ITT Response to NTIA Contraband Questions

Engineered for life

Introduction

The threat of contraband cell phones in prisons is not new. It has been a significant problem for the past seven or eight years, and is an ever increasing problem for corrections administrators. Cell phones in the hands of inmates have proven to be a threat to other inmates and staff, as well as the public at large.

While all prison contraband poses a threat, cell phones have proven over time to be the most lethal contraband an inmate can acquire.

ITT has been working with several state Departments of Corrections (DOC) and the Federal Bureau of Prisons (FBOP) over the past six years to address the issue.

Six years ago the contraband cell phone issue was raised as a threat by personnel in the Office of Security Technology at FBOP, the National Institute of Technology (NIJ), the North East Technology Council, and DOC's in Pennsylvania, Virginia, South Carolina, and California.

For the first three years, the cell phone problem primarily concerned technologists from the various organizations responding to input from security staff who were encountering the problem on a daily basis. On the frontline of the problem, corrections officers could see that it was a growing threat, but lacked two essential ingredients to address the problem. The first was a workable technical solution and the second was recognition by prison administration of the magnitude of the problem. Many state administrators were still denying they even had a problem while the security personnel were telling a totally different story.

Phones have become easier to introduce into prisons, passing through metal detectors without detection. Their small size has made them easy to conceal and now the wristwatch cell phone can get overlooked by screeners. Equally disturbing, the SIM cards, which can be used interchangeably on most cell phones, are smaller than a postage stamp.

Over the past two years several widely reported incidents involving threats to high profile individuals and, in at least one case contributing to the loss of life, have raised public awareness of the cell phone threat. They prompted some prison administrators to take a high profile role in addressing the threat and the public demand for a solution. Several companies, including ITT Corporation, had detection solutions on the market which were proving themselves in several prisons. However, even as these solutions have proven worthy of further study, prison budgets came under extreme pressure in the recession. Even if prisons wanted to purchase an available solution, funding was not available, causing further delays in implementing solutions.

During the latest round of the technology study, several technologies were proposed: jamming, managed access systems, and detection.

Jamming is currently prohibited by the Federal Communications Act of 1934. The law prohibiting prisons from jamming became the public poster child, and the Safe Prisons Communications Act of 2009 was introduced to allow corrections institutions to use jamming to block contraband cell phone signals. Jamming was portrayed as a simpler and more cost-effective solution to the problem. While passed by the U.S. Senate, to date the House has yet to address the issue, so jamming remains illegal. Those advocates who claim that a jamming system will render all cell phones useless need to investigate why New Zealand recently abandoned their two-year trial after spending $5 million dollars.[1]

ITT is the U.S.'s largest developer and manufacturer of jamming equipment. We evaluated how a prison jamming solution might be implemented. Jamming can be accomplished in one of two primary ways. One is a single high power transmitter with sufficient power to overcome the fringes of the jammed area, ensuring coverage aided by directional antenna. The second type of system is more complicated, but might be able to overcome some of the interference to phones outside the prison associated with the first configuration. In the second method, an array of jammers, each transmitting at low power and distributing the jamming power over the area of interest, would be deployed.

The current Senate bill, as written, may preclude the first solution except for prisons in the most remote locations where cell phone coverage might be weak in the first place and passersby few.

Even with distributed jamming it is likely that there will be blind spots, areas where it might be possible to make a call. To remove the majority of blind spots would require extensive RF surveys after installation, which would add to the costs and require adjustments to the deployment to cover areas outside the jamming envelope, followed by a new round of surveys to confirm coverage.

Both jamming systems and managed access systems will require a number of fail safe triggers to deactivate jamming during an emergency or detected interference. The jamming system must be connected via some interface to all onsite emergency systems such as fire or other emergency systems. The lack of such an interrupt might prevent first responders and prison staff from using cell phones to communicate during an emergency. An external or remote emergency off button that disables the jamming or managed access system in the event of a fire or some other emergency must be capable of deactivating the system much like the elevator keys used by fire departments. The distributed jamming array with all of the fail-safe requirements could make a viable jamming system unaffordable.

Managed access systems have the potential to yield additional intelligence beyond what a detection system can provide. The ability to gather intelligence, by whatever method, improves the security staff's ability to develop a prison threat picture. Gaining access to the phone numbers or even intercepting the calls could produce valuable information for the security staff. An added

[1] http://www.stuff.co.nz/dominion-post/national/3568020/Prison-cellphone-jammers-fail

benefit to managed access is that the system will allow authorized staff to carry cell phones and use them, while jamming would block both licit and illicit use of cell phones.

While managed access systems have the potential to provide security with additional intelligence, they have a downside as well. First, managed access and jamming are "all or nothing" systems. That is, they have to be installed all at once around the prison, whereas detection can be deployed incrementally or only in certain high threat areas of the prison. Therefore, centralized jamming and managed access have high initial cost compared to detection systems and require more RF survey work. Additionally, they need to be monitored on an ongoing basis. Detection systems tend to have better location accuracy than managed access systems, particularly indoors. Manage access systems need to determine how and when to deny service to a cell phone. For example, if a person is making a call from the employee or visitor parking lot adjacent to a housing unit and the phone's GPS is turned off, a call could be denied even though it is legitimate because of the system location resolution accuracy.

Because RF detection systems do not interfere with any communication system, including cellular traffic, all options that transmit or intercept must be able to have very defined boundaries.

It is likely that in individual cases the application of one system will have an advantage over the others. However, there is only one way to ensure no interference is produced and that is not to transmit any power. Detection systems are the only current solution that meets that criterion.

When it comes to system evaluation, there should be a very clear list of criteria to which these systems must comply. It is strongly recommend that a diverse panel of correction practitioners (federal, state, and local) be convened for the purpose of developing and documenting an operational requirements document independent of the technology. The requirements document should include expectations for allowable operational complexity, dependence on the supplying vendor, permissible costs, and maintenance expectations. This information can form the basis of an evaluation checklist. Secondly, the federal government should issue clear guidelines as to the data or information which it is or is not permissible to collect on inmate conversations collected by these systems. Third, we suggest that the Department of Health and Human Services issue guidelines for permissible levels of continuous radiated RF energy to which an inmate or staff member can be exposed.

Following are the answers to the questions asked by the National Telecommunications and Information Administration.

Questions and Responses

Technologies or Approaches

Jamming, Managed Access and Detection, are these characterizations accurate and complete?

They are the most popular methods currently discussed or implemented. RF paint and window coverings are other methods but are extremely expensive and not very effective, but are potential options for in-building protection.

Are there technologies other than these categories, and if so, how do they work?

The paint and window coverings are intended to act as a faraday cage or screen room preventing the transmission of RF energy. The problem with them as a solution is that they would also prevent the officers' radios from working as well unless repeaters were placed everywhere a radio was to be used.

What approaches can be taken to jam within irregular structures such as prisons, within indoor and outdoor areas, and within rural versus urban settings?

The Senate bill, as written, requires the jamming source to transmit the minimum amount of power required to overcome the cellular network's transmitted power. A jammer with a single antenna must transmit sufficient energy to reach the boundaries of the intended coverage area. In order to comply with the bill, the solution would require an array of transmitting antennas to distribute the power more evenly over the jammed area. An array of antennas which distributes the power more evenly may be the only solution that even comes close to working in non-rural areas. Distributed antennas or transmitting sources may be the only viable solution for irregular shaped buildings.

What specific types of managed access and detection techniques are available?

- Pico-cell
- Up and coming femtocell technology
- Incumbent carrier "black-listing"

What risk does each system pose to legitimate cell phone use by the general public outside the prison?

Detection poses no risk because it does not intercept or transmit RF power. Managed access could deny legitimate use if improperly configured or managed. Again, the issue with managed access is getting the location accuracy to discriminate between phones in close proximity. Jamming, of course, will prevent all cell phone use in the covered areas and maybe beyond the covered area.

What risk does each system pose to public safety and government use of spectrum?

Jamming poses the greatest risk if a complete solution is implemented, which would include all cell phone bands in North America. Aside from the obvious interference with the surrounding areas, any jamming system could interfere with first responders and others that use cell phones as a communication device during an emergency. The current iDEN band having part of is frequency spectrum interwoven with the public service band creates another issue. Managed access will have a similar set of issues. Managed access, as the name implies, will allow white-listed phones to communicate while rejecting all others. This would be a problem during a crisis or emergency if the first responder numbers are not on the white list. Detections systems, by design, have none of these issues because they do not transmit RF power.

How can any of the foregoing risks be mitigated or eliminated?

Both jamming and managed access systems will need to be tied into a facility's emergency systems. For example, if a fire alarm is initiated, that action should be capable of shutting down the jammer or managed access system. Every facility emergency system should be tied together such that when an emergency is declared by whatever means, the jamming or managed access system is disabled. It may be necessary to have a remote external to the building that is capable of disabling the system for first responders, much like the key system used in elevators during an emergency.

What are the benefits and drawbacks of implementing these techniques?

Implementation brings a level of safety that will potentially save staff, first responders, and inmates. Detection allows the facility to monitor cell phone activity 24/7 and use that information to assist staff in targeted interdiction as they see fit. The drawback to detection is that someone has to take an action to retrieve the phone. The drawbacks to implementing jamming and managed access systems are that they need to be tied to the site's emergency systems and false alarms could disrupt the function of the two systems. In the case of jamming, it would not be an issue but legitimate calls from a managed access system would be dropped.

Are certain systems more suitable for certain prison environments or locations?

Physical location of the facility does have an impact on some solutions. For prisons located in remote locations far from other potential cell phone users, jamming's negative effects might not have as big an impact. However, when in a high cell phone usage area, jamming would not be practical. For the managed access configuration, the same rules apply. Detection, on the other hand, is pretty much independent of physical location.

To what extent does the installation of each system require a customized approach for each prison?

All three systems require some level of installation planning and customization. Detection planning, which is the simplest, considers building configuration, materials, and proximity to areas where cell phones are allowed. Jamming – depending on the type of jamming approach implemented (multiple or single antenna) – must pay particular attention to areas in close proximity to the prison, like parking lots, that must be avoided. Jamming will also need to pass any FCC tests that are developed if the legislation to allow jamming becomes law. Managed access has similar issues to jamming but a managed access approach must also have the cooperation of the local carriers in the area of deployment, as well as an FCC license to operate.

How disruptive is the installation process?

The disruption will be a function of building construction and design. It is possible that managed access would be the least disruptive if a single tower system is implemented. Detection requires an array of sensors interconnected via low voltage Ethernet Cat-5 or Cat-6 type cabling. A jamming system will consist of either a single transmitter connected to multiple antennas which distribute the RF pollution, or an array of smaller transmitters with distributed antennas much like a detection system.

What approaches can be used in the implementation of systems employing detection techniques?

Detection systems are really intelligence systems that yield information on a phone's locations and duration of the call. Additional information collected includes transmit power levels and frequency. A cell phone detection system actually acts like a compass pointing towards contraband cell phones. Not only does the system indicate the location of cell phone activity, but experience has shown that where you find phones you find other contraband.

How does each system provide for completion of critical calls or radio communications such as those from public safety officers (including use of handheld two-way radios) or 911?

Detection systems do not transmit, and therefore do not interfere with, E911 or two-way staff communication devices. Managed access systems can be configured to allow all E911 calls to connect. While it is always possible for any transmitter to interfere with other receivers, well-controlled transmissions can be configured to prevent interference. Jamming, on the other hand, would prevent all calls, including E911 calls.

What ability does each of these technologies possess for upgrades to include new frequency bands, technologies, modulation techniques, etc., as they are introduced into the marketplace?

The ITT Cell Hound® product has a built-in expansion port that can be used for a number of add-ons and provides the base from which to add new receiver frequencies as they become available, thereby protecting the customer's investment. Detection sensors are modu-

lation agnostic for the most part since they are a sensor system and do not demodulate the signal. Both jammers and managed access systems will need to add new transmitters and receivers to support the new bands.

How quickly can they be upgraded?

The ITT product is already capable of handling the Nextel re-band when it occurs. However, to design and integrate a new frequency – including testing, integration, releasing to manufacturing, and deploying – could take 6 to 8 months. The actual deployment at a facility is a matter of days. Jamming systems would, at worst, require new hardware. If the existing system is hardware capable, then at the very least it would require new controlling software. Managed access systems would be similar to the jamming system.

Devices and Frequency Bands

What other frequency bands could be used by technologies that inmates could acquire with which to communicate?

Voice over IP (VoIP) could be used when carried over any data connection, including 802.11, 802.15.4 (Zigbee, 6LoPan, ANT, etc.), and Bluetooth. All of these use the unlicensed ISM spectrum (915 MHz and 2.4 GHz), and are commercially available with high power options for extended range.

Do, or will, the technologies identified above effectively cover all of the bands likely to be used for commercial wireless services and how do, or will, they do so?

Scanning detection methods are compatible with any system since they don't require protocol participation. Managed access solutions are unlikely to operate with unlicensed solutions, and have natural barriers to multi-standard coverage (i.e., simultaneous GSM/CDMA/WCDMA/802.11, etc.). Jamming will have the requirement to jam large swaths of spectrum, becoming broadband in nature, or necessitate intelligence which requires detection first, then jam only bands in use (i.e., smart jamming).

Specifically, which frequency bands does each approach currently best address, and which could they best address in the future?

Detection offers the widest range of coverage, being compatible with any system that transmits RF energy to communicate, unlike a system that transmits or acts as a radio.

How can the technologies prevent an inmate from communicating with a device employing proprietary technology (e.g., SMR radios)?

A detection solution would require the addition of the proprietary frequencies to the sensor itself. This is relatively easy to accomplish because the sensor systems are protocol agnostic. A jamming implementation would be straightforward as well, but of course would

have to deal with the other issues associated with jamming. Managed access would have the biggest issue because new radios would have to be developed to not only receive the proprietary transmissions, but to deal with the decoding and encoding of the protocol as well.

Will the technologies deal with phones that plan to operate in other bands where new services will be offered in the future, such as in the 700 MHz band?

Detection is easily scalable to any frequency band used for wireless communications. Jamming can be scaled but requires new transmitters to cover the new band. Managed access would require new transmitters and receivers, and if the protocol changes new software, as well.

What will be necessary to extend the capabilities of the technologies to new bands (new hardware or software, new antennas, agreements, etc.)?

Detection requires relatively little change if the hardware is capable of scanning the new frequency. If hardware capable, then a firmware-only change would be required for currently marketed products. Software would need to be updated to include the new frequencies but most vendors provide remote upgrade capability and may not require an on-site service call. Scanning rate and the ability to effectively cover the additional spectrum may impact some system's probability to detect. This is likely an easily managed detection system consideration. For jamming and managed access systems, new hardware and software would be required.

Interference to Other Radio Services

If jamming configurations are set up properly (that is, based upon site-specific radio frequency (RF) engineering), can these unwanted emissions be reduced or eliminated at a distance that is based on jammer and site parameters at each individual prison?

This is likely an intractable technical problem and requires sophisticated site measurements and surveys, which are likely more complicated than any practical implementation could justify. Even if it could be made to operate initially, any site change or aging of the devices could cause the covered area to change and require constant monitoring.

Is the location of the prison (rural versus urban) also a factor, and if so, why and how would that affect the feasibility or implementation of a jamming system?

Yes, it is a factor. Jamming intrinsically cannot discriminate between legitimate and illegitimate calls/phones. Dense urban areas will pose significant challenges to keeping jamming effective only for contraband phones.

What jammer system parameters (e.g., power levels, modulation, antennas) can be used to control out-of-band (OOB) and unwanted emissions?

Out-of-band and unwanted emissions are primarily properties of the transmitter linearity. High linearity is technically challenging and expensive.

Which of these parameters have the greatest impact on the effectiveness of the jammer transmitter?

Transmitted power and location have the greatest impact. The ability of jammers to disrupt contraband phone use is purely a function of the jammer RF energy present at the contraband device antenna. This can be accomplished by raw power, or by optimizing the propagation loss between the jammer and contraband device.

What other jamming techniques can be employed to disrupt wireless communication systems?

Managed access systems, although not strictly a "jamming" type of system.

Are filters commercially available that could be used to reduce the OOB and unwanted emission levels from jammer transmitters?

Yes, but the more linear the transmitter the better, but at a higher associated cost. There are many considerations in OOB filtering, such as jammer frequency range and the speed at which the jammer sweeps. These considerations may necessitate the use of switched and/or tunable filters. Cost and complexity are significant factors in applying a filtering strategy to reduce OOB emissions.

Will jamming multiple frequency bands simultaneously affect the emission characteristics of the jammer transmitter (e.g., generation of intermodulation products)?

Yes, this will also make management of OOB emissions more difficult.

Can spectrum sensing be used in conjunction with jamming techniques to reduce the transmit duty cycle of the jammer transmitter?

Yes, but it drive up the transmitter cost and complexity.

Are there variable strength cell phone jammers that are capable of dynamically adjusting their strength?

Yes, but how the jammer strength is set is critical. Is there a feedback mechanism that "deduces" what jammer power is effective? Is this done as a "site survey" (which could be costly)? Additionally, as the macro network controlled by the carriers change transmission power, the system must be capable of responding to these changes.

What are the factors that can vary the signal strength of the jammer if it is putting out too much power?

No comment.

How should the IPC for these handsets be established?

By lab measurement.

What IPC values should be used for assessing potential interference to these handset receivers?

Unknown; would require analysis and characterization.

Since the variations in the jammer configurations, effects of multiple jamming transmitters, structural characteristics of buildings, and propagation factors will be different depending on the installation and the facility, can analytical analysis techniques be used to develop the distances or EIRP limits necessary to protect in-band and out-of-band receivers?

To a certain extent with an analysis being an estimate, onsite adjustments must be made to ensure conformance to requirements. The complexity of a 3D propagation model for a structure as complex as a prison should not be underestimated. This could be an intractable problem, and at the very least a very expensive and time-consuming installation problem.

If analytical analysis techniques can be employed, explain the methodology to be used and all appropriate conditions considered in the analysis, including, but not limited to, propagation loss modeling and building attenuation modeling.

See previous answer.

How should the effect of multiple jammer transmitters and antennas be taken into consideration?

As with a single jammer, the SAR impact on any nearby personnel must be considered. Multiple co-located jammers will affect the location's specific radiated power. This could create locations where the power levels exceed safe SAR levels for any personnel in that area. This depends on how precisely the power must be controlled.

Are there other approaches that can be used to regulate jammer systems?

No comment.

Outside of the facility, will the variations in the measured levels of the jammer transmitter signal make it difficult to distinguish such a signal from the cellular and PCS signals in the environment, for example?

No.

If so, is this problem exacerbated in areas where there is a high density of cellular and PCS signals, such as in and around an urban prison location?

If you are not using broadband jamming, it would not be difficult.

Given variations in signal levels and the potential to distinguish the jammer signal from the background signals, is it possible to measure accurately the jammer transmitter signal outside of a facility?

Yes. Note that signal levels outside the facility will vary greatly due to propagation effects. If the concern behind this question is protection of legitimate devices outside a facility, then accuracy is not the issue, but rather the completeness of a spatial survey external to the facility is.

Within a facility, is it possible to distribute the jammer transmitter power spatially across an array of antennas (or, in some cases, lossy cables) in order to better control and provide lower power density around individual antennas than could be produced if a single antenna were used to radiate a high-power signal?

Yes. There are many advantages from managing the power. A distributed array of jammers or a jamming antenna would allow the maximum transmitted power to be minimized while distributing a more even power level across the facility. While this form of jamming may be more expensive, it may be the only solution that can overcome many of the negative aspects of jamming.

What techniques can be employed in the design of the jamming system to reduce the potential for interference to in-band and out-of-band receivers?

Yes, through the use of reactive filters.

Can restrictions be placed on the jammer transmitter antenna height to minimize the potential for interference outside of the area that is being jammed?

Yes, but this may be very difficult to accomplish and the height may vary with the jammed frequency and changes to the carrier's macro network.

Is it possible to employ directional or sector antennas to focus the jammer transmitter signal in the intended areas within a facility while minimizing the signal levels outside of the facility?

Yes, but this may not be effective if the prison/compound is not a clear line-of-site RF environment and/or has many irregular shaped buildings and areas.

Can down tilting the antennas be used to minimize the jammer transmitter signal level at the horizon?

Yes.

What restrictions can be placed on the antennas without impacting the effectiveness of the jamming system?

This is a very open-ended question. The more restrictions, the more complicated the system and the more costly the implementation.

Given all of the possible variations in a jammer system installation, will operators need to conduct on-site compliance measurements at each facility?

Yes, both pre-design and post-installation RF surveys will be required. The initial survey will be required to evaluate macro cellular power levels by carrier and potential antenna locations. This information would be used for system design. After installation, extensive measurements will be required, covering the entire campus or building(s) in order to measure jammer power for both coverage and compliance. Additionally, the owners of the macro network will need to coordinate with those operating the prison jamming system when changes are made to the carrier's network.

What techniques should be used to measure the emissions of a jammer system?

Power and field strength measurement.

Is it possible to accurately measure the jammer transmitter signals in the presence of other background signals?

Yes.

How shall an operator, in its request for authorization of such equipment, be required to demonstrate that it meets any interference protection requirements?

In field demonstration, under all macrocell operating conditions.

Do other technologies or approaches have the potential to interfere with other authorized radio services within the same bands or adjacent bands?

Yes, but only applicable to systems that transmit RF energy.

If so, under what conditions and how can an operator mitigate interference?

Time, frequency, and space are the three main parameters that can be varied to mitigate interference.

How will internal and external land mobile systems, including systems used by the prisons themselves, as well as other public safety operations, be protected?

No significant OOB signals and prison not using IBS for communications.

Are there other radio communications systems within prisons that could also experience interference, such as internal private land mobile systems used by prison officials or medical telemetry devices in prison infirmaries?

Possibly, particularly if any of the prison staff uses cell phones or use modem devices on computers or other equipment that communicate over the cellular frequencies.

Protecting 911 Calls and Authorized Users

How are 911 calls preserved in areas around the prisons where the public is making a call to 911 if they come in proximity to the prison?

This is not an issue with detection systems. Managed access systems can be set to allow all E911 calls to connect. Jamming is a different story, because an E911 call would be prevented unless the jamming signal is disabled.

Are there any other technologies identified that can protect 911 calls and how do they do so?

No comment.

How are authorized users allowed to make calls with the technologies described?

No comment.

If the caller passes through a "dummy" cell site set-up within the prison vicinity, will the call go through if a call is initiated within that cell (e.g., will it result in a busy signal or a dropped call)?

No comment.

Are calls handed off to the carrier cell site and network?

No comment.

How does managed access work if the caller is an authorized user, but the phone number is not known (i.e., in the database of authorized users) to the managed access system?

The call would be rejected unless the phone is added to the white list or the local HLR.

Cost Considerations

What factors impact the cost of implementing each of the technologies as described above?

All technical issues aside, the largest unknown cost issue for both detection and distributed jamming systems is infrastructure costs. Detection systems are generally powered over a Cat-5 or Cat-6 cable. Cat-5/6 cable was implemented because prison staff are familiar with

this technology, which they currently use on both their Information LAN systems as well as the security camera systems. Most prison staff already possess both the tools and the knowledge to implement and maintain such a system with minimum dependence on a contractor or vendor, allowing them to better control costs. Centralized jamming systems may distribute RF energy to remote antennas via coax cable similar to coax used in cable TV. Considerations when implementing a system that uses distributed devices will depend on the area of the country installing the system. For example, if the code rules require that low voltage cable or coax must be installed in rigid conduit, the installation costs will be higher than if the cable were run in open trays or in plenum shafts. Managed access systems, while much higher in initial cost to detection systems, may have a lower installation cost, but will require a lot of staff training to operate and a heavy dependency on the supplying vendor.

Are there on-going or recurring costs associated with each?

Detection systems have much lower ongoing or recurring costs than jamming and managed access systems. The lower costs are due in large part to the fact that the detection systems do not utilize proprietary operating and communication software. Additionally, the computers and Ethernet switches utilized are off-the-shelf products that can be purchased from existing Federal, State, and local contracts, again allowing the customers to further control costs. In addition, they will be working with hardware and software with which they are already familiar. Jamming systems may need to be adjusted in order to maintain compliance and jamming systems are affected by infrastructure changes, such as metal furniture reconfiguration. Managed access is just as the name describes – it needs to be managed. This will either require a heavy dependence on the system provider or a lot of training for the prison staff to manage since it requires that someone be in charge of the white lists to keep legitimate phones updated. It also requires close coordination with the various carriers in the area to manage not only power, but the frequency use plan.

To what extent will installation costs vary in light of the particular characteristics of each prison (e.g., geographic setting)?

Distributed jamming systems and detection system infrastructure installation costs will depend on the building codes that must be followed, and if they are to be installed in a right-to-work state or non-right-to-work state.

What characteristics are most likely to affect costs?

For detection system, the location accuracy desired drives the number of sensors required. That is, the closer the sensors are to each other, the more accurate the location prediction. For distributed jamming systems, the jamming power must be kept low so as not to produce unwanted interference. This will require more antenna or more low power transmitters. Both approaches deal with the same RF physics. Detection systems require little setup but do require the establishment of detection thresholds for the specific location, and the system must be setup so as not to trigger on non-cell phone interfering sources. The ITT system constantly surveys the RF background and automatically adjusts the thresholds. All

other adjustments can be made at the server managing the system or from a remote location if desired. Jamming systems require a thorough RF survey of the site and may require recurring or ongoing surveys if the environment changes and may apply to managed access as well.

What are the ancillary costs for each type of approach (e.g., maintaining network connectivity for managed access systems, resources required to physically locate the phone for detection/location systems such as canines, staff time, etc.)?

Detection systems save prison staff time by pointing to the high value target areas, thereby reducing the time to search, the number of staff involved, and the area to search. Also, where there are phones, there is usually other contraband. Locating cell phones allows the prison staff to gain one more piece of intelligence into the potential problem areas.

Are there typical costs or a range for each, and if so, what are they?

ITT can speak to the currently produced and installed detection systems and give an estimate for a distributed jamming system. The detection system component prices are published on our GSA schedule. Total system pricing depends on different factors as previously described, such as desired location accuracy and number of individual buildings. ITT has systems installed that range in price from $20,000 that cover 200 inmates in two dorms, to a 65-acre campus with 11 building of various configurations housing 3,500 inmates for $600,000. Another example covered three, three-storied buildings occupied by 1,500 inmates for $75,000. A distributed jamming system that covers the same area as a detection system and meets the law as currently passed by the Senate is estimated to cost about two to three times that of the detection system. It should be noted that a key difference of the detection system over the other two primary options is that detection systems can be incrementally installed. A prison can install in one area at a time as the budget allows. Managed access and jamming tend to be an all-or-nothing installation. Detection systems can also be installed with different buildings or areas having different degrees of location accuracy, allowing the customer to configure the most cost-effective solution for their needs.

Is training required for prison staff to properly operate the equipment?

Yes, for the ITT detection system a one-day training session is provided. Users of the system are instructed in how to interpret the output, run reports, and improve their search effectiveness. Information Technology (IT) personnel at the facility are taught how to install the user software and add and delete user access and Facilities staff are trained in how to investigate and replace a failed sensor. Managed access and jamming systems will require even more training than detection systems unless the management of those systems is handled by the vendor.

What staff costs are associated with each technology?

For detection systems, some staff members in the IT and Facilities staff would be required to receive training. IT staff would be required to add and delete users on an as-needed ba-

sis. Currently, ITT charges $1,500 for a one-day training session for those operating and maintaining the system.

Locating Contraband Phones

How do managed access and detection technologies locate a cell phone caller?

Detection systems use RF signal triangulation while managed access systems could use a combination of RF signal triangulation and GPS, if the GPS is enabled on the phone. Managed access systems do not have the same location accuracy as the detection system . The GPS may or may not be an advantage in location accuracy because the user can turn off the GPS function, or the GPS may not be able to get sufficient satellite signal strength to derive a location.

What software and hardware is needed?

The ITT detection system runs on a Microsoft® SQL Server® with detected data stored in a relational database. The operating system software and database can be purchased off-the-shelf by the customer, along with the required hardware, such as a server, workstation(s), and Ethernet switches. The ITT software and hardware system components consist of a software server application, three client software packages, and sensor hardware. The system was designed to utilize uninterruptible power supplies (UPS) to protect the server and switches while keeping the system operational in case of a total power failure.

How accurate are detection technologies?

As mentioned before, the location accuracy is dependent upon the number of sensors installed. The ITT technology has demonstrated accuracy within 3 to 5 meters.

With the insertion of GPS chip-sets into mobile devices, are cell phone locations easily identifiable through managed access or are other means necessary (e.g., hardware or software)?

GPS is easily defeated by simply turning off the GPS receiver. Access to GPS coordinates even when the receiver is operating requires software located on the phone, which the user can easily disable.

Do managed access and detection technologies have the capability of providing intelligence-gathering information for prison officials, and if so, what type of information?

While the current ITT detection system will generally yield better location accuracy than a managed access system, the managed access system can yield source and destination phone numbers and more, if allowed by law.

What other means are necessary to physically locate the phones once a position is known?

Generally speaking, when someone comes on the cell block floor, inmates turn their phones off unless it's someone they are sure will not check in on them. With a detection system, the confidence level or search area can be quantified, which targets the search area. The targeted area can be physically searched by officers or cell phone sniffing dogs or a non-linear junction detector can be used to scan the potential hiding areas within a cell block area.

Regulatory/Legal Issues

We seek comment on State/local or Federal laws, rules, or policies that need clarification or that may hinder deployment of any of these technologies or others that may be raised by commenters.

Jamming systems could pose health risks to nearby personnel if radiated power levels are high enough. Jamming systems in particular should be studied by the U.S. Department of Health and Human Services as to the effects of higher-than-normal levels of radiated power. When using the cell phone, the user is only subjected to power during the call and using a hands-free device or a headset adds further protection for the user. In order to jam the phone, the RF pollution generated by the jammer must overcome the signal from the macro cellular tower. This means that employees assigned to work in the jammed area will be subjected to these higher levels of radiated energy on a continuous basis during their work shift. Inmates, on the other hand, will be subject to this elevated power on a continuous basis throughout the day, every day.

These might include not only radio regulatory issues, such as the approval necessary to operate or conduct experimentation and demonstration, but also ancillary issues such as the privacy and legal implications of trap-and-trace technologies?

One legal point to investigate is when using a managed access system – even though it might be forbidden for an inmate to possess and use a cell phone – are calls from the inmate to his lawyer or doctor protected, and if so, how would the system distinguish these calls from other calls?

What agreements, agency relationships, or licensing requirements between the prison, service provider, and access provider would be required for temporary or experimental demonstration or for permanent operation?

No agreement is required for the ITT detection system. Jamming systems would need to be authorized by the FCC. Managed access systems would require both a license to transmit and authorization by the carriers servicing the area.

Technical Issues

Are there any technical issues to be considered for the technologies identified above?

While not a technical issue so much as a technical use issue, jamming systems in particular should be studied by the U.S. Department of Health and Human Services as to the effects of higher-than-normal levels of radiated power on those exposed.

How accurate are the location technologies?

Detection system accuracy is a function of the distance between sensors. Current systems have the ability to locate within 3 to 5 meters.

Does each site need specific RF engineering for each of the approaches?

The ITT detection system requires very little onsite RF engineering because it is a receiver only and not a transmitter. Most of the RF adjustments are completed at the time of installation. In comparison, jamming systems and managed access systems require much more onsite RF engineering plus ongoing monitoring.

How do the technologies allow authorized users, including 911 calls, to be protected?

Detection systems do not transmit and therefore do not interfere with E911.Jamming system will jam all E911 calls while managed access systems can be enabled to allow all E911 calls to connect.

How are different modulation schemes or channel access methods (for example, Global System for Mobile Communications – GSM, or Code Division Multiple Access – CDMA) handled for each category and does the solutions depend on the type of access method that the wireless carrier is using?

The ITT detection system measures power and frequency and is therefore modulation agnostic. Jamming systems tend to be modulation agnostic, but managed access systems must handle each unique scheme to operate.

Is there a need to differentiate between voice and data, such as text messages, and are the technologies discussed above effective against data use by prison inmates?

No. For the detection system, all transmissions from the phone to the tower are treated the same as the phone periodically checking in with the tower. Jamming systems would treat them both the same as well.

Does shorter air-time use from text messaging present problems with detection and/or capturing the call and ultimately locating the phone?

No, there is sufficient handshaking between the phone and tower during a text message to derive a location at least for the ITT system. Since jamming is assumed to be constant, there is no issue there, and managed access systems are designed to handle all cases as well.

Will the technologies identified above be effective against high-speed, high-capacity data formats, such as Long Term Evolution (LTE) for devices that are expected to operate in the 700 MHz band?

Detection systems are effective against any system that radiates RF energy. The modulation format and bandwidth do not affect the ability of adequately designed systems to operate correctly. Jamming systems would be effective as well. Managed access systems will need to be modified to handle the different technologies.