/Force Protection (AT/FP) Program*

DoDI 2000.16, *DoD Antiterrorism Standards*

AFMND 39, *Air Force Office of Special Investigations*

AFPD 10-2, *Readiness*

AFPD 14-1, *Intelligence Applications and Requirements Planning*

AFPD 14-3, *Control, Protection and Dissemination of Intelligence Information*

AFPD 71-1, *Criminal Investigations and Counterintelligence*

AFI 10-245, *Air Force Antiterrorism (AT) Standards*

AFI 14-105, *Unit Intelligence Mission and Responsibilities*

AFI 71-101 Vol. 4, *Counterintelligence*

CSAF message (DTG 060928Z Feb 01), *Policy Guidance for Intelligence Support to Antiterrorism/Force Protection*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AOI—Area of Interest

AOR—Area of Responsibility

ARC—Air Reserve Component

AT—Antiterrorism

CE—Civil Engineering

CI—Counterintelligence

COA—Course of Action

CONOPS—Concept of Operations

DHS—Defense HUMINT Service

DoD—Department of Defense

DoS—Department of State

DTRA—Defense Threat Reduction Agency

EEI—Essential Elements of Information

FBI—Federal Bureau of Investigation

FP—Force Protection

FPWG—Force Protection Working Group

G—Gamma

GCC—Geographic Combatant Commander

HAF—Headquarters Air Force

HCS—HUMINT Control System

HHQ—Higher Headquarters

HUMINT—Human Intelligence

IAW—In Accordance With

IMA—Individual Mobilization Augmentee

IMSC—Intelligence Master Skills Course

IN—Intelligence

IPB—Intelligence Preparation of the Battlespace

IQT—Initial Qualification Training

JAC—Joint Analysis Center

JIC—Joint Intelligence Center

LE—Law Enforcement

LES—Law Enforcement Sensitive

MAJCOM—Major Command

MANPAD—Man-portable Air Defense System

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

MQT—Mission Qualification Training

MWR—Morale, Welfare and Recreation

NCO—Non-Commissioned Officer

NRT—Near-Real-Time

OI—Operating Instruction

OPREP—Operations Report

OSS—Operations Support Squadron

PDO—Publishing Distribution Office

PIR—Priority Intelligence Requirement

POC—Point of Contact

PR—Production Requirement

RPG—Rocket Propelled Grenade

RSO—Regional Security Office

SC—Systems Communications and Information

SCI—Sensitive Compartmented Information

SF—Security Forces

SG—Surgeon General

SIO—Senior Intelligence Officer

SSO—Special Security Office

TACC—Tanker Airlift Control Center

TS—Top Secret

TTP—Tactics, Techniques and Procedures

TWG—Threat Working Group

UMD—Unit Manning Document

USDAO—US Defense Attaché Office

VAT—Vulnerability Assessment Team

Terms

Information—Data pertaining to any number of sources including CI, foreign intelligence, medical, engineering, security, local law LE, host nation, etc. Threat information specifically refers to information about the adversary derived from CI, LE and intelligence sources.

LE Information—Information provided by any agency chartered and empowered to enforce laws in the US; a state or political subdivision of the US; a territory, possession or political subdivision of the US; or within the borders of a host nation. Law Enforcement Sensitive (LES) information specifically refers to unclassified FOR OFFICIAL USE ONLY information that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence and the integrity of pretrial investigative reports.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities. CI specifically refers to information about the adversary gathered through activities conducted by the AFOSI or other service and national CI organizations.

AFOSI—Responsible for providing counterintelligence, force protection, and antiterrorism services. It is the only Air Force organization authorized to initiate and conduct counterintelligence investigations, operations, collections, and other related activities. It maintains liaisons and is the Air Force single point of contact with federal, state, local and foreign national law enforcement, counterintelligence and security

agencies for matters falling within the AFOSI mission. It is also the sole repository for the collection and retention of reportable information IAW AFI 71-101 V4, Counterintelligence.

Intelligence—Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including CI (except for information on international terrorist activities). Intelligence collects and analyzes information in order to forewarn decision makers, commanders and operators (aircrews, security forces, etc) before an act occurs.

Unit—A unit is defined as squadron level and/or above.