Enterprise Electronics
22826 Mariposa Avenue
Torrance, CA 90502
Phone 310.534.4456 Fax 310.534.1233
www.EEonTheWeb.com **www.CellBusted.com**

Date: June 8, 2010

To: NTIA-DOC

Attn: Richard J. Orsulak

Response From: Robert L. Burchett C.E.

Re: Preventing Contraband Cell Phone Use in Prisons

Docket: 100504212-0212-01 Notice of Inquiry

Statement of qualifications to respond:

Robert Burchett is President of Enterpise Electronics serving the land mobile radio and cellular telephone community for 40+ years, a Certified Communications Engineer, Commercial Radiotelephone license holder and whose company has been actively engaged specifically in design, engineering and marketing of cell phone detection systems and related products since 1997 when cell phone detection was first introduced.

Enterprise Electronics has provided cell phone detection equipment during this period of time, consistently rejecting queries from manufacturers seeking retailers and marketing outlets for equally contraband jamming devices so as to remain in compliance with the Communications Act of 1934 as amended (the "Act") and referred to constantly in the NOI. The Act prohibits malicious and/ or intentional (willful) interference with radio signals.

Enterprise Electronics (EE) maintains a position consistent with the Federal Communications Commission (FCC), the National Telecommunications and Information Administration (NTIA), the Cellular Telephone Industry Association (CTIA), the Association of Public Safety Communications Officers (APCO) and many others that introducing a jamming component into even a so-called "controlled environment" such as a prison area does indeed violate the Act. We further maintain there can and should be absolutely no proper, legal nor wavier solution that works-around this fundamental protective doctrine for self-serving interests at the expense of others.

NTIA spent considerable time evaluating the issues as outlined in the six page detailed NOI docket and has arrived at the same conclusion the FCC, CTIA, APCO and the rest of the telecommunications industry are well aware of. The extensive text devoted to the problems vs. the potential benefits to be gained from the use of jamming equipment in any form by any manufacturer even under so-called "controlled-conditions" results in a magnitude of issues generated beyond the scope the vendors(s) are able to confine, rectify or work-around.

Testing of such equipment in prisons (conducted under protest by both CTIA and the FCC) resulted in more questions in the NOI than answers as are clearly outlined in the text.

Statement by Enterprise Electronics regarding jamming:

Jamming, even if permitted, results in a lose-lose situation whereas the vendor of the jamming product is the sole beneficiary of the outcome. Consider the following:

- Jammers are currently FCC unlicensed and uncertified transmitters and in order to make them have basic certification and/ or type acceptance/ approval the procedure expenses will surely increase the cost of the product making it at potentially cost-prohibitive to deploy.
- NTIA correctly brought out the obvious question that the uncontrolled and poorly managed radio signal coverage of jammers is not 100% under the best of circumstances especially indoors with varying building and construction models where no reliable computer propagation and RF penetration models currently exist.
- This means that unless overpowering RF signals are permitted to be used; then there will always be "dead spots" in the jamming coverage area where the contraband phones will immediately resume illegal activity.
- Jammers are radio transmitters required to operate at 100% capacity 100% of the time and as any engineer knows; if you operate any piece of electronic equipment at its maximum ratings then the Mean Time Between Failure (MTBF) is considerably shortened.
- The result is that any product designed to introduce willful and powerful interference into an environment must do so 24/ 7/ 365 without any possibility of failure least the inmate discover it and reinitiate use of their cell phone far faster than the system can be restored to full power and coverage.
- Jamming equipment does not offer a mechanism that alerts the facility owner/ operator that a failure of the signal generator has occurred and the first ones to be made aware of it will certainly be the inmates.
- Jamming does not locate, capture nor eliminate the problem from the prison environment; it simply renders the offending phone temporarily nonfunctional in certain areas during the time that the jamming equipment is 100% functional. The moment it breaks down, experiences lapses in coverage or suffers any temporary loss of signal output the contraband cell phones immediately commence to function and return to service.
- Inmates have nothing to do 24 hours a day but try and find ways to outwit and thwart such countermeasures while guards and other staff are tasked with many issues and concerns so inmates can find the elusive dead-spots in coverage and are well aware of failures in the jamming transmission when cellular service is restored.
- While it is off-topic, it is highly relevant that abduction and home-invasion criminals are known to use cell phone jammers to stop their intended victim(s) from calling 911 on their phones while commission of the crime is in progress. Permitting these illegal devices to continue to be imported into our country creates a constant threat to personal security as well as the NTIA issue at hand regarding prisons.
- Note that jammers are currently unlicensed and illegal transmitters of radio frequency energy that if ultimately permitted in any fashion or form factor will surely increase the technical burden upon the overtaxed FCC, NTIA and other regulation and supervisory authorities in a period of reduced staffing, income and economic uncertainty. NTIA must ask itself the obvious question if this is yet another unfunded congressional mandate burden that neither agency needs nor has the staff, equipment, facilities and time to certify, test and validate each device on the endless list of products.
- These offshore manufacturers (note that there are no domestic suppliers) of poorly built devices that Customs and Border Protection (CBP) intercepts at our ports constantly increase the workload of every department to contend with as it is and opening the floodgates of interfering products will only further prove that the FCC, CTIA and APCO were always right in their assertion that jamming does not provide even a small component of the solution to the issues faced.
- **Installation issues**: Placement of jamming equipment must be done in retrofit to existing facilities and scarce resources are available to support it. Each signal generator must have multiple antennas to support the frequencies jammed and they require substantial protection to keep inmates from damaging them once

their presence is known. Equipment housing installations must be done in a hardened and protected manner directly into the inmate environment. AC power must be supplied by the facility and this will cause substantial labor cost to be incurred by the installing contractor to core drill and run appropriate hardened conduit and cable raceways for power. These 'hidden' costs are in many cases far beyond the simple expense of the hardware jammer product itself and must be taken into account.

- **Legal implications**: Even a single incident of public safety being hampered, a doctor being unable to communicate to render life-saving aid or interrupting a prison radio systems coverage during tenuous times will result in legal costs far in excess of any potential (real or imagined) savings that jamming can be extrapolated to return.
- NTIA/ FCC/ Congress must be prepared to demand that the vendor/ manufacturer of the jamming equipment post a performance/ surety bond equal to the amount of expected litigation costs when legitimate users of wireless devices in any and all radio services (radio or cellular) are denied or prohibited access to their communications and commences lawsuit.
- Ultimately, ff there is any potential for approval of such devices then NTIA must demand that the manufacturer(s) agree to defend, indemnify and hold harmless the agency and all related governmental entities including but not limited to the prison system and local Dep't of Correction(s) of authority where deployed, US Government and all state, local and city officials in any action resulting from the deployment of their jamming devices at their sole expense to insure that the taxpayers are not saddled with this responsibility.
- NTIA/ FCC/ Congress must be prepared to demand that the vendor/ manufacturer of the jamming equipment post a performance/ surety/ insurance bond equal to the amount of expected litigation costs when legitimate users of wireless devices in any and all radio services (radio or cellular) are denied or prohibited access to their communications and commences lawsuit.
- Note that this remedy can only be deemed acceptable by their posting bond in advance so as to not permit them simple escape by bankruptcy or insolvency protection which will inevitably result when first confronted with any legal proceeding.

William Sill and Billy Layton who are partners in the law firm of Wilkinson, Barker and Knauer write in their well researched dissertation that:

"Jammers are illegal and dangerous. Given the serious public safety concerns over the widespread use of jamming devices, the FCC should make it clear through its actions and statements that the previous laissez-faire policy toward jammers is no longer the FCC's policy."

"Whether the purpose is to quiet cell phones in a church, theater or business; in one's personal space; or in a detention facility, the use of cell phone jammers in the United States is illegal."

Sill and Layton discuss that Senators Bailey Hutchinson and Jim DeMint introduce legislation to permit the FCC to grant waivers and have sent representatives to these highly protested jamming demonstration events. The authors point out that legislators rarely have the technical expertise to rule or pressure regulatory bodies (such as FCC and NTIA) into making strategically poor decisions based upon little real substantive information.

They further assert that the prior FCC chair passively granted (by lack of denial) use of cell phone jammers but that later policy makers reaffirmed their intent to maintain the full force and effect of The Act in forward proceedings.

Source: AGL Magazine June/ July 2009

Summary: Therefore Enterprise Electronics agrees with the opponents of and hereby contends that jamming is at best useless in that it merely masks the issue and does not eliminate the contraband cell phone from the prison allowing it to go back into operation with any lapse of interfering signal and at worst to generate potentially harmful interference. We further note that NTIA, FCC, CTIA and APCO are absolutely correct in being highly concerned with and openly opposed to the possibility of introducing these harmful and illegal devices into the US environment.

Statement regarding Managed Access:

On the surface; the Managed Access (MA) methodology seems to be a reasonable and prudent way of dealing with the issue; simply listen to everything and route it according to its grant-or-deny table. While appearing noble, this is a very expensive way to attempt to manage the issue and will result in essentially the same end-result as jamming; here is why.

The NTIA discussion against jamming works properly in reverse: the MA receiving signal coverage area must also be contained solely within the prison walls just as it is incumbent upon jamming in order to make even the most fundamental of cases. Further; MA receiving coverage must not extend beyond it any more than jamming coverage can be permitted otherwise if a casual passerby, worker, visitor or nearby resident attempts to use their lawfully permitted wireless device they will be categorically denied service due to not being previously allowed in the "grant of service" table in the MA machine.

Questions and issues relating to MA devices:

Varying power may render their method moot: The first issue of concern is the RF power output of the cell phones that the MA devices must listen to. NTIA is aware that cellular networks transmit commands via the control channel to the handsets requiring them to increase or decrease their transmit power as the system demands it. This varying power level depends upon many factors including the distance the caller is from each of the wireless networks closest cell site to the facility plus other variables clearly not able to be taken into account by the MA device.

Since the power output of the cell phone varies constantly under control of the Mobile Telephone Switching Office (MTSO) how does the manufacturer of the MA devices determine the internal coverage 100% of the time since they must HEAR only phones inside of their specified coverage area that it listens to and EXCLUDE hearing legal phones outside of their well defined listening zone? The clear answer is that they cannot guarantee that they will hear all transmissions from varying locations while listening from fixed stations. The MA device cannot be deployed in a mobile or variable manner and since inmates can wander about the premises to seek coverage dead spots in which to hide the MA device cannot follow them.

MA products are not permitted to radiate a signal to the offending cell phone as they are burdened by the same rules that govern jammers; therefore they can only route or not-route a call based upon the rights table. Further, they cannot tell the cell phone to transmit with a specific power level to permit them to be established receivers of fixed-level signals as they have no access to the MTSO control channel data stream.

Since the MA vendor cannot guarantee 100% coverage of ONLY the prison building and property with no 'reverse leakage" or outside-the-building coverage or disruption of service to legal phones then the potential for hearing a legal phone outside of their permitted and well-defined protected zone (prison walls, fences, borders, property line, etc.) appears quite high and this raises questions that may well be unanswerable due to the RF power not being under the control of the MA product manufacturer.

The following are questions and issues not answered in the NTIA text and dissertation and, while not necessary for EE to make a statement regarding the fitness or suitability of their products, NTIA and any potential purchaser of such products would do well to present these issues to the MA vendor(s) and take their answers into account.

Operator alerting question: These products utilize "negative logic" defined as everyone heard talking on a phone inside of the defined prison zone of protection is presumed to be an inmate at the onset and denied service until they are so granted by the MA device. By their statement, all calls are intercepted and while monitoring them is not this issue; the negative logic employed creates additional questions. Once installed, any system creates dependency upon it by the facility that deploys it. Certainly they can't guarantee 100% up-time with zero possibility of failure, then how does the system alert the facility owner/ operator to the failure event?

Backup/ contingency plan question: When failure occurs in the MA system, what is their backup/ contingency plan to render contraband cell phones useless while granting permitted phones service?

Failure method question: When the MA device fails (as all do eventually) does the unit "fail hard" and deny 100% of service to both legal and illegal phones during such computer program failure or does it "fail soft" by granting access to both? NTIA and potential purchasers must know the outcome since neither of them appear to be positive logic or reaction to the event.

911 contacting issue: One of their selling features is that supposedly 911 calls are permitted by the MA device even from cell phones not in the rights-granted partition of the table and again this seems noble but it has an inherent flaw. Inmates have no regard for the law which is why they are there in the first place and they already willfully violate the law by harboring a concealed contraband cell phone as further proof of their disregard for it. Expecting them to respect the law regarding frivolous contact with 911 is absurd. When inmates are granted free use of calling 911 all they want then this is exactly what they will do.

The 911 operator PSAP system does not need nor want the added burden of inmates flooding them with crank and frivolous "emergency" calls to report bogus issues, create false and misleading reports of crimes-in-progress and cause law enforcement trouble for their own amusement and retaliation purposes.

NTIA correctly states that while MA systems have the ability to sense and ignore 911 calls (granting them access) while detection technology does not interfere with them; they are properly concerned that legitimate 911 calling not be interfered with.

EE believes that inmates are not a positive 911 event reporting source of reliable information and should not be granted access to this most important of services. The only proper way to grant legitimate access to 911 and deny it to inmates is to locate and remove their contraband cell phones from the facility; not to mask and selectively grant access to some of them at great expense to taxpayers that get the bill.

Hold-Harmless question: As in the event of the jamming device vendor; is the MA vendor prepared to offer NTIA and FCC a performance/ surety bond in-advance equal to the costs of expected litigation when their equipment denies legitimate wireless subscribers the right to use their device?

Cellular telephone carriers, as NTIA correctly points out, constantly change radio frequencies deployed, power levels, formats (GSM, CDMA, IDEN and in the near future LTE) so the costs of constant upgrade, maintenance, changing of software and hardware to keep up with the varying product will inevitably place the

purchasing facility into a budget crisis. Many states (such as California) are in the middle of an immense prison budget shortfall and purchasing expensive-to-deploy systems such as this with inordinately high upkeep, upgrade and updating maintenance costs forever makes even the best of these products appear to be a very poor choice to resolve the issue at hand. The cost may well outweigh the benefits.

As previously noted; inmates have all the time in the world to outwit these devices, find their "dead zones" and be a perfect moving target eluding capture and positive removal of the phone from the facility which EE maintains is still the only acceptable end result.

Summary: MA devices, in a manner consistent with jamming products, fail to remove the offending cell phone from the facility. This has the undesired effect of leaving the inmate with the contraband phone that might not be permitted to work on Monday in a particular area but suddenly operate on Tuesday in that same location due to changing coverage patterns or perhaps failure of the MA product. In either case; the facility is out a lot of money spent and the inmate uses their phone unmolested.

Statement regarding detection, location, capture and elimination:

Enterprise Electronics with more than 10 years of experience in working specifically with cell phone detection methods is well qualified to provide evidence and information in this particular field. Detection has and will continue to be our sole method of remediation of the contraband cell phone issue.

Detection, location, capture and ultimately elimination of the contraband cell phone from the prison environment is the only real acceptable outcome. Anything less is simply masking the issue while leaving the phone in the hands of a potential enemy and neither NTIA nor Bureau of Prisons should accept less than this.

This method violates no laws, causes no known problems or side-effects, has none of the prior related issues, creates no interference or difficulties with litigation as the outcome and has no toxic failure modes that will be introduced into the already hostile prison environment. Most everyone is aware that there are also active methods of detection of contraband devices. Enterprise Electronics sells all of these and more so we are very familiar with them.

Here is a summary of active locators along with pro and con arguments:

Metal detectors; actively transmit a magnetic field which the contraband items interrupt the field and alert the operator to the detection event. Location is done by LED lights and indicators and instantly alerts operators. **Plus**: detects inanimate metallic objects and cell phones even while turned OFF. **Minus**: can be construed as labor intensive as it requires an operator for constant monitoring and detection is limited in scope as the inmate must pass between the bars or the unit will not detect the event.

Body Scanning Detectors: These devices are an active offshoot of the metal detector family and are also magnetometers that work the same way walk-thru, handheld, underground and in-bedding sweepers work as outlined above except the signal is concentrated to penetrate the body cavity specifically. **Plus**: locates contraband hidden inside of the human body; practically nothing else will do this job and it appears to have no competitor. **Minus:** large, cumbersome and expensive; requires individual inmate attention by an operator, inmate is seated in the "chair" apparatus and multiple magnetometers scan the body for contraband. These units are not easily deployed or transported to the scene where inmates might be harboring contraband but still provide a very useful and highly accurate method of checking inmates on arrival for ingested contraband.

This from the distributor website:

Body Cavity searches are the most invasive and the new BOSS makes it fast and easy without disrobing. Concealing weapons or contraband in body cavities is a constant threat in many facilities and loss prevention by this method is one of the most difficult to detect. The BOSS is the complete answer.

Source: http://www.eeontheweb.com/Body%20Orfice%20Metal%20Detectors.htm

Non-linear junction detection: actively sends signals similar to the way that metal detectors work in that they hunt for semiconductor junctions (integrated circuits, transistors, diodes, etc.) **Plus**: does not generate cell phone interfering signals, has no illegal side-effects, finds phones and other illegal items (such as IPODs, CD players or other unapproved electronic devices) when turned off and hidden in inmate bedding or laundry piles. **Minus:** sends a radio signal invasive to people so is not recommended to sweep the human body, is a large type hand-carried detector (resembles in-ground metal/ treasure hunter detectors) and cannot be deployed in the open area to detect presence of phones.

This from the manufacturer website:

ORION (The Great Hunter) provides the capability to detect hidden electronic devices, regardless of whether the device is radiating, hard wired, or even turned on at all! ORION is the latest advancement in Non-linear Junction Detection and evaluation for Countersurveillance.

Source: http://www.reiusa.net/cgi-bin/main.cgi?action=viewprod&ct=products&pct=ORION&num=NJE-4000

X-Ray Radiation Scanners: Extensively used for baggage and packages. **Plus**: excellent imaging and in-depth penetration capability, imaging technology is well developed and in use worldwide, able to discern between types of contraband, etc. **Minus**: very expensive, inability to be deployed in the prison environment cannot be used to check human body due to radiation issues that are well known, expensive, limited to cargo, baggage and packages. Labor intensive in that serious management of the device is a requisite along with considerable training and precautionary measures.

Note that in the examples above that all are ACTIVE generators of signals (magnetic, high-energy photons or radio) that are employed to pass through, 'ping' or return indication of contraband items. Each has pro and con values and arguments for and against their use. These devices are common and popular for induction screening upon arrival and work well. Training is minimal for the most part and the units are well developed to alert operators with easy-to-learn knowledge required.

Passive/ listen-only detection is our specialty: This product line fills the void created by having to send signals into a confined area which requires operator attendance which are by design and operation very labor intensive. Passive detection technology works well in the prison and related environments, to open the discussion first we define how they work:

Passive "listen-only" Detection relies upon the five conditions under which cell phones send out radio signals which may then be detected:

1. Inmate calls out
2. Inmate receives call
3. Inmate sends text message
4. Inmate receives text message

5. The inmate phone registers on the cellular network

The first 4 are the most common and when the phone is transmitting are easily spotted by correctly designed passive detection systems in that the transmitter is engaged and will most likely send more than one burst of data, often at or near full power (in the case of texting or initial transmission but this is not necessarily always so).

The 5th mode of transmission is the registration burst, often referred to as 'pinging' the network. This is a transmission based upon somewhat random timing algorithms in the cell phone operating system and is not under inmate/ user control. It is not possible for the detection system to accurately predict when these will occur and this introduces minor ambiguity into the detection process which must be taken into account.

All passive listener-detectors have some points in common;

- The cell phone must be at least turned ON to locate them for the registration burst to be emitted
- The Detection System must be introduced into the environment prior to the phone; this is due to the fact that inmates do not leave their phones normally powered-up as the battery life is quite short and they are rarely afforded the luxury of recharging stations.
- Inmates turn their phone on, make a call (or send text message) and then quickly turn it off to save battery life and therefore any listening detection system must be constantly vigilant to these short transmissions.
- Registration bursts are one way of detecting these phones but in reality this can be discounted to nearly zero value in the prison environment due to the phones only being on for short periods and not presenting the detector with opportunity to pickup the random signals of the registrations.
- This leaves the primary 4 sources of signal for these detectors to hear and report their existence.
- Listener detectors report collected data back to their responders base of operation and so there has to be some carrier be it wired or wireless to alert the guard/ responder dispatch station to the event
- Power supply to the detector location will be required in some form AC or DC and this will need to be provided by either the manufacturer of the detector in the form of self-contained (battery) operation or AC provided by the facility infrastructure.
- When the inmate presses the **<send>** key the signal is detected and the listener device forwards the alert to the responding system.

At this point there are differing systems in the marketplace and they are described here.

1. Triangulation/ Pinpointing location
2. Multiple detectors with omni directional antennas set to receive in a fixed pickup zone without triangulation

Type 1 systems have many positive features; they are relatively precise, indicate on GUI defined maps or other software programs to present the location to the responders and then report to print or other email alerting and computer/ Internet/ LAN notification methods. Clearly these are the premier system on the market when discussing detection and location and they, like all other "listener" systems do not violate any laws nor subject the facility to potential litigation issues.

This is an excerpt from the manufacturer website regarding one such product:

Cell Hound® detects and locates all active cell phones located within or near a facility. The system utilizes an array of sensors that listen for cell phone activity. When a cellular call is detected, information about the call is transmitted via a standard Ethernet LAN to the central server. The data is processed in real-time by the software, which then displays the location of the cell phone onto a computer monitor.

Source: http://iiw.itt.com/products/cellHound/prodCell.shtml

The negative concerns are: that they require substantial infrastructure support with LAN wire cabling and power supply at remote antenna/ pickup points which are often nearly impossible to provision in a retrofit application. Were they to be specified upon design and buildout of a new prison facility this would not be as much of an issue; but the "NIMBY" (Not In My Back Yard) syndrome plus expense of construction makes new prisons harder to site and construct now more than ever.

The hardware consists of computers running single-platform proprietary programs which require substantial processor capability, space for monitors & keyboards in often overcrowded and confined responder locations and these units must be supported with extensive UPS and power management to insure clean energy as the computers do not care for power interruptions, spikes or transients.

Frequency, band and format implications: Type 1 systems by design have multiple frequency band and format detectors in them that do substantial analysis so they are sensitive to these differences. This means that when carriers change their frequency, band, format, waveform or power levels that these detection systems (like the MA product) must reactively follow with software and hardware upgrades.

These systems are so well developed and software, hardware and labor intensive to install that they are nearly 100% cost prohibitive to deploy in the current economic state. Common pricing for a medium facility to be retrofitted is reported to be in the 6 to 7 figures range.

This statement appeared in an October 2006 NPR article regarding price:

Source: http://www.npr.org/templates/story/story.php?storyId=6248833

EDO's system is one of only two that are commercially available. The systems can cost several hundred thousand dollars per prison. But as cell phones get smaller and harder to trace, prison officials may have few other options.

Alerting methods for these complex systems is reportedly to email, monitor video and audio .wav or .mp3 types of files to audibly notify the operators to an event.

Type 2 systems have their share of both sides as well; on the plus side are ease of installation requiring little or no infrastructure support in nearly all cases (no LAN wiring or cabling) as they carry their alert signal back over VHF or UHF radio channels. Installation of the remote detectors consists primarily of drilling holes in a wall for 4 anchor bolts and mounting it to a wall. The base responder consists of a common AC powered base station radio listening to the carrier channel and a selective decoder that responds to the special encoder that is contained in the detector.

How they work: These systems are near-field cell phone signal detectors that are spaced far enough apart to distinguish one area from another and close enough together to form a grid or pickup coverage sensitive area that can narrow up the search to a few inmate cells. Near-field RF sensing detection is nearly format-agnostic and can be broadband listeners to provide a high degree of service without having to deploy several receivers with separate antennas or different detectors which raise the cost.

What they look like: One type of device EE offers is the Hidden In Plain Sight (H.I.P.S.) units as they are built into common highly-visible radio call boxes and are considered "covert" while other models are clearly overt. Being highly visible and overtly obvious with multiple antennas, etc. and perhaps even marked accordingly, the mere installation and presence of these along with appropriate signage may well be a deterrent in and of itself.

Both of these methodologies can be seen at this link:
http://www.eeontheweb.com/Prisons%20and%20Jails.htm

How they report back: The responding base location(s) can be a single receiving station in the central dispatch or in some cases direct to the responder. As inexpensive to deploy VHF or UHF radio channels are used, often the detention facility already employs radios that utilize them to communicate with guards and staff. This means the detector system can also be setup to alert direct-to-responder when proper site-code decoding is available in the existing 2-way radios.

Use of this method cuts out the time spent to alert the guard station who in turn must then alert the guards. Speed of response is everything and if a cell phone is detected in an area the sooner that a responder can arrive, locate and confiscate it the threat is neutralized and ultimately eliminated from the facility.

Pro and con aspects: All systems have their two sides to the discussion and it can be easily debated how the positives of this system outweigh the negatives this way.

- **Argument:** Near-field energy detectors are capable of hearing 2-way radios used by the guards or put another way; lacking expensive and complex processing algorithms to discern the difference they are open to mistakenly detect the guards as well. This is especially true of radios in the 800-900 MHz range which federal prisons use extensively.
- **Response:** EE developed products contain filtering to help resolve this issue. Filtering works well in frequencies below 700 MHz to attenuate the VHF and UHF ranges (150-512 MHz bands) popular with state and local facilities but EE is aware that it leaves the 800-950 MHz band which is shared with cellular carriers open to near-field detection by accident. We believe that the method to deal with this is not to throw money at the problem by increasing the cost to the point of being prohibitive but to educate the guards to simply not transmit as often near the obvious detectors spaced around the facility. This is enhanced by use of resources (like cameras) to see if a guard is near an alerting detector and simply ignore the false positive.
- **Argument:** These units need to have batteries (typically size D alkaline cells) changed out by maintenance crew/ staff periodically increasing their workload.
- **Response:** Mean time between battery replacement varies with the amount of alternate use the units get. These radio call boxes offer 3 valuable services; inmate-intercom (used to communicate with the responders) a remote-listening method (dispatch operators can signal the call box to open the microphone and listen in to the area) as well as provide cell phone detection in the area. The call box operations are timed in that when you push the Push To Talk button the battery starts being used and then times-out after a previously determined programmable time (typically 10 seconds). If the dispatcher signals the call box to engage the transmitter to listen-in remotely in surveillance mode then the current draw goes up as well and

uses the batteries more. The cell phone detector runs all the time in a very low-current mode and if used by itself (probably unlikely) will require that the alkaline D size batteries be changed about every 60-90 days.

These call boxes can be operated from an AC power source if one is readily available with an internal power supply so if the location permits it then facility power is certainly an excellent option to use.

EE believes that the expense of changing out batteries which may be purchased in bulk at competitive low rates will more than save the facility the cost of providing AC power sourcing to inaccessible areas where drilling and conduit installation would make the cost to deploy highly prohibitive.

Handheld portable cell phone detection:

The alternative to fixed location detection is handheld/ portable use deployed by the officers or responders. These units are battery operated and being hand-carried can be brought to the scene of the contraband phone, detected and captured. Like the fixed operation units; they locate and eliminate the cell phones from the environment vs. masking and jamming.

One manufacturer makes two versions called the Bloodhound and Wolfhound; this from their website:

Bloodhound Cell Detector™ is a handheld, wireless sniffer specifically tuned to the RF signature of common cell phones including PCS, CDMA / WCDMA, GSM and Cellular bands (specify North American or European/Asian model). Bloodhound Cell Detector's high speed scanning receiver utilizes a multi-band DF (Direction Finding) antenna system allowing security personnel to locate all nearby cell phones in either standby mode or actively using voice, text (SMS) or data transmissions making it the perfect tool for enforcing your NO WIRELESS security policy in universities, government & military installations, hospitals, law enforcement agencies, financial institutions and prisons & correctional facilties. Instead of blanket, no-wireless jam signals (which are illegal and unsafe in many instances), Bloodhound Cell Detector prevents wireless usage by detecting and even locating the perpetrator.

Another group of portable/ handheld detectors can be found at this website:

http://www.eeontheweb.com/handheld_&_portable_detectors.htm

This from the website:

CELLBUSTED UNIT FINDS THOSE ELUSIVE CELL PHONES AND SHOWS THE RELATIVE SIGNAL STRENGTH AS YOU GET CLOSER. FEATURES A SILENT ALERT VIA EARPIECE (SUPPLIED) AND HAS RECHARGEABLE BATTERIES & CHARGER

Pros and cons of handheld devices: On the plus side, handheld detectors have the positive effect of lower cost-to-deploy in terms of purchase price while the argument to this is that they remain labor-intensive requiring cash-strapped state and local prison systems to have fewer responders doing more "cell phone sweeps" with guards carrying the device room-to-room.

With the requirement that the detector be brought to the source of the signal, this relies upon the inmate being brazen enough to use their phone in "detection view" of the guard carrying it. Clearly this happens often enough to make handheld units pay their way today; but once inmates get to know when guards approach to simply turn it off these units will diminish somewhat in value.

Their lower cost to deploy in the onset makes them appear highly attractive and the "something is better than nothing" approach is something to be considered when sourcing a solution that can have many facets. They are certainly part of the overall solution but most likely not all of it.

The commercial cell phone detection marketplace does not lack for product and technical expertise as can be clearly shown by the multiple products shown on these websites. Any cost-to-benefit analysis would be remiss in leaving out the capabilities of detection and capture when evaluating what the industry has to offer.

The mere fact that most prisons have little or no cell phone countermeasure products in place today fosters an environment where currently the inmates are obviously in control of the situation. Therefore even the most rudimentary detection and capture technique needs to be implemented nationwide and this immediately brings up the cost issue where the vendor for jamming product appears to have artificially created an "our product costs less" mentality in the legislature and media.

Cost to benefit analysis and consideration:

NTIA, FCC, APCO and many others including this author believe that even if jamming technology were to be deemed the lowest cost-to-purchase methodology in any particular facility that the long run results, expenses and poor-to-negligible results do not make it cost effective when examined by competent thinkers.

Consider that all jamming products are currently illegal in the USA which forces all manufacturing and subsequent purchasing of product to pay offshore vendors and this has several negative effects considering the state of our own economy:

- The "Buy American" clauses that are in many government contracts and bids must be 100% negated by statements that no domestic provider exists and this fact alone should give any prospective buyer pause
- As there is no domestic provider of jamming product there is no American source to offer competitive manufacturing or bidding
- Repairs, maintenance and replacement parts have an Asian supply line for the most part and product longevity is not their primary design criteria
- As with most cell phones; the life expectancy of these and similar products is in the order of 18 to 24 months with "discard rather than repair" mentality built into the design fostered by zero parts availability which renders routine maintenance and upkeep moot
- Purchasing of these products with sole-sourcing offshore eliminates jobs for American workers

Since jamming product is solely made by offshore manufacturers it can be argued that the purchasing cost will be relatively low at the onset due to lower manufacturing expense vs. a domestic product but when you factor in the results the outcome changes dramatically.

Failure to remove the device from the facility is the primary cost in that when (not IF) the jamming device fails the inmates proceed with business as usual with zero implications. This makes the cost factor moot when the money has been spent and the results are negated by bad design, early failure and zero parts availability.

Both the jamming and MA solutions work under the premise of spend the money now and when it fails they are powerless to prevent the calls since the phones still exist inside. Detection on the other hand, works in an entirely different manner with the end result that the phone is removed from the premises and so the cost analysis must take into account the onset cost-to-deploy and ongoing maintenance and upgrade expenses.

One method of detection & capture is the "call box" or inmate-intercom system that is a rapid deployment "instant installation" product that can be delivered and working in a matter of hours. Taking into account the wireless (VHF/ UHF radio) reporting detection system requires minimal installation and zero infrastructure burdens, EE feels this is a major plus gained by not requiring complex and expensive cabling and infrastructure the labor costs to install such a system approach zero. This is due to the fact the facility maintenance staff can attach the detectors to the building and walk away.

While it is true that this method does not 'triangulate' the offending signal to a single-inmate or room, the cost-to-deploy and thereby raise the detection standard is minimized and made affordable so the facility gets a system they would have been otherwise economically prohibited from purchasing.

The legislative and Bureau of Prisons administration did not provide cost-analysis of the products on the market to determine what the differential was between jamming, MA and detection methodologies in the NTIA Request For Comment. This author believes that properly engineered detection and elimination solutions can be highly cost competitive to even the most reasonably priced jamming equipment solution when deployed in a reliable manner using available off-the-shelf product.

EE believes that if you can't afford the product then it doesn't matter how good or capable it is; with this in mind there is real necessity to minimize purchase, installation, deployment as well as ongoing maintenance, upkeep and upgrade costs for the future for any solution provided by any vendor. All of these must be taken into account when seeking a solution otherwise the hidden expenses far outweighs the short-term benefits if there are any to be had. Consistently detecting, capturing and eliminating even a few cell phones from the facility on a regular basis will cause word to spread that this facility is "cell phone hostile". This combined with the stiffening penalties being imposed upon inmates that are caught with them will reduce the problem by several orders of magnitude.

In California; State Senator John Beloit has introduced legislation to increase the inmate penalty from 30 to 90 days of loss-of-credit for good behavior if caught with a cell phone and this is not an isolated event as many other states follow suit. Both components of the total solution must be implemented across the board for a favorable outcome to be expected.

Conclusions:

The least expensive system on the market today with the most return on investment, low long-term costs and minimal-to-nonexistent upgrade mandates is by far the simple near-field detection and capture method.

NTIA and BOP/ DOC would do well to fund projects that use developed products using off-the-shelf American made technology that poses zero litigation risk with the maximum return on investment in terms of eliminating the threat from the facilities.

Once the word spreads within a prison that the facility is 'cell phone hostile' then the proliferation problem will be self-solving, but this will take time and only capture of the phones with the users will fully resolve the complex issue.

Robert L. "Bob" Burchett C.E.
Enterpise Electronics
www.CellBusted.com