
Joint Protection Enterprise Network

By Mr. Jeffery Porter and Mr. James Crumley

The guard on the gate, the military and civilian police on the street, the desk sergeant, and ultimately the installation provost marshal (PM) collect and disseminate information on potential threats to their installation and support force protection (FP) programs. This information can be passed to or viewed by other Army installations and Department of Defense (DOD) facilities to enhance the sharing of police intelligence information. The commander of US Northern Command (NORTHCOM) is assigned to manage the Joint Protection Enterprise Network (JPEN) as an integrated information-sharing system. Army Regulation 190-45, *Law Enforcement Reporting*, informs Army PMs and directors of emergency services (DESS) of the availability of JPEN as a DOD tool that may be used to share police intelligence with—

- DOD law enforcement agencies.
- Military police.
- The US Army Criminal Investigation Command.
- Local, state, federal, and international law enforcement agencies.

JPEN also gives users the ability to post, retrieve, filter, and analyze real-world events. JPEN is a Web-based automated program that allows the timely sharing of FP-related information to provide situational awareness to the DOD law enforcement, FP, and antiterrorism (AT) communities. Designated staff members from the office of the installation PM or DES can access this information from any computer with access to the World Wide Web. JPEN data is collected using the threat and local observation notice (TALON) report. The TALON report is similar to a tactical size, activity, location, unit, time, and equipment (SALUTE) report in that it is used to collect the “who, what, when, where, why, and what actions,” if any are taken. TALON reports are preliminary reports on ambiguous activity and may contain raw, unvalidated information. The intent of TALON and JPEN is to ensure standardized reporting.

The seven criteria that may generate a TALON report in JPEN are as follows:

- **Nonspecific threats.** These are threats that may be received from any number of sources and contain a specific time, location, or area for an attack against US forces, facilities, or missions.
- **Surveillance.** Surveillance includes attempts by individuals to record information about an installation.
- **Elicitation.** Elicitation is any attempt to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and need to know.
- **Tests of security.** Tests of security are attempts to measure security reaction times or strengths; test or penetrate physical security barriers or procedures; or acquire or duplicate uniforms, badges, passes, or other security activities.
- **Repetitive activities.** These are activities that meet one of the categories above and have occurred two or more times within a one-month period.
- **Bomb threats.** Bomb threats are communications by any means that specifically threaten to use a bomb to attack US forces, facilities, or missions.
- **Suspicious activities and/or incidents.** These are activities and/or incidents that do not meet any of the previously listed activities or incidents but represent a potential FP threat.

Installation commanders are responsible for ensuring adequate use of the JPEN system to maximize its potential to provide assessment and situational awareness at installation, regional, and national levels. Installation commanders must designate site coordinators to manage the system on their installations. Site coordinators will identify users and assist them with establishing JPEN accounts from NORTHCOM. Typical JPEN users on an

installation could include representatives from the staffs of the PM; the assistant chief of staff (operations and training); the Directorate of Emergency Services; and the Directorate of Plans, Training, Mobilization, and Security and AT officers.

For the first time, JPEN and TALON reports now present the opportunity for multiple disciplines to

merge the results of their information gathering and begin information fusion and analysis at the lowest level possible, specifically focusing on suspicious activities as a proactive countermeasure to potential threats. All Army law enforcement and/or security agencies will complete the actions necessary to employ JPEN and TALON reporting.