June 9, 2010

To: Mr. Richard J. Orsulak
Emergency Planning and Public Safety Division,
Office of Spectrum Management,
National Telecommunications and Information Administration,
U.S. Department of Commerce,
1212 New York Avenue, NW, Suite 600B,
Washington, DC 20005

Ph: (202) 482–9139
rorsulak@ntia.doc.gov

Re: BVS NOI Response: NTIA Seeks Comment on How to Prevent Contraband Cell Phone Use in Prisons

Dear Mr. Orsulak,

Please see the following PDF in response to NTIA's request for information on technical approaches to preventing contraband cell phone use in prisons. The following document Berkeley Varitronics Systems, Inc. (BVS) is providing may be utilized for public knowledge in efforts to effectively reduce contraband cell phone use in correctional facilities without interfering with 911 calls, first responders, or any commercial and public wireless services.

Best Regards,

Scott N. Schober
President/CEO
Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840

Ph: (732)-548-3737
email: **scott@bvsystems.com**
www.bvsystems.com

Berkeley Varitronics Systems (BVS) Comments on the NOI to Prevent Contraband Cell Phone Use

This document has been prepared in response to NTIA's Request for Comments (Federal Register/Vol.75, No. 91/Wednesday, May 12, 2010/Notices, pp 26735-26738) on a number of questions in order to assist in evaluating technology solutions to prevent contraband cell phone use in prisons. These comments have been provided in the same order, as follows:

TECHNOLOGIES OR APPROACHES:

Technologies for preventing *cell phone use in real-time* may be classified in terms of underlying strategies, namely:

a. jamming,

b. managed access

c. detection.

All three of these strategies are well-suited for stealthy implementation hence capable of preventing contraband cell phone use because they do not require the cell phone to be at very close range (i.e. within sight of the cell phone user) to be functional. Of these, jamming and managed access rely on active RF Transmissions to prevent access to the servicing Base Station (BS). Whereas, the third strategy relies on RF reception alone to detect and locate the cell phone use.

There are other strategies for locating active or inactive cell phones (such as the Non-Linear Junction Detection method) which are not well-suited for stealthy implementation because they typically require the cell phone to be literally next to the detector (within inches) to be functional, which consequently require excessive amounts of time to scan even limited amounts of space.

Table 1 provides a synopsis of the relative strengths and weaknesses of the above three strategies that are well suited for stealthy implementation (jamming, managed access and detection), toward the prevention of contraband cell phone use. Each strategy may be assessed in terms of "dimensions" deemed important by NTIA (leftmost column): [1]

Table 1. Synopsis of Relative Strengths and Weaknesses

	Jamming	**Managed Access**	**Detection**
Facility Constraints	problematic	no	no
Cost	high	high	attractive
Technical Feasibility	proven	proven	proven
Legal Issues	problematic	potentially problematic	no
Health Issues	may be problematic	unknown	no
Locating Source	no	no	yes
Denial of Service	indiscriminate	selective (un-proven)	by deterrence
Forensic Value	none	none	yes
Overall	problematic	expensive/uncertain	promising

Each of these dimensions is defined and evaluated for the three strategies considered by NTIA:

Facility Constraints: Inside buildings where masonry walls and lots of steel structures are pervasive, RF signals transmitted by cell phones will undergo relatively heavy attenuation and scattering before they diffuse out of the building boundaries (via windows, doors and other glassed apertures in walls) and are able to reach the nearest Base Station (BS). For the same reasons, RF signals originating from the BS will be relatively weak by the time they reach the interior spaces of the building where a cell phone is trying to establish a two-way link with the BS.

This condition will induce the cell phone to automatically raise its RF output power level to a much higher level than if the cell phone and BS were in direct line of sight at the same distance. *Hence, if the cell phone were able to establish contact with the BS at all, it would be much easier for it to be passively detected and located inside the building boundaries in the up-link channel(s).*

In the same situation, if one tried implementing jamming, *more* RF power would have to be pumped into the interior environment of the building to overshadow the multi-band RF link channels for air interface technologies (GSM, CDMA etc), which could be problematic in terms of system cost, technical feasibility, legal issues, health issues, etc. (see the other "dimensions" in Table 1 above). Another difficulty with jamming is that it cannot locate sources. Managed Access is not directly impacted by facility constraints because to be functional it would have to be located outside the boundaries of the building(s).

Another type of facility constraint has to do with the inability of installing power and signal cables and fixtures on exposed wall surfaces in the building(s) because

masonry will not allow it and any wall fixtures would be vulnerable to tampering and vandalism. This constraint seriously handicaps the jamming strategy, because the requirements of RF propagation for the jamming signals would not be satisfied if antennas could not be located (with lots of cabling for distributing RF throughout the building) at multiple key locations throughout the building, even assuming cost was no concern.

Cost Considerations: Given the facility constraints defined above, any distributed system hard-wired to the building walls and structures is sure to be costly. The Bloodhound product on the other hand, does not require an infrastructure, but being a hand-held device, each unit needs a dedicated operator. Independent of the method of detection, since contraband cell phones need to be located anyway, and the Bloodhound unit provides both functions, its cost is very attractive. Also, detection is the only strategy that allows implementation gradually, without requiring a massive "up-front" financial commitment.

Technical Feasibility: All three strategies in Table 1 have proven technical feasibility. However, given the heavy attenuation and scattering of RF signals in buildings with masonry walls and a lot of steel structures, it would be reasonable to expect considerable hardship in selectively maintaining a uniform level of RF jamming signal strength over large buildings with many small rooms. The fact that the jamming signal needs to be neutralized at certain parts of the building(s) where 911 and other legitimate communications services have to be maintained complicates the technical challenge considerably.

Legal Issues: Jamming and Managed Access use RF transmitters have to meet transmitter certification and other legal requirements. Detection on the other hand uses passive receivers for detecting signal strength level in up-link channels only, hence are not subject to the same requirements.

Health Issues: Jamming and Managed Access use RF transmitters deployed continuously, therefore they may raise concerns of exposing people to the risks of non-ionizing radiation. Detection on the other hand uses passive receivers for detecting signal strength level in up-link channels only, and are not subject to the same concerns.

Locating Source: Of the three strategies considered by NTIA, Detection is the only strategy that can have the capability to locate detected cell phones. In particular,

BVS' Bloodhound product has clearly demonstrated this capability. In a 'real world' situation, in mid-March Maryland Department of Public Safety and Correctional Facilities officials using The Bloodhound detected and located five smuggled cell phones during a two hour sweep of the cell blocks.

One of the hidden phones was in a hollowed out brick covered by a capstone in a low wall that separates bunks areas in a dormitory. The second was inside an electrical box that had been covered with a solid utility plate that was held in place with security screws.

Denial of Service: Jamming will interfere with the RF links between the serving BS and the cell phone as soon as it is activated. Managed Access will effectively filter out all unrecognized cell phone calls. Detection will deter cell phone use once the cell phone is detected or the user has the perception of the same.

Forensic Value: The information available from the SIM card has definite forensic value. When contraband cell phones are detected and located within the correctional facilities the value is what is in the phone (on the SIMM card). Mobile phone forensics is the science of recovering digital evidence that is inside a mobile phone. BVS has partnered with Teel Technologies* who are experts in performing mobile phone forensics on confiscated cell phones. The information that has been gathered, such as initiated threats on witnesses, drug information; gang related activities are essential to prosecute inmates that are conducting crimes out of their cells. As mobile phones continue to advance it is essential to utilize the advanced forensics software packages gather this critical evidence.

Jamming and Managed Access can effectively deny access to the serving BS but cannot positively locate cell phones; whereas Detection can locate and capture a phone which can subsequently be analyzed to extract data from the SIM card which every cell phone must have to be functional.

Devices and Frequency Bands

The Bloodhound sensor unit is a multi-band receiver controlled by an on-board processor to sequentially scan up-link channels for GSM, CDMA, WCDMA and PCS cell phone activity. The Bloodhound systematically covers all the bands of specific frequency allocated to cell phone signals including:

GSM: 890-915 MHz
CDMA: 824-849 MHz
WCDMA: 1920-1980 MHz
PCS: 1850-1910 MHz

Interference to Other Services

The only strategy which may be subject to this concern is Jamming. Given that in a building with masonry interior walls and pervasive steel structures it will be necessary to maintain relatively high levels of RF jamming energy, it is not clear how jamming would be selectively prevented from interfering with other legitimate communication services.

Regulatory/Legal Issues

Given that Jamming and Managed Access use active transmitters, these two strategies are subject to regulatory and legal issues. Whereas, Detection is not subject to same because a passive receiver is used only to detect signal strength in cell phone up-link channels of CDMA, GSM and W-CDMA bands.

Technical Issues

Jamming

The intentional 'jamming' of cell phones within correctional facilities at first sounds like a viable solution. However, we believe cell phone detection and location is a superior solution to the problem at hand for the following reasons;

1) Jamming is outright illegal. We support CTIA's stand as well as the FCC's position on the dangers of jamming.

2) Jamming can disrupt or interfere with legal wireless communications as well as 911 calls, police, fire, emergency response personnel and first responders.

3) Jamming can also interfere with cell broadcast communications that enable a government entity to transmit an emergency alert of natural or manmade disasters to every cell phone in a affected area, regardless of carrier.

4) Jamming can disrupt search and rescue operations where a cell phone signal may be the only means to locate trapped or missing individuals.

5) Many companies claim that they can 'control' the jamming, however keeping the RF energy selectively confined to an arbitrary floor space can be extremely complex and expensive. This is because there are multiple frequency bands and modulation techniques the jammer would have to address (i.e. Cellular, PCS, iDEN, CDMA, GSM, Wifi 2.4 GHz, 5.8 GHz, Bluetooth).

SUMMARY OF THE BVS APPROACH:

For 37 years BVS has been a leading provider of advanced wireless solutions and products to the domestic and international wireless telecommunications industry. Since 1986 BVS has designed and manufactured thousands of drive study solutions that were used for Cellular, iDEN, PCS, and more recently WiMAX cell tower build-outs In December 2009 the company announced the release of an advanced hand-held cell phone detector fittingly called The Bloodhound.

The Bloodhound cell phone detector enables security officers to scan real-time for unauthorized cell phone activity in correctional facilities and detect the precise location of the caller by using a Direction Finding Antenna. The Bloodhound was recognized as the leading product in the wireless security category at the 2010 GovSec Expo and Conference in Washington, D.C. in April.

The unique DF antenna/receiver combination of BVS' Bloodhound product delivers an assortment of accessories allowing security officers to 'sniff out' the RF energy as an actual Bloodhound can detect a scent, pursue it and find the source. When hunting down a cell phone, Bloodhound's proprietary algorithms embedded in firmware provide the user with an intuitive graphic presentation of the detected signal strength as a function of the user's azimuthal orientation. Thus, once a cell phone is detected, Bloodhound enables the user to progressively approach the source while making continuous small adjustments to his/her heading, till the cell phone is within arm's reach or closer.

The unit also has a headphone jack providing a progressive audible tone and an accompanying vibrator that can help a security officer to perceive not only of cell phone activity but also whether the source is getting near or getting away. The unit also drives a pulsating green laser with variable duty cycle to help the user make small adjustments in real-time while pointing the DF antenna to objects within sight but not necessarily within reach (such as a small opening in a door or a window at a higher level or from a distance for stealth operation). The duty cycle of the laser pulse and the frequency of the audible tone will increase as the detected signal magnitude increases, thereby empowering the user to actually become part of the locking mechanism in pursuing and locating a source.

More recently, BVS has also developed the stealthier and more affordable Wolfhound Lite product which can be carried in one's pocket or be deployed as a sensor to activate other devices such as still or video cameras.

Photo of Wolfhound Lite Cell Detector

Berkeley Varitronics Systems, Inc. will continue to provide technical guidance to the NTIA, the FCC, the Federal Bureau of Prisons and the National Institute of Justice. BVS is actively working with correctional facilities on the State and Federal levels to develop

effective technologies and methods toward finding and prosecuting inmates that are wrongfully brining contraband cell phones to the prisons. We are also closely working with the CTIA –The Wireless Association who are strong advocates against unauthorized jamming in correctional facilities.

Berkeley Varitronics Systems, Inc.
Liberty Corporate Park
255 Liberty Street
Metuchen, NJ 08840
- Clarifying RF -

Ph: (732)-548-3737
www. bvsystems.com

About Berkeley Varitronics Systems: Berkeley Varitronics Systems, located in Metuchen, New Jersey, has been providing advanced wireless solutions and products to the domestic and international wireless telecommunications industry for over 35 years. Since 1995, BVS has introduced over 50 unique wireless test devices for a variety of applications including the popular
Cellular, iDEN, PCS, CDMA, RFID, LTE, Mobile WiMAX, FIXED WiMAX, 802.11b/a/n/g & Bluetooth specifications. For more information visit www.bvsystems.com.

About Teel Technologies: Teel Technologies is today's leading supplier of Mobile Device Forensics solutions and services for local, state and federal law enforcement customers, as well as private forensic firms. www.teeltech.com.