



**THE AIR FORCE INSTALLATION SECURITY
PROGRAM**

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: ANG/XOF (CMSgt D. Obetz)

Certified by: ANGRC/CV (Col D. Larrabee)

Pages: 7

Distribution: F

Air Force Instruction (AFI) 31-101, *The Air Force Installation Security Program*, 1 March 2003, is supplemented as follows. Compliance with this instruction is mandatory and applies to all Air National Guard (ANG) military and civilian personnel including contract personnel responsible for its implementation.

1.6. The ANG Security Forces (ANG/XOF) provides MAJCOM guidance and approval for all ANG Security Forces (SF) units.

1.7. The Installation Security Council (ISC) will replace the Base Security Executive Council (BSEC) as the commander's focal point for all installation security matters. The installation commander is considered the full-time individual with overall responsibility for day-to-day operations of the installation/facilities/site.

1.9. At ANG installations the senior full-time security forces representative assigned to the unit is the primary advisor for the installation security program. This position ensures the full-time continuity of the force protection mission. Effective immediately, when the senior full-time security forces representative is an enlisted person his/her title will reflect the proper position they are assigned, for example, Superintendent or Security Forces Manager. When the senior full-time security forces representative is an Officer he/she will hold the proper title of Chief of Security Forces (CSF) or acting CSF when the Squadron Commander is a traditional guardsman.

1.10. The CSF should consider assigning ISS responsibilities as an additional duty to the full time security forces members.

2.8.3.4. During increase FPCONs, commanders should consider the arming of support forces personnel during SF shortages on the base. Personnel, who work in or around PL resources, where the arming would not hinder their primary duties, must be trained in accordance with (IAW) AFI 36-2225, *Security Forces Training and Standardization Evaluation Programs*, Paragraph 1.9.

3.3. ANG units collocated on a DoD or other US Government installations will not publish a separate instruction if security standards have been coordinated and incorporated within the host installation's Installation Security Instruction (ISI).

3.3.2. The installation commander and state or unit legal staff will identify the SF jurisdictional boundaries throughout the installation. Special consideration will be given to restricted and controlled areas concerning federal and state agreements for other than exclusive jurisdiction.

3.6.1. Unit Commanders will appoint primary and alternate monitors for each controlled area as required by AFI 31-101. The primary monitor will be a full-time person whose duties require them to be in and around areas or resources of responsibility. The alternate should also be a full-time person, however, exceptions are authorized at the discretion of the installation commander. All monitors will receive training as directed by the CSF.

4.2. All ANG installations will have an ISC that meets at least semi-annually. The ISC may meet as frequently as required to address open items and other areas pertaining to the security of protection level resources.

4.2.1. ANG units without AFOSI counterintelligence support will use the local FBI detachment or Intelligence office, to provide counterintelligence information relating to the installation's threat.

4.5. FPCONs will only be implemented in response to actual or suspected terrorist activities. Use applicable reporting and local contingency procedures in your ISP to deal with non-terrorist threats.

4.11. The Security Forces Commander is the OPR for publishing and maintaining the ISP at all ANG installations. ANG units that do not have a full-time CSF the senior ranking full-time Security Forces member will act as the OPR with appropriate coordination with the local SF Commander.

5.2. The installation Chief of the Command Post will coordinate reporting requirements and criteria with SF personnel to ensure all events or incidents are promptly and continuously reported. If a security incident is reported during non-duty hours, the Central Security Control (CSC) will contact ANG/XO at DSN 858-6001 or COMM 310-981-6001. SFMIS reports will be submitted from units within six hours after the time the incident has been terminated.

5.3. Units reporting Helping Hands must contact local commanders and notify ANG/XO Operations Center, DSN 858-6001 or COMM 301-981-6001.

5.4. Units reporting Covered Wagons must contact local commanders and notify ANG/XO Operations Center, DSN 858-6001 or COMM 301-981-6001.

5.6. Units will ensure locally generated FPCON changes are reported to the ANG/XO Operations Center, DSN 858-6001 or COMM 301-981-6001, as soon as possible. ANG/XO Operations Center will notify all MAJCOM/SFs, HQ USAF/XOF, and HQ AFSFC Operations Center.

6.5. The CSF will establish and monitor the security deviation program. Security deviations will be accomplished for any deviation from established security procedures, equipment requirements, posting requirements or any other factor affecting security of protection level resources within the purview of this instruction unless it meets the requirements of paragraph 6.7. of the basic instruction. The ISC must be informed of security deviation requests, approvals and deletions.

6.5.1. ANG/XOF is the reviewing authority for deviations from non-nuclear standards, unless otherwise stated, for all ANG installations. If the request for deviation affects a tenant unit, ensure they receive a

copy of an approved deviation. Once the AF 116 is reviewed by ANG/XOF, it is sent to the installation commander for final approval or disapproval by utilizing blocks 30 thru 32.

6.9.1. Security Forces will implement compensatory measures immediately upon detection of vulnerability. Coordinate proposed compensatory measures electronically with ANG/XOF as soon as possible. Do not wait for written approval of a deviation request. ANG Units will ensure compensatory measures are used to bring deviations closer to the intent of the security standard.

6.9.2. Apply the rules from paragraph 6.9.1. of the basic instruction when developing compensatory measures. Take into account the overall security of the area, the total number of deviations in place and the inherent danger to resources created by numerous compensatory measures. If the same compensatory measures apply to more than one deviation, security forces must be able to determine which is the most vulnerable and which requires priority response. Do not establish compensatory measures for convenience purposes. If possible, apply force-multiplying equipment such as, Close Circuit Television and Alarm Systems to compensate for deviations.

7.2.4.1. Continuation training will be provided annually at the unit level. This training will include unit specific security processes, requirements, and local threat briefings.

7.2.4.2. The ISS will evaluate the installation program during assistance visits, or when conducting detection exercises within restricted or controlled areas. Training exercises will be documented by the ISS and briefed to the Installation Security Council (ISC) for AT/FP planning and evaluation.

7.4.2. Units will conduct annual exercises testing the ability of the unit to respond to contingencies listed in the ISP. When possible include off-base support agencies to assist in emergency actions. Contingency exercises will be conducted during day-to-day operations and Unit Training Assemblies (UTAs). Results of these exercises will be documented by the Unit Security Manager and kept on file for two years.

7.6. ANG Force Protection and Operations (ANG/XOFP) will assist with the coordination process for ANG staff or gained MAJCOM staff assistance visits. However, the ANG Compliance and Standardization Requirements List (C&SRL) is the primary tool for self-assessments within the ANG.

8.2.1. Units must determine jurisdictional boundaries for areas under the operational control of the installation commander. Use the jurisdictional status of the area as the basis for establishing plans and procedures in handling offenders. The Chief of Security Forces will work closely with the legal office and local civilian authorities to establish protocols for violators.

8.10. Community oriented policing is not mandated by the ANG. However, units are highly encouraged to utilize this program to expand and develop partnerships between the installation populous and the local community.

8.12. The storage of privately owned weapons within ANG arms rooms and facilities is prohibited. The installation commander may identify and publish special requirements regarding the possession of firearms on the installation by civil authorities. Local instructions should include applicability to unit member's armed IAW state law. For example, federal and civilian law enforcement officers assigned to the installation and law enforcement officials when on official business may possess a duty weapon.

9.7.8. The ISC will determine who will have access to local duress code.

9.10.1. The local entry authority list (EAL) will be completed by the badge issuing authority and authenticated by a Security Forces supervisor (E-6 and above) prior to distribution. Publish approved authenticators (other than SF) by duty position in the ISI.

9.12.2. Inspection and search policies will be coordinated with the legal office and published in the ISI. Implementation will be directed by ISC and approved by the installation commander. Current local threats should be used to determine frequency and process.

9.12.2.2. AF 1109, *Visitor Register Log*, is not required to record escorted or unescorted visits to areas containing PL 3 or PL 4 resources.

10.2.4. Operations and Maintenance (O&M) contract guards will be used to assist Active Guard and Reserve (AGR) security forces during normal and contingency operations. Ensure personnel meet minimum training, certification, and clearance requirements prior to arming and granting unescorted entry to PL areas. CSF will use training requirements IAW AFI 36-2225 and AFI 36-2226, *Combat Arms Program*, Paragraph 2.1.8.1. CSF may include additional training as deemed necessary.

10.5. For the protection of PL 1, 2, and 3, resources security forces personnel will use the M-16 series rifle or M-4 carbine. When required to protect PL 4 resources, M-9s are authorized. Installation commanders of ANG units collocated on commercial airports can authorize the use of shotguns in lieu of the M-16. The use of shotguns must be supplemented with an M-9 and its basic load. The use of shotguns is an alternative for those units in close proximity to civilian runways, where the use of an M-16 is not feasible. Arming requirements will be included in the ISP or AT/FP plans.

10.5.1. ANG units are not authorized to utilize M-203, M-240, or M-249 in day-to-day operations.

10.6. Supporting Forces are subject to the arming restrictions outlined in paragraph 10.5. and 10.5.1. of this instruction.

10.7.7. (Added)) Security Forces vehicles will not be equipped with snowplows or other burdensome non-security related equipment.

11.2.1. Units supporting protection level resources will maintain a combined law enforcement desk and Central Security Control operation under the single title of CSC.

11.2.3. ANG units with an MSCF will consolidate those functions with the CSC.

11.6. ANG units with restricted area boundaries bordering FAA controlled airports and unable to comply with the distance requirements; and ANG units with restricted area boundaries bordering civil property unable to meet distance requirements, must submit and maintain an exception deviation using AF 116.

11.7. Restricted areas with PL 3 resources that are not upgraded to a higher PL status during contingencies will maintain clear zones that allow early detection of intruders. The ISC will direct the width of the clear zone to meet local threat and environmental conditions. Dips, ridges, ditch, and objects that could provide an intruder's unobserved access to the area boundary will be leveled and cleared. Area vegetation will be maintained at a height not to exceed 12 inches in and around restricted areas.

12.4.6. Lines of detection at restricted areas or individual resource boundaries for PL 3 resources must meet a Pd of .90 at the 90 percent confidence level. **NOTE:** Deviations will be required for the absence of this capability after 1 October 2004.

12.12.1.2. The ISC will be responsible, with the technical guidance of the Electronic Security Systems (ESS) NCO, for establishing criteria for the certification testing of IDS used to protect PL 3 resources. The designed certification test must ensure systems meet the effectiveness standards listed, before new systems are certified as useable. Use guidance listed in AFI 31-101, Paragraphs 12.12.2. and 12.12.3. when developing certification requirements. Test older and locally purchased systems using new certifica-

tion requirements and compensate for system failures. Systems do not need to be replaced until the normal replacement cycle is reached or as approved by the ISC.

12.13.1. The ESS NCO (E5 or above) duties will be assigned as an additional duty to a full-time SF NCO who must possess or be able to acquire SEI 323. Units supporting PL 1, 2, 3, or 4 resources will ensure one person from training or stan-eval sections obtains SEI 323 consistent with course availability, or use the correspondence course. It is recommended that all alarm monitors receive the identifier. The ESS NCO and training section will use the ESS Non-Resident STP Course as a guide for developing local training programs for all alarm monitors unable, for what ever reason, to attend the BISS course. **NOTE:** The ESS STP Non-Resident Course will be made available only to units that can show they have sensor equipment on hand to complete the training contained within the course.

12.13.4. Full-time alarm monitors (quarterly) and drill status alarm monitors (semi-annually), must be evaluated with unannounced test on their actions when confronted with a sensor activation message caused by an attempted intrusion. Use a task performance checklist in conjunction with local TEOs to conduct these no-notice evaluations.

12.17.4.3. The ISC/Alarm Working Group will ensure IDS maintenance personnel respond within 48 hours to IDS failures. The ISC will decide when it is necessary to contract local service providers to meet minimum response times. The use of local providers will not degrade response time requirements.

12.19.1. Reports will be sent to ANG/XOF for IDS performance after installation and identification of vulnerabilities. Periodic systems reports, to include catastrophic failure or major malfunction condition in excess of 72-hours, will be submitted using the RCS report (RCS: HAFSPO [(AR) (9346)], Intrusion Detection Equipment Performance Report).

13.5.1. Security forces provide training for owner user personnel responsible for C2-C4 facilities. Test the effectiveness of owner/user entry control as part of the security education and training program. Provide feedback and reports as necessary to maintain an effective level of entry control at these facilities.

13.6. Security required for antenna fields, antennas, and beam forming buildings deviates from normal protection standards because two significant threats, espionage and exploitation, are absent from antennas. Absence of these threats negates the need for continual security forces presence. Protect them with random patrol coverage and physical security checks. All checks will be documented on a locally devised physical security check sheet or included on the AF 53, *Security Police Desk Blotter*.

13.6.1. When areas are located off the installation and it is determined by the ISC that boundary barriers are impractical, for whatever reason, submit a detailed wavier request package AF 116, including photographs to ANG/XOF for consideration.

13.6.3. Vegetation in and around off-base areas containing PL 3 facilities will not exceed 12 inches in height or conceal physical security barriers.

13.6.4.2. If items listed in the basic directive are not alarmed then use Type I locks as listed in (CID) A-A-1927C and MIL standards (STDs) 21313G, Pad Lock Sets Individually Keyed and Keyed Alike and 35647E, Pad Lock, Key Operated.

13.6.6. The ISC will determine the IDS requirements for unmanned PL 3 facilities consistent with local threats. At a minimum, use at least one level of alarm terminating at a central control center able to dispatch response forces.

14.8. The ISC will mandate, within the ISP and ISI, local requirements for the protection of aircrews and their billets. Refer to AFI 31-101, Paragraph 14.8.3. for physical security measures.

16.1. ANG units will follow published Air Force instructions and applicable MAJCOM directives relating to specifically to their Space mission.

20.5. ANG units will combine the IDS and IDE under the technical guidance of the ESS NCO. All IDE purchased by owner/user will be from the approved AF equipment list and approved by the ISC, or Alarm Working Group to ensure compatibility with existing or planned IDS for PL 1, 2, or 3 resources.

20.5.1. Owners/users that lack organic installation or maintenance support will ensure that prior to purchasing IDE/IDS system, a contract for maintenance and installation are included.

23.1.1. ANG firearm storage facilities will not be used to store non-appropriated fund activities or privately owned firearms. Exception: Wing commanders have the authority to approve storage of firearms for federal, state, and civilian law enforcement officers. The use of AF 1473, *Gun Equipment Room Inventory*, (localized) or a computer-generated product with required information is approved for arms room inventories.

23.1.10. The protection deviations for M-1 and .30 caliber rifles (NSN 1005-00-599-3289) and M-16 (1005-01-460-3280) category IV firearms will be forwarded to ANG/XOFP. Deviation requests must state the manner in which these firearms will be protected and the reason for the deviation. **NOTE:** Convenience is not an acceptable reason for a deviation request.

23.3.2. Areas containing category III and IV AA&E will have one level of IDE provided to detect entry into facilities. Security forces will provide as a minimum one non-duty hour check daily to these facilities. When IDE fails or is inoperable, the owner/user will be responsible for the protection of the facility and immediate visual assessment and post a sentry during non-duty hours.

23.5. All deviations to AA&E transportation requirements will be coordinated through ANG/XOFP. Ensure deviation procedures are included in the ISP. Also, the local threat and available resources must be considered.

23.11.1. The base CSF will immediately notify ANG/XOFP of all significant losses by phone or through the ANG/XO Operations Center DSN 858-6001 or COMM 301-981-6001. Follow reporting procedures IAW AFI 31-101, Chapter 23, Paragraph 23.11.3.

23.11.3. Units will ensure that MOU/MOAs are established with servicing AFOSI and local authorities to meet this requirement.

24.1. Every effort should be made to place mission support aircraft within designated mass parking areas or restricted areas.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

BSEC—Base Security Executive Council

C&SRL—Compliance and Standardization Requirements List

IAW—In Accordance With

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

O&M—Operations and Maintenance

SFMIS—Security Forces Management Information System

TEEO—Training Exercise Evaluation Outline

UTA—Unit Training Assembly

DANIEL JAMES III, Lieutenant General, USAF
Director, Air National Guard