No More "Cell" Phones

By National Institute of Justice Staff

Editor's Note: This article was reprinted from the Winter 2005 edition of TechBeat, the quarterly news magazine of the National Law Enforcement and Corrections Technology Center, an NIJ program. Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corp. Points of view or opinions contained in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

In the late-night quiet of a prison cellblock, an inmate slips his hand into a small slit under his mattress and pulls out a cell phone. Speed dial connects him to his outside contact, he speaks a few prearranged words, and another drug deal is made. Technology allows him to operate as if he were still on the streets.

As cell phones become smaller, it becomes easier to smuggle them inside correctional facilities and easier for inmates to continue their criminal activities, harass victims or transmit photographs of information.

Fortunately, in today's technology-driven society, when one innovation creates a problem, a new one usually comes along to solve it. But, for corrections the question becomes where to find the right innovation.

Several possible technology approaches have been identified to deal with the cell phone problem in prisons and correctional facilities:

Locate and confiscate cell phones. This approach, says Ike Eichenlaub, chief of the Federal Bureau of Prisons' Office of Security Technology, requires a technology that minimally will:

- Work even when cell phones are turned on for only a few minutes at a time;
- Detect signals coming from any area of a facility; and
- Find transmissions through thick concrete walls in single story to multifloored buildings and in locations from urban areas to remote rural districts.

Ideally, he says, such technology would require minimal or no training to use, expand to cover other wireless technologies such as two-way pagers and operate on a 24/7 basis.

Overpower the signal with a stronger signal. "Another potential approach is commonly referred to as 'jamming,' which emits a signal stronger than a cell phone's signal and renders it useless," Eichenlaub says. Senior BOP Technologist Jim Mahan adds, "There are two types. One is called brute force jamming, which just blocks everything. The problem is, it's like power-washing the airwaves, and it bleeds over into the public broadcast area. The other type puts out a small amount of interference, and you could potentially confine it within a single cellblock. You could use lots of little pockets of small jamming to keep a facility under control."

"Trick" the phone. Eichenlaub describes a third possible approach, commonly called "spoofing," as tricking the cell phone to react as if a "no service" signal is received.

The Federal Communications Commission, however, prohibits both jamming and spoofing, he says, so implementing either of these technologies would require legal and regulatory changes.

Intercept the signal. A fourth possible approach, signal interception, retrieves telephone and serial numbers from operational phones, but can be implemented only under a judge's order.

Eichenlaub says that although signal interception is feasible, "We are looking for the simplest option, which is signal detection. There are no regulatory or legal issues here; if you can find it, you can go get it."

Cellular providers use different communications protocols, but all cell phones use radio frequency (RF) antenna power. The BOP has studied a number of off-the-shelf technologies to detect RF signals. Although detection equipment is available, costs can reach tens of thousands of dollars. "Some work better than others," Mahan adds. "Some work for only a short distance, maybe about 15 to 20 feet. This is impractical if you're trying to cover 50 acres. Also, each device may cost about $1,000. There is some promising new technology that is showing better results than anything else we've ever seen, but they are still prototypes. The question is whether the technology can be made at a cost that we can afford.

In response, BOP, the National Institute of Justice (NIJ), and the Naval Surface Warfare Center–Dahlgren are collaborating on a multiyear project to evaluate the problem and ultimately help develop that technology. BOP spent the first 6 months of 2004 evaluating and testing various possibilities. Now Dahlgren staff members (with NIJ funding) will evaluate the problem and potential technical solutions to provide a roadmap for addressing it. In the course of this evaluation, they will:

- Analyze and document BOP's work;
- Discuss this issue with the American Correctional Association and the Association of State Correctional Administrators to ascertain the needs of state and local correctional institutions and determine how they might differ from BOP requirements;
- Assess the spectrum of potential approaches and technology solutions; and
- Ultimately, incorporate BOP's work and other information into a report that recommends NIJ's next technology development steps.

Gary Maclellan, project manager for NIJ, expects the report to be released in FY 2006. For more information on the BOP's research into cell phone use by inmates, contact Ike Eichenlaub at (202) 305-8448 or LEichenlaub@bop.gov. For more information on NIJ's involvement, contact Gary Maclellan at (202) 305-7339 or Gary.Maclellan@usdoj.gov.