

Multiforce Protection In a Portal

October 2004 - By Cheryl Lilie



The Joint Protection Enterprise Network (JPEN) allows gate officers to document suspicious or repetitive activity such as a vehicle that has been denied base entry. Once the information is entered, personnel at nearby bases can be notified immediately to be on the lookout for the same vehicle.

Web-based network provides situational awareness across military installations.

A cross-service network that shares sensitive but unclassified information among U.S. Defense Department installations is moving nationwide. The Web-portal technology allows users to document and immediately disseminate information regarding potential threats to personnel, facilities and resources to meet antiterrorism and force protection needs.

Work began shortly after the September 11, 2001, terrorist attacks to establish an integrated force protection information-sharing system that would provide common situational awareness around military facilities for all the services. Concept development and design for Protect America, the precursor to the system, now dubbed the Joint Protection Enterprise Network (JPEN), began in February 2003 (*SIGNAL*, June 2003, page 35). By the end of April, the pilot program was

operational in the national capital region, and shortly thereafter the project was renamed Vision. With some additional guidance from Defense Department staff and Secretary of Defense Donald Rumsfeld, the program was focused on Defense Department installations for a proof-of-concept approach. In July 2003, the project took its current name, JPEN.

Program management responsibilities, originally under the Joint Staff, transferred to U.S. Northern Command (NORTHCOM), Colorado Springs, Colorado, in December 2003. NORTHCOM plans, programs and directs JPEN funding; coordinates requirements for software enhancements; and prioritizes JPEN deployment with staff elements. In addition, the command provides operational guidance to the JPEN program manager in the command and control program office, U.S. Navy Program Executive Office for Command, Control, Communications, Computers, Intelligence and Space, and the JPEN engineering element at the Space and Naval Warfare Systems Command Systems Center, both in San Diego.

“NORTHCOM assumes responsibility for the force protection mission within its area of

responsibility as of October 1, 2004, so it makes perfect sense that NORTHCOM maintains program management of JPEN,” says Maj. Gen. Dale W. Meyerrose, USAF, director of command and control systems, North American Aerospace Defense Command; director of architectures and integration, NORTHCOM; and chief information officer for both commands.

Although JPEN has changed hands and names several times since its inception, the way the program works essentially has remained the same. Users can document and share suspected criminal and suspicious activity information formatted as threat and local observation notice (TALON) reports. These reports consist of nonvalidated domestic threat information that may or may not be related to an actual threat against a facility. TALON reports include nonspecific threats, suspected surveillance activity, elicitation attempts, tests of security, unusual repetitive activity, bomb threats and any other suspicious, potential terrorist-related activity directed against Defense Department assets. JPEN also records information about other force protection incidents, including vehicles denied entry to installations—or vehicle turnarounds—and “be on the lookout” (BOLO) reports of suspicious vehicles or individuals.

Each incident or TALON report is documented in JPEN as an “event.” An event report contains all the information related to an incident, such as a vehicle turnaround, including individual and vehicle descriptions. Once the information is entered into the system, it is available immediately to all users. If the same individual tries to gain access to another military base, for instance, JPEN will notify the appropriate users of the previous attempt. “It may or may not be terrorist related,” the general says, “but proof of repetitive activity is definitely more concerning than an individual making a wrong turn.”

Information on events entered in JPEN is available to all designated users at a Defense Department installation, agency or facility from any nonsecure Internet protocol router network through Internet Explorer version 5.5 or higher. This capability not only expands the potential user base but also minimizes or eliminates the need for users to obtain additional hardware or software to access the system. Using existing information technology infrastructure at each installation makes JPEN easily scalable, accessible and—because there are no access fees—affordable.

Although all users can read reports on force protection incidents and search the database, only certain users can update an installation’s force protection condition or event status. The network allows for different levels of access based on mission requirements. Security also is maintained by 128-bit secure socket layer encryption, firewalls, intrusion detection devices, Internet protocol filtering and audit trails.

JPEN is limited to storing and sharing unclassified data because it documents only raw force protection reports and conditions, such as information gathered by gate guards at military installations. Some data may be law enforcement sensitive if it supports an ongoing investigation, and this information would be limited to access by law enforcement professionals. Overall, JPEN operates at the unclassified level, and its data is considered for official use only.

Users can search the database to find events of interest based on city, state, installation/facility name, or type of event; or they can conduct a keyword search for correlation, verification and to uncover trends. While most of the incident data is not deleted from the database, data that falls under the purview of JPEN’s privacy guidelines is purged

after 90 days unless it is part of an ongoing investigation.

Gen. Meyerrose considers the ability to share information horizontally as well as vertically to be one of JPEN's key strengths. "Traditionally, vertical information sharing has essentially worked, but horizontal sharing has been difficult at best," he says. "JPEN allows base-level installations and agency locations to share information at the tactical level, warfighter to warfighter."

JPEN is a force multiplier because the information entered into the system is available to military policemen at a U.S. Army post, service operations centers and headquarters all at the same time. There is no need to coordinate the information up the chain of command and then wait for an analysis and a response. If an incident may affect another installation, that installation immediately can take precursory action.

Currently, JPEN is a Defense Department-wide system that has been fielded at approximately 40 locations throughout the country. Expansion to other locations is scheduled to take place this month. NORTHCOM also plans to further expand JPEN across the continental United States over the next two years, but the command is first focusing on service components and subordinate units—the organizations it calls upon to execute its missions. At the same time, it is fielding JPEN to selected Defense Department agency locations. These sites are scheduled to be operational this month as well. Training teams will follow up with the other service and defense agency sites, focusing on regions with greater numbers of installations.

However, further fielding of the system is a concern. "Expanding JPEN to other federal entities will entail some added policy and procedure work ahead to ensure that it's done correctly," Gen. Meyerrose says. "But we are convinced it won't be a technology issue that holds us up."

With a much larger user base, additional requirements from new users will need to be addressed. "Many of these requirements will be installation- or service-specific, while others will be great ideas that we couldn't get into the current release version of the software, or those that come from widespread use," the general explains. NORTHCOM plans to take the best of these ideas, implement and field them as rapidly as possible using a standard block and spiral approach, and provide a comprehensive system that meets all critical user requirements.

The command recognizes that an architecture is needed that allows users to post information once and then automatically shares that information with all users who need it, irrespective of their service or the system used. "If they enter information into their current system and then need to re-enter it into JPEN," he says, "they won't use the system."

"We want the system to interface with all existing service and agency systems that record and maintain force protection data," the general continues. "We need to get the information to and from frontline force protection personnel quickly without causing redundant actions that add to their existing workload."

Gen. Meyerrose states that JPEN is expected to become merely one of the components in the future force protection toolkit used by all services and the 16 Defense Department field activities. NORTHCOM intends to architect a common information exchange environment for the force protection warfighter in an interoperable format. According to Gen. Meyerrose,

rather than using separate, stand-alone systems and “swivel chair integration” to pass data back and forth, each system would seamlessly share the appropriate data with other systems. “The user may not even know which system provides his or her data needs. All they know is it’s there when they need it among all the applications they use with no manual effort,” he says.

Military installations may not be the only beneficiaries of JPEN. The first responder and civilian communities also may find JPEN capabilities useful. Cell Exchange, the company that initially developed JPEN, has created a similar version of the technology for the city of Jacksonville, Florida, as a citywide homeland security and crime prevention application.

In addition, JPEN was one of the many programs tested at Joint Warrior Interoperability Demonstration 2004 in June. One portion of the test included collaboration with the Disaster Management Interoperability Services (*SIGNAL*, June 2004, page 63), another Webportal-based system that provides disaster information and awareness to first responders and citizens.

Web Resources

U.S. Northern Command: www.northcom.mil

JWID: www.jwid.js.mil

Disaster Management Interoperability Services: www.cmi-services.org

SIGNAL Magazine

<http://www.afcea.org/signal/>