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.