

**12 OCTOBER 2004**



**Command Policy**

**SECURITY FORCES MISSION  
PERFORMANCE CHECKLIST –  
SECURITY FORCES MANAGEMENT  
INFORMATION SYSTEM (SFMIS)**

---

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

---

OPR: HQ PACAF/SFO (Lt Col Gus M. Green)

Certified by: HQ PACAF/SFO  
(Lt Col Gus M. Green)

Pages: 4

Distribution: F

---

This Directory implements AFD 90-2, *Inspector General – The Inspection System*, and AFI 90-201, *Inspector General Activities*. **Attachment 1** of this directory is a Security Forces Management Information System (SFMIS) Mission Performance Checklist (MPC) and supports guidance in AFI 31-203, *Security Forces Management Information System*, and related PACAF Supplement 1. This publication does not apply to the Air National Guard (ANG) or Air Force Reserve Command (AFRC).

**1. General.** This MPC expands the Common Core Compliance Areas (CCCA) listed in AFI 90-201, Attachment 6, and contains functions essential to mission accomplishment at all levels of a unit. **A pound sign (#) identifies items critical to the proper operation of the functional areas.**

1.1. This checklist was created for use by the PACAF Inspector General to inspect the mission performance of units during Unit Compliance Inspections (UCIs) and is not intended to be the sole source of guidance for program management, but should be used in conjunction with the applicable governing DoD, Air Force, and PACAF instructions, manuals, and other directives.

1.2. This MPC does not constitute the order or limit the scope of the inspection/assessment. As a minimum, units should use this checklist in conjunction with the annual Unit Self Assessment. Units may supplement this publication to add internal compliance items. This checklist may be used in whole or in part by HHQ during visits or exercises.

**2. Responsibilities:**

2.1. Directorate of Security Forces.

2.1.1. Identifies mandatory inspection areas for Unit Compliance Inspections (UCI).

2.1.2. Develops and maintains this directory.

2.1.3. Determines scope and what exercises will be included in UCI.

2.2. Inspector General for Security Forces (IGSF).

- 2.2.1. Conducts Unit Compliance Inspection of mandatory inspection areas as determined by the Directorate of Security Forces.
- 2.2.2. Conducts exercises as determined by the Directorate of Security Forces.
- 2.3. Installation Chief of Security Forces.
  - 2.3.1. Conducts semi-annual self-inspections using these MPCs.
  - 2.3.2. Provides IGSF with the following:
    - 2.3.2.1. Self-inspection reports.
    - 2.3.2.2. Evaluation reports of all exercises.
    - 2.3.2.3. Last 90-days of Security Forces Blotters.
    - 2.3.2.4. Installation Security Plan/Full Spectrum Contingency Plan and Installation Security Instruction.
    - 2.3.2.5. Copies of all checklists, operating instructions, and special security instructions.
    - 2.3.2.6. Room equipped with a telephone, computer, and computer printer.
    - 2.3.2.7. Standardization Evaluation personnel to act as trusted agents during UCI exercises.
    - 2.3.2.8. Any other documents/support specified in the Inspector General transmitted letter of instruction.

MICHAEL F. PASQUIN, Colonel, USAF  
Director of Security Forces

## Attachment 1

**SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS) –  
MISSION PERFORMANCE CHECKLIST**

**Table A1.1. Security Forces Management Information System (SFMIS) – Mission Performance Checklist.**

No.	Item	Reference
<b>1. Does/Has the Security Forces Commander:</b>		
1.1	<b>(#) Appointed a System Administrator (SA) (Primary &amp; Alternate) to act as the grantor of permissions and accesses for personnel requiring access to SFMIS in the performance of official duty?</b>	AFI 31-203, Para 1.2.7.1.
1.2	<b>(#) Ensure all reportable Defense Incident-Based Reporting System (DIBRS) incidents, identified in DoD 7730.47-M, are accomplished using AF Form 3545? NOTE: No deviations are authorized.</b>	AFI 31-203, Para 2.1.4.
1.3	Along with the SA, complied with the minimum SFMIS system hardware and software standards?	AFI 31-203, Para 3.2.3. & PACAF Sup 1, Para 3.2.3.
<b>2. Does/Has the System Administrator:</b>		
2.1	<b>(#) On a monthly basis conduct a review of all reports containing DIBRS and National Incident-Based Reporting System (NIBRS) to ensure proper compliance?</b>	AFI 31-203, Para 1.2.5. & PACAF Sup 1, Para 1.2.5.
2.2	<b>(#) Ensure that all incidents identified under DIBRS reporting criteria are reported through SFMIS?</b>	AFI 31-203, Para 1.2.7.1
2.3	(#) Developed criteria or system to carefully scrutinize personnel access to ensure integrity of the system and protection of For Official Use Only (FOUO) information?	AFI 31-203, Para 1.2.7.2.
2.4	Developed localized procedures and requirements to ensure the sensitivity of the information entered into DIBRS, and the requirement to report data only to those who have a need to know in the performance of official duty?	PACAF Sup1, Para 1.2.7.2.
2.5	<b>(#) Developed a SFMIS life-cycle-system plan and an annual budget to accommodate future upgrades and enhancements?</b>	PACAF Sup 1, Para 3.2.3.
2.6	<b>(#) Develop, monitor, and account for all “Password” security issues and as a minimum, are passwords changed once every 90 days?</b>	AFI 31-203, Para 3.3.1.
2.7	<b>(#) Develop lockout procedures and necessary actions to assign new passwords for all SFMIS users?</b>	AFI 31-203, Para 3.3.2. & PACAF Sup 1, Para 3.3.2.

No.	Item	Reference
2.8	<b>(#) Monitor, manage, and develop procedures to immediately report known violations of the system operation or unauthorized dissemination of the “For Official Use Only” (FOUO) information?</b>	AFI 31-203, Para 3.3.3. & PACAF Sup 1, Para 3.3.3.
2.8.1	<b>(#) Are completed reports forwarded to PACAF/SFOP no later than 15 workdays from the date of occurrence?</b>	
2.9	<b>(#) Manage and coordinate access requirements for all base functions to SFMIS information and are out of the ordinary requests forwarded to HQ PACAF/SFOP?</b>	AFI 31-203, Para 3.3.4. & PACAF Sup 1, Para 3.3.4.
2.10	Ensure all SFMIS users are using the latest Internet Browser? (Netscape or Microsoft Internet Explorer)	AFI 31-203, Para 4.1.
2.11	Established procedures to ensure SFMIS users are aware that data displayed on monitors is always susceptible to unauthorized viewing? And does these procedures include appropriate protection actions?	AFI 31-203, Para 4.2.1.
2.12	Established or installed “time-out” or “screen savers” features when the SFMIS system is not being used?	AFI 31-203, Para 4.2.2.
2.13	Ensure that unit SFMIS users are aware of the availability of on-line SFMIS program manuals? If there are problems with a manual’s content, does the SA up-channel reports through HQ PACAF/SFOP to HQ AFSFC/SFOP for resolution?	AFI 31-203, Para 4.4.
<b>3. Does the Reports and Analysis Section:</b>		
3.1	<b>(#) On the first duty day of each month, perform a computer run of the previous month’s Criminal Summary Report?</b>	AFI 31-203, Para 1.2.7.4.
3.2	<b>(#) Conduct a comparison with the local AFOSI and the Security Forces Investigation section to ensure all pertinent criminal activity falling under AFOSI’s Defense Clearance and Investigation (DCII) reporting criteria is reported?</b>	AFI 31-203, Para 1.2.7.4.
3.3	<b>(#) Ensure all original AF Form 3545s and criminal DD Form 1805s falling within the DCII reporting criteria are transferred to the local AFOSI detachment and are copies properly filed in Reports and Analysis filing system?</b>	AFI 31-203, Para 1.2.7.4.
<b>4. General Compliance Items:</b>		
4.1	Is the capability to monitor and apply law enforcement selective enforcement measures to meet their specific needs and perform data analysis for law enforcement statistics offered to all levels of base management?	AFI 31-203, Para 1.1.2.