AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

§ 637.15 Polygraph activities.

MPI and DAC detectives/investigators will utilize the polygraph to the full extent authorized. Requests for polygraph examination assistance will be forwarded to the supporting USACIDC element in accordance with provisions of AR 195–6. The investigative or intelligence element requesting approval to conduct a polygraph examination will submit a completed DA Form 2805 (Polygraph Examination Authorization) to the authorizing official. A request may also be sent via an electronic message or electronic mail or media provided all elements of the DA Form 2805 are included in the request. Approvals will be obtained prior to the conduct of an examination. Telephonic requests, followed with written requests, may be used in emergencies. The requesting official will include the following data on every polygraph examination request for criminal investigations:

(a) The offense, which formed the basis of the investigation, is punishable under Federal law or the UCMJ by death or confinement for a term of 1 year or more. Even though such an offense may be disposed of with a lesser penalty, the person may be given a polygraph examination to eliminate suspicion.

(b) The person to be examined has been interviewed and there is reasonable cause to believe that the person has knowledge of, or was involved in, the matter under investigation.

(c) Consistent with the circumstances, data to be obtained by polygraph examination are needed for further conduct of the investigation.

(d) Investigation by other means has been as thorough as circumstances permit.

(e) Examinee has been interviewed on all relevant subjects requested for testing and the polygraph examination is essential and timely.

§ 637.16 Evidence.

Military police are authorized to receive, process, safeguard and dispose of evidence, to include non-narcotic controlled substances, in accordance with AR 195–5. If no suitable facility is available for the establishment of a military police evidence depository or other operational circumstances so dictate, the evidence custodian of the appropriate USACIDC element may be requested to receipt for and assume responsibility for military police evidence. Personnel selected as military police evidence custodians need not be trained as MPI and should not be issued MPI credentials, unless they are also employed as operational MPI. Further information concerning evidence collection and examination procedures can be found in Field Manual (FM) 3–19.13, Law Enforcement Investigations.

§ 637.17 Police Intelligence.

(a) The purpose of gathering police intelligence is to identify individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity. If police intelligence is developed to the point where it factually establishes a criminal offense, an investigation by the military police, (USACIDC) or other investigative agency will be initiated.

(b) Police intelligence will be actively exchanged between Department of Defense (DOD) law enforcement agencies, military police, USACIDC, local, state, federal, and international law enforcement agencies. One tool under development by DOD for sharing police intelligence is the Joint Protection Enterprise Network (JPEN). JPEN provides users with the ability to post, retrieve, filter, and analyze real-world events. There are seven reporting criteria for JPEN:

(1) Non-specific threats;
(2) Surveillance;
(3) Elicitation;
(4) Tests of Security;
(5) Repetitive Activities;
(6) Bomb Threats/Incidents; and
(7) Suspicious Activities/Incidents.

(c) If a written extract from local police intelligence files is provided to an authorized investigative agency, the following will be included on the transmittal documents: ''This document is provided for information and use. Copies of this document, enclosures thereto, and information therefrom, will not be further released without the prior approval of the installation Provost Marhsall.

(d) Local police intelligence files may be exempt from certain disclosure requirements by AR 25–55 and the Freedom of Information Act (FOIA).

§ 637.18 Electronic equipment procedures.

(a) DOD Directive 5505.9 and AR 190–53 provide policy for the wiretap, investigative monitoring and eavesdrop activities by DA personnel. The recording of telephone communications at MP operations desks is considered to be a form of command center communications monitoring which may be conducted to provide an uncontroversial record of emergency communications. This includes reports of emergencies, analysis of reported information, records of instructions, such as commands issued, warnings received, requests for assistance, and instructions as to the location of serious incidents.

(b) The following procedures are applicable to the recording of emergency telephone and/or radio communications at MP operations desks within the 50 states of the United States, the District of Columbia, the Commonwealth of Puerto Rico, Panama, and Guam.

(1) All telephones connected to recording equipment will be conspicuously marked ''For Official Use Only-connected to recording device'' and access to use will be restricted to MP operations desk personnel.

(2) The connection of voice-recording equipment or private-line service with the telecommunications network will be in accordance with applicable telephone company tariffs which permit direct electrical connection through telephone company recorder-connector equipment. An automatic audible-tone device is not required.

(3) Official emergency telephone numbers for MP desks will be listed in appropriate command, activity, or installation telephone directories with a statement that emergency conversations will be recorded for accuracy of record purposes. Other forms of prewarning are not required.

(4) Recordings, which contain conversations described in this section, will be retained for a period of 60 days. Transcripts may be made for permanent files, as appropriate.

(5) The recording of telephone communications or radio transmissions by MP personnel for other than emergency purposes is prohibited. If an investigator requires the use of electronic surveillance equipment, assistance must be requested from the USACIDC. This policy is established pursuant to Department of Defense directives that limit such activity to the criminal investigative organizations of the Services and DOD.

(6) Commanders having general courts-martial convening authority will issue written authorizations for the recording of emergency telephone communications at MP operations desks. The letter of authorization will contain specific authority for the type of equipment to be used, the phone numbers identified as emergency lines and instructions limiting recordings to calls received on the phones so designated. One copy of the authorization will be forwarded to the Office of the Provost Marshal General (OPMG), 2800 Army Pentagon, Washington, DC 20310–2800.

§ 637.19 Overseas MP desk.

The recording of telephone communications at MP operations desks outside the United States will be conducted within restrictions contained in international agreements between the U.S. and host nations.

§ 637.20 Security surveillance systems.

Closed circuit video recording systems, to include those with an audio capability, may be employed for security purposes in public places so long as notices are conspicuously displayed at all entrances, providing persons who enter with a clear warning that this type of monitoring is being conducted.

§ 637.21 Recording interviews and interrogations.

The recording of interviews and interrogations by military police personnel is authorized, provided the interviewee is on notice that the testimony or statement is being recorded. This procedure is a long-accepted law enforcement procedure, not precluded by DA policies pertaining to wiretap, investigative monitoring, and eavesdrop activities.