

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



AIR FORCE INSTRUCTION 31-203

PACIFIC AIR FORCES COMMAND

Supplement 1

11 JUNE 2004

Security

**SECURITY FORCES MANAGEMENT
INFORMATION SYSTEM (SFMIS)**

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 PACAF/SFOP (Bernard V. Mann)

Certified by: HQ PACAF/SFO
(Maj Joshua D. Fowler)

Pages: 3

Distribution: F

This publication supplements AFI 31-203, *Security Forces Management Information System*, and provides additional and command-unique requirements. This publication does not apply to the Air National Guard (ANG) or Air Force Reserve Command (AFRC) units.

AFI 31-203, 15 August 2001, is supplemented as follows:

1.2.2. Chiefs of Security Forces (CSFs) are required to establish procedures for inputting incident, accident, and ticket information. Procedures must ensure Defense Incident-Based Reporting System (DIBRS) reportable information is inputted accurately. CSFs will establish unit procedures for ensuring information is transferred from blotters to SFMIS when an AF Form 3545 is not accomplished, but is reportable in DIBRS. CSFs will ensure procedures are in-place for entering information gained during investigations that must be reported in DIBRS. CSFs will establish training requirements for SFMIS users and SFMIS administrators will ensure all personnel receive training prior to being allowed access.

1.2.5. At a minimum, each installation will conduct a review of all reports containing Defense Incident-Based Reporting System (DIBRS) and National Incident-Based Reporting System (NIBRS) to ensure proper compliance at least monthly. Errors should be corrected as soon as possible, and the System Administrator (SA) will forward all issues to the SFMIS Field Assistance Branch (FAB) at DSN 596-5771 or COMM: (334) 416-5771 if errors cannot be corrected immediately.

1.2.6.1. The Security Forces Operations Policy Branch (PACAF/SFOP) is responsible for policy, resource advocacy, and oversight of this program for Pacific Air Forces. All SFMIS users are required to complete web-based training and forward a signed letter from the SFMIS administrator on each individual within 30 days of gaining access to SFMIS. Training from the FAB will be distributed to the units when available, but is not sufficient to train all individuals requiring access. CSFs will establish unit training requirements for SFMIS users. Systems Administrators are required to document the training and to have it available in the work centers.

1.2.7.1. CSF will appoint a primary and alternate System Administrator (SA) and forward a SFMIS appointment letter to PACAF/SFOP. The SA at each PACAF installation will also serve as the single focal point for all installation SFMIS issues. Units are responsible for maintaining a current list of SFMIS users and the modules to which they are authorized. This list must be forwarded to PACAF/SFOP.

1.2.7.2. As a minimum, the SA will develop an operating instruction that includes guidelines and procedures for proper implementation, management, training, and access control of the SFMIS program. The overall objective is to ensure integrity of the system and protection of personal data information.

1.2.7.5. (Added) . CSFs will determine policy for maintaining on-hand program manuals and the frequency of downloading the manual to ensure most current information is used. Questions can be addressed to the FAB and sent to PACAF/SFOP for inclusion with command correspondence to AFSFC and the FAB. SAs will forward concerns and inputs to PACAF/SFOP for inclusion in command communications with the AFSFC and FAB offices. Day to day questions may be addressed directly to the FAB for timely resolution.

3.1. Units will consider SFMIS requirements when replacing computers within the unit. CSFs should establish procedures to ensure future expenses to continue modernization of the system are reflected in the annual budgets.

3.2.3. As technology advances, the CSF and the SA will comply with minimum SFMIS system hardware and software standards. SAs will also develop a SFMIS life-cycle-system plan and annual budget to accommodate future upgrades and enhancements.

3.2.4. Units will use all modules and are required to develop a plan to fully integrate these modules into daily operations. EXCEPTIONS: The issue and turn-in function is not required to be integrated until units receive card readers and scanners to expedite issue and turn-in.

3.2.4.1. (Added) . Units in Korea are not required to use SFMIS for registration of visitors or vehicles due to mandated Biometric Identification System requirements.

3.2.4.2. (Added) . All deviations to the use of SFMIS must be submitted in memorandum format through PACAF/SF, who will coordinate them with AFSFC for final approval.

3.2.4.3. (Added) . Utilization of Commercial-Off-The-Shelf (COTS) information management systems is not authorized without PACAF/SF approval. Units will coordinate all issues involving procurement of any COTS information management systems with PACAF/SF prior to purchase of COT software and hardware. The requirements in AFI 31-101 for production of Automated Entry Card Systems are applicable, and MAJCOM approval will be coordinated prior to purchase and implementation.

3.3.2. SAs are responsible for development of lockout procedures and necessary actions to assign new passwords for all SFMIS users.

3.3.3. SAs will monitor, manage, and develop procedures to immediately report known violations of the system operation or unauthorized dissemination of "For Official Use Only" (FOUO) information. Completed reports will be forwarded by the violator's unit commander to PACAF/SFOP no later than 15 duty days from the date of occurrence.

3.3.4. SAs will be the focal point in coordinating with all base functions that may require access to SFMIS information.

ALBERT F. RIGGLE, Colonel, USAF
Director of Security Forces