

**BY ORDER OF THE COMMANDER,
PACIFIC AIR FORCES**



AIR FORCE INSTRUCTION 14-119

PACIFIC AIR FORCES COMMAND

Supplement 1

8 APRIL 2005

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: PACAF/INXU (MSgt Rosario Aiello)

Certified by: HQ PACAF/INX
(Col Martha K. Jordan)

Pages: 7

Distribution: F

This instruction supplements AFI 14-119, 6 January 2004. This is the initial publication of this supplement and it applies to all PACIFIC AIR FORCES (PACAF) units and members. It applies to PACAF-gained National Guard Bureau (NGB) and Air Force Reserve Command (AFRC) units and members. Requests for waivers to this supplement will be forwarded to HQ PACAF/INXU and must identify the specific requirements to be waived and include justification. If approved, a waiver stays in effect for the life of the publication unless HQ PACAF/IN specifies a shorter period of time, cancels it in writing, or issues a change to the waiver. Maintain and dispose of records created as a result of prescribed processes in accordance with the approved Air Force retention and disposition schedule. Contact supporting records managers as required. Send comments and suggested improvements to this supplement on AF Information Management Tool (IMT) 847, **Recommendation for Change of Publication**, through channels to PACAF IN/INXU, 25 E. Street Suite J-205 Hickam AFB HI 98653.

AFI 14-119, 6 January 2004, is supplemented as follows:

2.1.2.1.1. (Added) The Senior Intelligence Officer (SIO) will designate an intelligence professional(s) in writing (minimum 14N3 officer, 1N051 or civilian equivalent) to provide intelligence support to FP. Access must be validated by cognizant Special Security Office (SSO) prior to FP training and support. HQ PACAF/INXU will coordinate formal training to ensure all intelligence professionals performing FP functions receive, Level II AT training at USAF approved Schools IAW AFI 10-245.

2.3.1.7.1. (Added) NAF IN's main purpose in the FP forum will be to provide, as required, intelligence support and general oversight to the FP efforts resident at subordinate wings.

3.1.1. (Added) PACAF units will submit requirements IAW AFI 14-105/PACAFSUP1.

3.2.3.1.1. (Added) In conjunction with the TWG, provide the commander recommended courses of action to mitigate the threat IAW AFI 10-245.

3.2.3.2.1. (Added) PACAF units will brief FP requirements IAW AFI 14-10/PACAFSUP1.

3.2.3.4.1.1. (Added) PACAF units will assign as a minimum one 14N3 officer or 1N051 NCO or civilian equivalent. Place the appointment letter in the AT/FP Continuity book, forward a copy to PACAF INXU.

3.2.3.4.3. (Added) The SIO will not be assigned as the wing's Anti-terrorism Officer.

3.2.6.1. (Added) Forward lessons learned to HQ PACAF IN/INXU and PACAF AIS/INA for action (as required).

3.2.7.1. (Added) All procedures will include support to transient units who previously coordinated current and anticipated intelligence requirements as outlined in AFI 14-105, paragraph 3.5.

3.2.8.1. (Added) Forward requirements to HQ PACAF/INXU and PACAF AIS/INA accordingly.

3.2.10.1. (Added) In Coordination with the Force Protection Working Group participates in installation Vulnerability Assessments as required.

3.2.11.1. (Added) Keep a copy of the minutes and a list of attendees for each meeting of the Threat Working Group (TWG) in the Force Protection Continuity Book for a minimum of 90 days.

3.3.2.2.1. (Added) Track all IQT, MQT, and CT requirements on the AF Form 797. Ensure the internal intelligence training program addresses Force Protection issues relevant to unit operations (this includes squadron intelligence personnel) during each training cycle. In addition to requirements outlined below in paragraphs 3.3.2.5.1 thru 3.3.2.5.8, make sure training includes:

3.3.2.2.1.1. (Added) Analytical focus on FP message traffic.

3.3.2.2.1.2. (Added) FP responsibilities at deployed locations.

3.3.2.3.1. (Added) Units will coordinate with PACAF/INXU Formal Training Manager to identify personnel designated to perform FP duties and arrange formal training en route when ever possible. ANG and AFRC units will coordinate FP training through their appropriate Formal Training channels.

3.3.2.7. (Added) Create an appropriate external training program to conduct training, at least annually, on FP issues relevant to unit operations (this includes SF and OSI and should be tracked by their training personnel). Document procedures, responsibilities and guidelines in a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) between AFOSI, Intel, and SF. At a minimum, ensure training includes requirements outlined above in paragraphs 3.3.2.6.1 thru 3.3.2.6.6. Establish procedures for conducting, documenting, testing, evaluating, and monitoring external intelligence training and ensure they are in place.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

(<http://www.e-publishing.af.mil/pubfiles/af/10/afi10-245/afi10-245.pdf>)

AFI 14-105PACAF SUP 1 *Unit Intelligence Mission and Responsibilities*

(http://www.e-publishing.af.mil/pubfiles/pacaf/14/afi14-105_pacafsup1/afi14-05_pacafsup1.pdf)

Attachment 2 (Added)**INTELLIGENCE SUPPORT TO FORCE PROTECTION****A2.1. (Added) Example Intelligence Support to Force Protection Checklists:****Table A2.1. (Added) In Garrison Checklist.**

Step	Process
1	Provide significant force protection intelligence to OSI and SFS.
2	Participate in all FP meetings, Threat Working Groups, and Base Defense Operations Center (BDOC) meetings (real world or exercise).
3	Conduct internal intelligence training on a semi-annual basis or as needed to Force Pro issues relevant to unit operations (this includes squadron intelligence personnel) to include: <ul style="list-style-type: none"> - Analytical focus on FP message traffic. - Online sites or homepages containing FP data. - Deployed FP responsibilities.
4	Coordinate with OSI and SF counterparts to identify FP training requirements and forward requirements to PACAF/INX.
5	Conduct annual external intelligence training on Force Protection. Coordinate with AFOSI and SF to identify training requirements and issues relevant to unit operations (this includes SF and OSI and should be tracked by their training personnel).
6	Maintain FP binder on FP, terrorist, and host nation threat data for in garrison and programmed deployment bases. Include: <ul style="list-style-type: none"> - Mood of local/indigenous population as reported by AFOSI. - Known/identified terrorist groups. - Historical incidents/targeting. - AFOSI assessments on local criminal elements. - Country restrictions. - FPCON levels. - In-place procedures.
7	Disseminate FP info: <ul style="list-style-type: none"> - Read Files/Web page. - Include FP issues in CIB regularly or at least quarterly.
8	Participate and add intelligence value to installation vulnerability assessments during FWGs.

Table A2.2. (Added) Exercise Checklist.

Step	Process
	In addition to in-garrison, pre-deployment, employment/sustainment, and redeployment actions the following actions need to be accomplished for local and major exercises:
1	Coordinate AT/FP threat scenarios with the TWG for realism during exercises.
2	Document FP lessons learned for inclusion into lessons learned databases.

Table A2.3. (Added) Pre-Deployment Checklist.

Step	Process
1	Once unit is identified for possible deployment; monitor world events if not already being done.
2	If its a short-notice deployment, contact the local AFOSI detachment: - Inform them of possible deployment location and obtain latest threat information.
3	Once deployment location identified, check files for issues and threats to the deployed location(s): - Submit RFIs /PRs as needed to the NAF. - Identify pre-deployment FP requirements to NAF or HQ PACAF/INXU.
4	Coordinate with TWG to provide commanders with overall assessment.
5	Ensure all relevant FP information is included in unit deployment briefing and/or chalk briefing provided by INO.

Table A2.4. (Added) Employment/Sustainment Checklist.

Step	Process
1	Contact onsite SFS and OSI. <ul style="list-style-type: none"> - Establish Force Protection Cell. - Establish the Threat Working Group Schedule. - Establish intelligence support requirements (maps, charts).
2	Create and maintain local read files (at appropriate classification levels).
3	Ensure SIPRNET and JWICS connectivity are established.
4	Coordinate with local intelligence agencies, to include: <ul style="list-style-type: none"> - US Embassy (OSI coordination). - Host nation security (OSI Coordination). - Other US Service organizations (USN, USA, USMC). - Other Coalition/Multi-National Organizations as required.
5	Ensure intelligence provides FP intelligence to SFS and OSI in a timely manner.
6	Contact theater J2/JISE: <ul style="list-style-type: none"> - Coordinate all FP-related PRs through the J2/JISE or home station if necessary. - Contact J2/JISE minimum three times a week for relevant reports - and information. - Work imagery requests through JTF J2/JISE. - J2/JISE should continue to provide data to the FP cell.
7	Coordinate all FP requirements with the TWG and submit PRs as needed.
8	Check with local OSI for additional information and reporting.
9	Ensure deployed unit is receiving FP-related traffic and updates.
10	Coordinate with local intelligence personnel to ensure: <ul style="list-style-type: none"> - Read files are updated. - Message traffic includes FP intelligence. - Updates on local anti-terrorism restrictions and security measures are provided. - FP issues are included in Current Intelligence Briefing. - SIO is kept abreast of all "hot" issues and back brief on breaking issues.

Table A2.5. (Added) Redeployment Checklist.

Step	Process
1	With the FP Cell, coordinate with senior leadership as to exactly when operations and coverage will cease.
2	FP Cell must continue receiving intel support until all personnel have departed deployed location: - OSI is still able to obtain information from their sources.
3	Pack classified materials.
4	Pack systems and computers.
5	Prepare for departure.

MARK E. KIPPHUT, Colonel, USAF
Director of Intelligence