STEP Up to Prison Security Planning

*A*n inmate escapes from a county jail into the community and subsequent analysis indicates that the facility's camera system is outdated and did not help to prevent the escape. Due to the ensuing media attention, the county commissioners want to fund a major upgrade of security technology, and jail administrators need to immediately offer a plan to proceed.

Too often, that plan does not exist.

In good times or bad, correctional facilities should always have a security technology enhancement plan (STEP) ready to present, according to Gene Atherton, institutions program manager at the National Law Enforcement and Corrections Technology Center's Weapons and Protective Systems Technologies Center of Excellence (WPSTC), hosted by the University of Denver. NLECTC is a program of the Office of Justice Programs' National Institute of Justice.

"A good STEP should be like a shopping list that is ready to use," Atherton says. "In the best of all worlds, it should be one portion of an overall plan for the institutional security program. Like a shopping list, it should reflect what you want, where to get the product and the best price."

In 2009, WPSTC helped the Security Systems section of the Texas Department of Criminal Justice-Correctional Institutions Division assess security enhancement strategies. Atherton examined strategies regarding surveillance and contraband interdiction and provided valuable analysis and feedback.

"His discussion of fundamental components inherent to a security enhancement strategy was highly informative," says Charles Bell, assistant director of security systems. "Of special interest was Gene's insight regarding the necessity for including a process to measure the effect of applied strategies. Having the opportunity to benefit from the knowledge and experience provided by the center was significant. The analysis provided validation to much of

our initiatives and added value to the security enhancement strategy product."

Bell adds that developing a viable security enhancement strategy is essential for any correctional unit or agency, although funding these initiatives often presents a challenge for law enforcement and corrections. However, STEP preparation plays a key role in readying an agency or department to act decisively when an opportunity arises.

A good STEP should accurately reflect institutional needs, Atherton says, and must connect the proposed technology with expected performance outcomes.

"It is easy to justify technology that relates to officer safety or prevents escapes," he says.

Decision makers presented with major funding issues require accountability. If an institution wants to strengthen perimeter technology with a detection system, administrators need to provide reliable information that past escapes have occurred through similar perimeters and that the proposed changes will make a difference, Atherton says.

"Strategies should begin with identifying the most critical need and transition incrementally toward a comprehensive package designed to achieve maximum security," Bell says. "Constructing a global security augmentation strategy requires a series of definable objectives. From these objectives, an institution or agency develops a series of strategies that may be either independent or integrated as opportunity dictates. Collectively, they form an avenue to achieve a larger security enhancement goal."

Atherton adds, "Technology costs and providers change constantly. However, once the format is established and support staff are made aware of the right sources of information, it should not be difficult to upgrade and adjust the plan over time."

A STEP has several operational segments:

- **Perimeter security.** Includes lighting, fencing materials, electronic detection of movement on the perimeter, equipment for staff duty stations (sally ports, towers and vehicles) and electronic contraband detection.

- **Staff and inmate communication.** Involves technology related to intercoms, radios, telephones, emergency callback systems, pagers and cell phones.

- **Contraband detection**. Entails metal detectors, x-ray machines and technologies such as ion scanners.

Each plan must address an institution's particular needs and highlight the high-priority ones. Technology specifics should include a product name, unit cost and overall summary of required funds. Suggest several different funding levels to provide options, Atherton says. The plan should also reflect short-term and long-term maintenance costs, answer how the system can be conveniently folded into an existing technology maintenance program at the facility and detail additional staff services required.

For more information on STEP in general, contact Gene Atherton at (800) 416-8086 or e-mail gene.atherton@ nlectc-rm.org. For more information on Texas' efforts, contact Charles Bell at Charles.Bell@tdcj.state.tx.us.