NLECTC
National Law Enforcement and Corrections Technology Center

Taking a STEP in the Right Direction

NIJ

A program of the National Institute of Justice

June 2013

FACT SHEET

A good security technology enhancement plan (STEP) for correctional agencies should be like a "shopping list" that is ready to use. In the best of all worlds, it makes up one portion of an overall plan for an institutional security program. Like a shopping list, it should reflect what an institution wants, where to get the products and the best price.

Correctional institutions may go for years without getting many resources for needed technology improvements, with a common result being a focus of attention on other management challenges, according to analysis conducted by the National Law Enforcement and Corrections Technology Center (NLECTC) System. The problem is that when an opportunity does arise (sometimes unexpectedly), poor decisions can result from an institution's not being prepared. For example, an inmate may escape from a county jail into the community. After-action analysis indicates that the outdated camera system in the jail needs replacement. In the midst of all the bad publicity, county commissioners are ready to fund a major upgrade of security technology at the jail, but jail leadership needs to offer a plan to proceed immediately. In good times or bad, correctional facility administration should always have a STEP plan ready to present. However, that plan too often does not exist.

The first function of a correctional institution is to protect the public. Thus, security is of primary importance to every correctional agency. An agency that cannot prevent escapes and control violence within its institutions is considered a failure (*Guidelines for the Development of a Security Program,* American Correctional Association, 2007). This mission is difficult to accomplish without a successful expression of resource needs.

Security Enhancement Success Story

In early 2009, the NLECTC System helped the Security Systems section of the Texas Department of Criminal Justice-Correctional Institutions Division assess its security enhancement strategies. NLECTC staff examined strategies regarding surveillance and contraband interdiction and provided analysis and feedback. The Security Systems section now has a STEP plan in place. Security Systems Assistant Director Charles Bell believes that developing a viable security enhancement strategy is essential for any correctional unit or agency, although funding these initiatives often presents challenges. However, STEP preparation plays a key role in readying an agency or department to act decisively when an opportunity presents itself. Some key issues related to its development follow:

- A good STEP should accurately reflect institutional needs and the ability to meet the mission requirements of an organization. For example, an institution can easily justify technology that relates to officer safety or technology that helps prevent escapes. The more direct the relationship between those outcomes and the product, the easier an institution finds it to justify the technology. Thus, a good STEP, wherever possible, must connect the proposed technology with expected performance outcomes.

- Decision makers on major funding issues require accountability. An administrator who wants to strengthen perimeter technology with a new detection system needs to reliably demonstrate that the proposed changes will make a substantial difference and reflect that information in the STEP plan. Also, the administrator needs to be able to describe results in the form of measurable objectives.

- The STEP must be ready to come off the shelf and be presented at any time. Once the format is established and support staff know about the right sources of information, administrators can easily upgrade and adjust the plan over time.

- Depending on the needs and style of the agency, the STEP can address different operational requirements. One section may be related to perimeter security in the form of lighting, fencing materials, electronic movement detection and equipment for staff duty stations (sally ports, towers and vehicles). Another section could be *staff and inmate communication,* which would involve technology related to intercoms, radios, telephones, emergency callback systems, pagers and cell phones. *Contraband detection,* including metal detectors, x-ray machines and technologies such as ion scan makes up a third section.

- Administrators should specify technologies in each functional area, including a capability requirement, unit cost and overall summary of funds needed. Options could suggest different funding levels; legislators and commissioners very often do not like to think there is only one option to address security concerns.

- Finally, the plan should reflect changes in short-term and long-term maintenance, answer whether the technology can be conveniently folded into an existing program and explain whether additional staff services are required.

The typical high dollar amounts for security technology demand accountability in the form of product knowledge and professional decision making in choosing technology. Each STEP plan must address an institution's particular needs and highlight the high-priority ones.

For More Information

The Corrections Technology Center of Excellence administers several corrections-related programs for the National Institute of Justice and the NLECTC System. Learn more about the CoE at http://www.justnet.org.