



SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS)

The basic publication has changed; however, the only revisions required in this supplement were made in the date line, leadline, supersession line, and approving authority.

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AETC Publishing WWW site at: <http://www.aetc.randolph.af.mil/im>. If you lack access, contact your base publishing manager.

OPR: HQ AETC/SFI (J. W. Helfenstein)
Supersedes AFI 31-203/AETC Sup 1, 16 July 2001

Certified by: HQ AETC/SFI (B. L. Kilgore)
Pages: 2
Distribution: F

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

This publication does not apply to Air National Guard and Air Force Reserve Command units. This publication requires collecting and maintaining information protected by the Privacy Act of 1974. System of Records Notice F031 AF SF B applies. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule*.

1.2.4. The noncommissioned officer in charge of confinement will ensure all information related to the confinement module of SFMIS is in compliance with Defense Incident-Based Reporting System (DIBRS) and National Incident-Based Reporting System (NIBRS) requirements.

1.2.5. Security forces will use the SFMIS to report DIBRS information. Reports and analysis personnel will review all SFMIS data inputs for DIBRS and NIBRS compliance and correct them, if necessary, by the 10th day of the next month. Reports and analysis personnel will go through the systems administrator (SA) when DIBRS and NIBRS errors cannot be resolved at their level.

1.2.7. Security forces commanders will determine in local operating instructions whether operations (flight level) or reports and analysis functions will be responsible for the initial input of incident, accident, and ticket information. They will also establish a process to ensure information is accurately input into the SFMIS.

1.2.7.1. The security forces commander shall appoint, in writing, a primary SA and as many alternate SAs as necessary to meet mission needs. Provide an initial primary and alternate SA designation memorandum to HQ AETC/SFI and updated memorandums as names are changed.

- 3.2.1. As technology advances, SAs need to be familiar with SFMIS upgrades of system hardware and software. Security forces squadrons will comply with the minimum hardware and software upgrades. The training and resources flight (SFT) is responsible for identifying cost factors for hardware and software upgrades and ensuring those costs are reflected in the security forces annual budget plan.
- 3.3.3. Submit a written report describing violations of the Privacy Act involving unauthorized dissemination of "for official use only" (FOUO) information to HQ AETC/SFI no later than 5 workdays from date of occurrence.
- 4.2. See paragraph 3.3.3, as supplemented, for procedures on reporting violations of the Privacy Act.
- 4.3. SAs will establish an account with the HQ SSG field assistance branch (FAB). SAs will:
- 4.3.1. (Added)(AETC) Contact the FAB for assistance with SFMIS-related problems.
- 4.3.2. (Added)(AETC) Maintain an SFMIS continuity book, to include a log of all trouble tickets established with the FAB.
- 4.3.3. (Added)(AETC) Establish a log each calendar year and maintain it for 1 year.
- 4.3.4. (Added)(AETC) If adequate assistance is not provided in a timely manner, submit a written report (email permitted) to HQ AETC/SFI explaining the service problems with the FAB.
- 4.5. Send a report of all unresolved SFMIS issues to HQ AETC/SFI, who, in turn, will work those issues through HQ AFSFC/SFOP for resolution.

JOHANN R. KINSEY, Colonel, USAF
Director of Security Forces