

**BY ORDER OF THE COMMANDER
FAIRCHILD AIR FORCE BASE (AMC)**

**FAIRCHILD AIR FORCE BASE
MANUAL**



31-105

7 JUNE 2021

Security

INFORMATION FUSION CELL (IFC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: Access to this publication is restricted; this publication may be released to Department of Defense (DoD) personnel only; requests for accessibility outside of the DoD must be approved by the OPR

OPR: 92 SFS/S2

Certified by: 92 ARW/DFC
(Maj. Brian S. Slater)

Supersedes: FAFBMAN31-105,
3 December 18

Pages: 13

FAIRCHILD AFBMAN31-105 is directive in nature and failure to adhere to the standards set out in this manual may form the basis for adverse action under the Uniform Code of Military Justice (UCMJ) and AFI 36-704, *Discipline and Adverse Actions*. An example would be a dereliction of duty offense under Article 92. As used in this manual, “Shall” or “Will” or an action verb in the imperative sense means a procedure is mandatory. “Should” means a recommended procedure. “May” means an optional procedure. To the extent its directions are inconsistent with other FAFB manuals, the information herein prevails. Units tasked by this manual must initiate procedures to support any procedural changes. There are prohibited practices and specific requirements throughout this manual. Violations of the specific prohibitions and requirements of this manual by military personnel may result in prosecution under the Uniform Code of Military Justice (UCMJ). Violations of this manual by Air Force civilian employees may result in appropriate disciplinary action without regard to criminal liability. Administrative action, such as a reprimand, may be taken with regard to military members and civilian employees who violate any requirements of this manual even if such violations do not constitute criminal misconduct. This manual applies to all personnel assigned to Fairchild AFB, both military and civilian, guard and reserve, as well as transient or TDY personnel.

The Fairchild Air Force Base (AFB) Information Fusion Cell (IFC) Manual is being published by the Defense Force Commander in accordance with the requirements of the 92 ARW Integrated Defense Plan 31-1. This manual provides information and "how-to-guidance" for establishing and maintaining an effective IFC on Fairchild AFB. In addition, it provides helpful information on "best business practices" and "lessons learned." This manual applies to active duty AF military; Air National Guard (ANG); AF Reserve Command (AFRC); AF civilian employees; and all DoD contractors as prescribed in AFI 16-1406, *Industrial Security Program* when contract performance depends on access to AF information.

This manual promulgates requirements contained in DoDIO-2000.16V1_AFI10-245-O *Antiterrorism (AT) Program Implementation* and AFI 31-101, *Integrated Defense*. To the extent there is a disagreement between this manual and any HHQs directives, the HHQs directives will prevail.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force (AF) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. This manual requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by 5 USC 552a. Systems of records notice F024 AF IL C applies. Ensure all records created by this manual containing For Official Use Only (FOUO) information, including privacy records, are marked IAW Department of Defense Manual (DoDM) 5200.01-V1, Information Security Program, and AFI 33-332, *Air Force Privacy and Civil Liberties Program*. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

1. ROLES AND RESPONSIBILITIES.

1.1. **Purpose.** This Manual establishes the 92 ARW IFC chartered by the 92 ARW/CC in the 92 ARW Integrated Defense Plan (IDP) as a tactical-level action team that functions in tandem with the DFC's (92 SFS/CC) operations staff in the planning and execution of ID.

1.2. **Authority.** The "Commanders Intent" is to Operationalize Force Protection Intelligence (FPI) in order to maintain optimal situational awareness throughout the Base Boundary (BB) and Base Security Zone (BSZ). The Information Fusion Cell (IFC) and its products are the primary information source that directly support the DFC in meeting this intent.

1.3. **Goal.** To leverage information and intelligence to support the timely identification of indicators and warnings of localized threats and provide products that directly support the Defense Forces Commander in Integrated Defense planning.

1.4. **Objectives.** The IFC and its products will be the primary information sources that directly support the DFC (and ultimately the 92 ARW/CC) in making immediate, proactive decisions for ID planning.

1.5. **Scope.** The IFC will generally limit the scope of its proceedings to the area of Fairchild AFB within the Base Boundary (BB) and the Base Security Zone (BSZ), including local crime trends in an effort to focus on identifying a broad spectrum of potential threats to FAFB personnel and assets.

1.6. **Management Structure.** IAW, AFI 31-101, the IFC is an action group whereby the Security Forces (S2) coordinates with subject matter experts (SMEs) from the Intelligence and OSI communities to identify emerging local threats. The IFC is chaired by the 92 SFS/CC (or designee) and facilitated by SFS Investigations (S2). FAFB membership consists of: SFS Reports and Analysis—92 SFS/S5R, Antiterrorism Program Manager (92 SFS/S5X), Office of Special Investigations (OSI Detachment 322), 92 OSS/IN, and advisory SMEs, as needed. Consider the following advisory members: Police Services (92 SFS/S3L), Information Protection—92 ARW/IP, Communications (Cyber)—92 CS, Medical Liaison—92 MDG, and Force Support (Personnel)—92 FSS).

1.7. **Administration.** The IFC will meet when actionable intelligence is received and more frequently as needed. All written documentation related to the meetings will be kept by the Facilitator to protect the overall classification and sensitivity of information discussed.

2. Information Fusion Cell Products.

2.1. **Classification.** The overall classification of the IFC products will be determined based on the highest classification of the information contained. The minimum classification of “For Official Use Only (FOUO)” is required for all IFC products. In some cases, the information may be Law Enforcement Sensitive (LES) so it is important that the IFC member presenting the details clarify the specific markings for each paragraph.

2.2. **All-Source Information.** S2 provides current information to the DFC’s Operations Staff on criminal trends and potential threats affecting the installation ID operations.

2.2.1. S2 will monitor and gather local crime trends obtained from Security Forces Blotters, Police Reports and Investigations.

2.2.2. S2 acts as the SF liaison to the installation’s intelligence and counterintelligence organizations/providers (92 OSS/IN and OSI) and will coordinate with them as applicable.

2.2.3. S2 will monitor crime trends from local state and federal law enforcement agencies for potential threat information.

2.2.4. S2 will monitor data entered into e-Guardian, the SF approved information system for record, and ensures criminal intelligence and LE information is incorporated into the threat analysis process.

2.3. **Dissemination.** The IFC will gather, analyze and provide a quarterly IFC product to the DFC’s Operations Staff enabling timely, predictive, proactive decisions or adjustments to the ID scheme, if applicable. Any emerging or time-sensitive criminal or threat information received by the IFC will be immediately disseminated to the DFC’s Operations Staff to act or respond to real-time information.

CASSIUS T. BENTLEY III, Colonel, USA
Commander, 92d Air Refueling Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References: If not listed below, see Air Force e-Publishing Site at: <http://www.e-publishing.af.mil/>

AFI 10-245, *Antiterrorism*
 AFI 14-104, *Intelligence Oversight*
 AFI 16-1406, *Industrial Security Program*
 AFI 31-101, *Integrated Defense*
 AFI 31-115, *Law and Order Operations*
 AFI 31-118, *Security Forces Standards and Procedures*
 AFI 33-332, *Air Force Privacy and Civil Liberties Program*
 AFI 36-704, *Discipline and Adverse Actions*
 AFI 71-101V1, *Criminal Investigations Program*
 AFMAN 31-101v1, *Integrated Defense Planning*
 AFMAN 33-363, *Management of Records*
 AFTTP 3-10.3, *Integrated Base Defense Command and Control*
 (DoDD) 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*
 DoDI 2000.12, *DoD Antiterrorism (AT) Program*
 DoDI 5200.08, *Physical Security Program*
 DoDM 5200.01-V1, *Information Security Program*
 50 USC § 797, *Penalty for Violation of Security Regulations and Orders*
 18 USC § 795, *Prohibits Photographing and Sketching Defense Installations*

Explanation of Terms: *If not listed below, see Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010 (As Amended through 15 Jun 2014). The Dictionary is available for browsing, searching, or can be downloaded at:*
http://www.dtic.mil/doctrine/dod_dictionary

Abbreviations and Acronyms: *If not listed below, see Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 Nov 2010 (As Amended through 15 Jun 2014). The Dictionary is available for browsing, searching, or can be downloaded at:*
http://www.dtic.mil/doctrine/dod_dictionary

AF—Air Force

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFP—Air Force Pamphlet

AFPD—Air Force Policy Directive

AFRC—AF Reserve Command

AFVA—Air Force Visual Aid

AMC—Air Mobility Command

ANG—Air National Guard
AO—Action Officers
AT—Antiterrorism
ATO—Antiterrorism Officer
BB—Base Boundary
BSZ—Base Security Zone
CI—Confidential Informants
COA—Course of Action
CPTED—Crime Prevention through Environmental Design
DCIP—Defense Critical Asset Infrastructure Program
DFC—Defense Force Commander
DOD—Department of Defense
DODD—DOD Directive
DODH—DOD Handbook
DODI—DOD Instruction
DODM—DOD Manual
EI—Essential Elements of Information
FAFB—Fairchild Air Force Base
FOUO—For Official Use Only
FP—Force Protection
FPI—Force Protection Intelligence
ID—Integrated Defense
IDP—Integrated Defense Plan
IFC—Intelligence Fusion Cell
IPB—Intelligence Preparation of the Battlefield/Battlespace
IPOE—Intelligence Preparation of the Operational Environment
IR—Information Requirements
ISR—Intelligence, Surveillance, and Reconnaissance
ISTAR—Information, Surveillance, Target Acquisition, and Reconnaissance
JTTF—Joint Terrorism Task Forces
LES—Law Enforcement Sensitive
LIMFAC—Limiting Factor

MANPADS—Man-Portable Air Defense System

NAI—Named Area of Interest

OB—Order of Battle

OPR—Office of Primary Responsibility

OPR—Office of Concurrent Responsibility

OSI—Office of Special Investigations

PIR—Priority Intelligence Requirement

RDS—Records Disposition Schedule

SAIC—Special Agent in Charge

SECDEF—Secretary of Defense

SF—Security Forces

SFMIS—Security Forces Management Information System

SIO—Senior Intelligence Officer

SIR—Specific Intelligence Requirement

SME—Subject Matter Experts

SOR—Specific Orders and Requests

TTP—Tactics, Techniques and Procedures

TWG—Threat Working Group

UCMJ—Uniform Code of Military Justice

WG—Working Group

Forms or IMTs Prescribed: If not listed below, see Air Force e—Publishing Site at:
<http://www.e-publishing.af.mil/>

Attachment 2

DEFENSE FORCE COMMANDER'S INFORMATION REQUIREMENTS

Figure A2.1. Defense Force Commander's Information Requirements.

Are threat groups targeting DoD forces, facilities, equipment or activities in the FAFB or surrounding area?

Is surveillance being conducted against US forces, facilities, equipment or activities?

- Report any attempts to record information on US forces, facilities, or activities.
- Report use of photographic equipment by unauthorized or unknown persons.
- Report any suspected unauthorized or unknown persons using note-taking material, maps or diagrams to record information on US forces, facilities or activities.
- Report the use of binoculars or other vision-enhancing devices by unauthorized or unknown persons.

Are threat groups eliciting security-related information regarding US forces, facilities or activities?

- Report any attempts to elicit security-related information regarding US forces, facilities or activities by any unauthorized persons.

Are tests of the security of US forces, facilities, equipment or activities being conducted?

- Report any actual or suspected attempts to measure security reaction times or strengths.
- Report any actual or suspected attempts to test or penetrate security barriers or procedures.
- Report any actual or suspected attempts to acquire or duplicate uniforms, badges, passes, or other security-related documents.
- Report any unauthorized access or attempts to access US facilities.

Are pre-incident rehearsals being conducted against US forces, facilities, equipment or activities?

- Report any suspicious activity that could be pre-incident preparation for an attack.

Are repetitive activities occurring in the vicinity of US forces, facilities, equipment, or activities?

- Report any repetitive activity by the same person or vehicle in the vicinity of US forces, facilities, equipment or activity.

Have threat groups initiated direct threats against US forces, facilities, equipment or activities?

- Report any threats which contain a specific time, location or area for an attack against US forces, facilities, equipment or activity.

- Report any event or incident, or series of events or incidents that may indicate the potential of a threat to US forces, facilities, equipment or activities, whether the threat posed is deliberately targeted or collateral.

Are threat groups conducting new or on-going training efforts on tactics or operations that could be used against US forces, facilities, equipment or activities?

Are threat groups moving equipment or personnel to support an attack on US forces, facilities, equipment or activities?

Have threat groups released media statements intended to incite emotional responses or influence action against US forces, facilities, equipment or activities?

Have threat groups communicated generic or non-specific threats or warnings against US interests in the AOR?

Has any specific event or series of events occurred that may prompt or trigger an anti-US response from any group?

Has a change of attitude in a given area reflecting anti-US feelings or behavior among the masses and/or specific segments of the population occurred?

What local areas pose a risk to FAFB members in the local community?

Is anti-military sentiment present in the area?

- Report anti-military propaganda found or available in the area.

- Report any criminal activity against US personnel in the area.

- Report any anti-US graffiti found in the area.

- Report harassment or suspicious activity aimed at US personnel.

Is there support for terrorist activities or groups, or allegiance to state-sponsors or terrorism?

- Report pro-terrorist propaganda present in the area.

What are the demographics of the area?

- Report any religious sect concentrations in the area.

- Report any identifiable ethnic concentrations in the area.

- What weapons are found or available in the area?

- Report the existence of automatic, suppressed, or illegal weapons in the area.
- Report the use of weapons in conjunction with any criminal activity.

What explosives are found in the area?

- Report the existence of any explosives or explosive projectiles in the area.

Are threat groups attempting to affect local populace?

What general activities are being conducted by threat groups in the AO/AI?

- Report any unusual gatherings among the local population.
- Report any disruption of normal social patterns.
- Report the establishment of any organizations of unexplained origin and of unclear or nebulous aims.
- Report the establishment of a new organization to replace an existing organizational structure with identical aims.
- Report the appearance of any new members in established organizations.
- Report the appearance of new organizations with titles stressing radical religious beliefs.
- Report large monetary donations to new or revamped organizations.
- Report lists of targets for planned terrorist acts.
- Report evidence of participation of paid and armed demonstrators.

Are threat groups promoting activities in the AO?

- Report trends of demonstrated hostility on the part of the local populace toward host nation, coalition and/or US forces.
- Report occurrence of actions previously considered taboo by local populace.
- Report disappearance of local population from or avoidance of certain areas.
- Reported incidents of attempted recruitment of people to join new movements or underground organizations.

- Report increased unrest and agitation among base employees.
- Report any attempts to obtain classified information from local officials or documents from local government offices.
- Report any leakage of classified information to news media.
- Report any sudden improvement in financial status of local government or police officials.
- Report any failure of government raids on suspected subversive meetings because of forewarning.
- Report any demonstrations against current government.
- Report any articles or advertisements in newspapers criticizing the government.
- Report any unusual and unsatisfactorily explained absences of base employees from their job.
- Report any sporadic, unexplained destruction, loss, or forgery of government identification cards.

Attachment 3

USER FEEDBACK

A3.1. Users in the field are highly encouraged to submit comments on any DoD or AF level publication using AF Form 847, *Recommendation for Change of Publication*. Users may submit comments concerning any Fairchild AFB and Security Forces Publication including this document by using the template in this attachment and sending it to 92 SFS/S5X.

Figure A3.1. USER FEEDBACK.

NOTE: Add any additional information on bond paper and include with this attachment. Please provide the following information as a minimum:

1.1. Full Name (Rank/First/Last):

1.2. Unit:

1.3. Address:

1.4. Phone (DSN or Commercial):

2. CONTENT:

2.1. Is the information provided accurate? If not, what needs to be updated?

2.2. Is this publication consistent with other AF documents?

2.3. Can this instruction be better organized for better understanding of the material presented?

2.4. Is the information provided useful? If not, how can we improve it?

3. Writing and Appearance.

3.1. Where does the publication need revision to make the writing more clear and concise? What words would you use?

3.2. Are the charts and figures clear and understandable? How would you revise them?

4. Recommended Urgent Change(s), if any:

5. Other Comments:

6. Send Responses to:

92 SFS/S5X (Plans)
2 East Arnold Street

Fairchild AFB, WA. 99011