DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES
Overview Of Cell Phone Demonstration

BACKGROUND

The use of illegal cell phones within jails and prisons is a growing concern among correctional administrators across the country. These phones are being used by inmates to continue their criminal behavior from behind secure walls. Under the leadership of Governor Martin O'Malley, the Maryland Department of Public Safety and Correctional Services has begun the process of investigating appropriate actions to prevent the introduction and use of cell phones within our correctional system.

The Department has employed a number of contraband interdiction methods that result from evidence based practices within the correctional field. These include:

- Secure View Scanner – provides scan of all individuals entering a facility;
- BOSS Chair – electronic body search device;
- X-Ray Machines – used to scan incoming packages and mail;
- Perimeter cameras – to monitor perimeter activity;
- Intelligence Unit – enhanced method of data collection and sharing;
- Searches – variety of searches for inmates, staff, and visitors; and
- K-9 Units – canines trained to detect cell phones.

The Department has had some success utilizing a combination of these methods and has confiscated over 2,000 phones since FY 08. Unfortunately, we know that these methods are not enough to completely prevent the use of cell phones. Across the country, cell phones have been used to orchestrate homicide, incite riots, intimidate witnesses and public officials, coordinate escapes, facilitate credit card fraud, and introduce contraband into correctional environments.

In order to develop an effective mechanism to prevent this type of activity from continuing, it is necessary to identify an effective and efficient method through the use of technology to detect and prevent calls from illegal cell phones. On July 15, 2009, Secretary Gary Maynard provided testimony in support of The Safe Prisons Communications Act of 2009, S. 251. This bill is designed to provide governors and correctional administrators with the ability to petition the Federal Communications Commission and request the operations of a wireless jamming device within a prison or jail. This type of technology, if administered appropriately, would render all cell phones within a prison useless. It would provide a broad strike against illegal cell phone use.

However, jamming technology is not the only type of cellular interdiction available to the corrections community. In addition to support of S. 251 at the federal level, Maryland collaborated with the Association of State Correctional Administrators to identify vendors providing technology alternatives to jamming. We convened a team with expertise crossing a variety of fields including membership from: Public Safety (corrections, security, policy, and information technology), the Governor's Office of

Homeland Security, and the Governor's Office of Crime Control and Prevention. Our team met with 12 vendors in a series of educational meetings designed to provide us with the best understanding of the various technologies that could be deployed in a correctional setting. The following is a list of those companies:

1 ASTIC Signals Defenses, LLC
2 Cell Antenna
3 Cell Scan
4 Computer Consulting Partners, Ltd
5 ITT
6 JFPC Solutions
7 Lockheed Martin
8 MicroTech\Air Patrol
9 Nortel
10 SoTech
11 Tecore
12 Triple Dragon

The companies offered one or a variety of the following types of technology:

- Blocking – uses material (mesh wiring, wallpaper paint, films, etc,) embedded with metal fragments to prevent cell-phone signals from reaching an antenna
- Detection – locates cell phones that are in use
- Interference – intercepts cell phone calls and directs call from authorized cell phones to their carrier. Emergency 911 calls are allowed through.
- Jamming – prevents a cell phone from connecting with a cell phone carrier

Of those who made the initial presentation to the team, many were invited to participate in a group demonstration to see first hand how technologies could be used within a correctional setting. Of those invited, six agreed to participate.

DEMONSTRATION

On September 3, 2009 the Maryland Department of Public Safety and Correctional Services hosted a cellular disruption demonstration at the decommissioned Maryland House of Correction in Jessup, Maryland. The purpose of the demonstration was to test various non-jamming technologies for their effectiveness within the correctional environment. Of the six vendors who participated, five were able to provide a live demonstration of their technology.

The Department invited colleagues from around the country to attend the event to share ideas and gain a better understanding of the existing technology. Below is a list of attendees:

- American Correctional Association (ACA)
- American Jail Association (AJA)

- Association of Public-Safety Communications Officials (APCO) International
- AT&T
- Baltimore City Police
- Baltimore Sun
- Baltimore Office of the State's Attorneys
- Carroll County Detention Center Count
- CNN
- CTIA - The Wireless Association
- Delaware Department of Correction
- Maryland Department of Legislative Services
- District of Columbia Division of Correction
- Governor's Office of Crime Control and Prevention
- Governor's Office of Homeland Security
- National Criminal Justice Association
- National Governor's Association
- National Institute of Justice Office Science & Technology
- New Jersey Department of Corrections
- Shawntech, Inc.
- South Carolina Division of Correction
- Sprint/Nextel
- T-Mobile
- Verizon
- Virginia Division of Correction
- West Virginia Division of Corrections

Each vendor was given an opportunity to set up and test their devices prior to the live demonstration. They were staged within the decommissioned Maryland House of Correction.

Each vendor was given one hour to provide an overall presentation of their company and the specific technology solution to be demonstrated. The Department assembled a team of officers equipped with activated cell phones throughout each tier during the respective company demonstrations. Companies were asked to demonstrate their capabilities according to the following six testing phases:

Phase 1 - Detection/Control of turned off cell phone.
Phase 2 - Detection/Control of turned on cell phone.
Phase 3 - Detection/Control/Intel of cell phone placing a call.
Phase 4 - Detection/Control/Intel of cell phone receiving a call.
Phase 5 - Detection/Control/Intel of sending and receiving text messages.
Phase 6 - Processing of 911 calls.

Cell phones from the four major carriers: Verizon, Sprint, T-Mobile, and AT&T; as well as a confiscated prepaid cell phone were used for the testing phases. The staging included a manager directing the specific steps through the use of a hand-

held radio. The manager directed five correctional officers. Each of the officers used a cell phone and was assigned to a specific location along the tier where the specific demonstration was taking place. The officers' function was to move their cell phone to a randomly selected cell at the start of each testing phase and then operate the cell phone as directed according to the requirements of the testing phase. A correctional supervisor was assigned to the decommissioned facility's master control, renamed "demo control" for testing purposes, and tasked with using a land line to receive and place calls with the cell phones in accordance with Phases 3 and 4 of the test script. An executive assistant at Division of Corrections Headquarters was tasked with receiving and sending text messages during Phase 5.

The following is a sample of the radio calls and steps used during the direction of each demonstration.

Demo 1 Commencing. (Officers enter the testing area)

Phase 1 Cell Phone Placement (Officers randomly enter cells)

The Director worked with the vendor verifying detection.

Phase 2 Cell Phone Placement

One at a time, each officer was directed to turn on their phone while the director confirmed detection with the vendor.

Phase 3 Cell Phone Placement

One at a time, each officer was directed to place a call to demo control while the director confirmed detection with the vendor.

Phase 4 Cell Phone Placement

One at a time, each officer was directed to receive a call from demo control while the director confirmed detection with the vendor.

Phase 5 Cell Phone Placement

One at a time, each officer was directed to send and receive a text message while the director confirmed detection with the vendor.

Phase 6 Cell Phone Placement

One at a time, each officer was directed to dial 911 while the director confirmed detection with the vendor with the vendor.

RESULTS AND FINDINGS

Below is a list of the participating vendors who were able to demonstrate a potential solution:

- Compucat, Washington, DC
- ITT, Columbia, MD
- MicroTech/Air Patrol, Vienna, VA
- Nortel, Fairfax, VA
- Tecore, Columbia, MD

Of the vendors, none were able to detect phones when they were placed in the off position. Four of the five vendors demonstrated passive, receive only, detection systems which were successful for Phases 2 through 5. While these four systems successfully detected test cases, the systems varied in their detectable parameters, location specificity, and implementation. One vendor, whose technology required a signed agreement with the Federal Communications Commission (FCC) demonstrated both detection and control technology and were able to successfully complete test Phases 2 – 6 and had specific intelligence gathering applications. The video at the following link provides an overview of the demonstration -- http://www.dpscs.state.md.us/media/Cell_phone_detection_flashvideo.shtml. In addition, the Department has DVDs, providing a full recording of each of the demonstrations, available for distribution.

CORRECTIONAL IMPLICATIONS AND ANALYSIS

Detection technology triangulates a cell phone signal and requires the use of correctional staff to physically search and seize the identified cell phone. This system works only when the phone is in the on position and varies based upon each company's technological abilities. Some used signal strength and were unable to differentiate the detected carrier or phone type. Others used a combination of signal strength and frequency with the ability to detect and differentiate both carrier and phone type. Three of the detection systems provided a graphical user interface depicting varying degrees of accuracy in terms of cell phone location. Some spoke of specific intelligence gathering applications associated with their specific solution.

The actual hardware associated with each of the demonstrations of detection technology varied. Some were hard wired, while others had wireless capabilities. The ability to locate cell phones was based upon a number of receiving antennas/receivers used in the implementation. Among the systems, antenna/receiver placement could be in pipe chases, wall mountings, outside the facility, on roofs, etc. Two of the detection technologies required network cable infrastructure to interconnect and power the antennas. Two of the systems used wireless technology to connect the antennas/receivers using either battery or external power – perfect for temporary usage and mobility, but requiring staff members to move and recharge equipment.

Control technology on the other hand, was able to "bend" or intercept a signal either allowing the call to go through or holding the call and indicating a "no signal" from the sender. This technology used a tower or "box" and did not rely upon receiver/antennas. The technology demonstrated several intelligence gathering abilities that could be implemented depending upon specific laws governing each state. Additionally, this type of technology could allow certain phones to operate and allow 911 calls to be processed.

RESULTS AND RECOMMENDATIONS

It is clear from the demonstrations that each state will have to identify their own specific needs. Specifically, the technology is such that one solution may not work for every facility within a given state. A combination may be better suited to control a specific type of institution or inmate security level. States should consider the following prior to preparing procurement requests:

- Do you want to completely stop all inmate cell phone communications and allow selected communications?
- Do you want to allow sporadic cell phone communications and detect, search for, and confiscate cell phones?
- Do you want to allow cell phone usage until a movable detection system is used to detect, search for, and confiscate cell phones?
- What types of intelligence capabilities are you concerned with?

The remaining decision point is one of cost. While our demonstration specifically avoided cost estimates, it is anticipated that the overall costs associated with each solution would vary and depend upon the specific needs of a correctional setting.

Detection systems may or may not require infrastructure. If wiring infrastructure is required there will be associated costs. Antennas/receivers are required and each has a cost and a life span plus associated maintenance and the consideration of inmate tampering. The number required will depend on the architecture of the facility and the desired cell detection location accuracy. Most detection systems require a PC and vendor software.

Control systems currently require an agreement between carriers and a vendor. Equipment and software are required to act as a cellular tower and process the calls.

The Department believes strongly that a combination of efforts will be necessary to prevent continued inmate cell phone use. Each prison is different, whether a result of its physical dimensions, location in either rural or urban centers, or the security level of inmates being housed. In addition, there is no definitive answer in terms of what implications jamming technology will have. Each state should consider an individual facility evaluation or seek a consultant based model to assist in identifying the best solution for the specific needs of its correctional system.