Before the
DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Washington, D.C. 20230

In the Matter of	)	
	)	
Preventing Contraband Cell	)	NTIA Docket No. 100504212–0212–01
Phone Use in Prisons	)	

COMMENTS OF TECORE NETWORKS

Tecore Networks (Tecore) hereby submits its Comments to the Notice of Inquiry (NOI) issued by the Department of Commerce, National Telecommunications and Information Administration (NTIA) in the above-referenced matter.

SUMMARY

Tecore Networks, a global supplier of cellular systems to commercial carriers and government agencies, is pleased to provide comments on the three broad categories of solutions to prevent contraband cell phone use: jamming, managed access and detection. Tecore has developed a unique managed access solution known as the Intelligent Network Access Controller (iNAC),[1] which forms a radio frequency (RF) umbrella around a precisely defined target area and attracts cellular devices within range. Subscribers are classified into categories and either allowed to access the commercial network or prohibited access on a subscriber-by-subscriber basis. Managed access provides the method for making the decision at the subscriber level rather than at the RF signal level, and therefore the iNAC is able to distinguish the allowed users from those not permitted service. This meets the requirement of service restriction while continuing to allow access to select individuals. This approach also enables the completion of 911 calls while otherwise restricting service. The iNAC does not require changes in existing laws in order to be operated. The iNAC has been effective in providing managed access in a prison outside the mainland United States, and Tecore has worked with the Federal Communications Commission (FCC) and the commercial cellular service providers to ensure it meets their requirements as well as those of the corrections community.

Although limited testing of jamming has been conducted in the U.S. to date, the significant remaining uncertainties regarding the interference potential of jamming, as well as the inherent complexity and dynamic nature of the commercial and public safety communications infrastructure, will substantially impede attempts to mitigate that potential. Tecore proposes more comprehensive testing of managed access technology to complete the public record on solutions for contraband cell phones in prisons. The iNAC enables more comprehensive testing due to characteristics such as the ability of a single system to cover an entire prison, and the

[1] "Intelligent Network Access Controller" and "iNAC" are trademarks of Tecore Networks.

availability of device and call data to measure the efficacy of the technology in selectively preventing cellular communications.

TECORE NETWORKS

As a global supplier of cellular systems to commercial carriers and government agencies, Tecore Networks has significant experience and data to inform the critical work undertaken by several agencies to investigate and evaluate how technologies might be utilized for law enforcement and corrections applications.

More background on Tecore's experience and expertise in cellular communications has been provided in Appendix A.

COMMENTS ON NOTICE OF INQUIRY[2]

1. Technologies or Approaches

We have initially identified three broad categories of approaches that provide solutions for preventing contraband cell phone use: jamming, managed access, and detection. Are these characterizations accurate and complete?

Tecore agrees that these are the three principal categories of technology solutions to address contraband cell phone use. However, we do not believe that detection prevents cell phone usage, but rather that it identifies device location and then leaves it to corrections personnel to retrieve the phones. Such efforts at retrieval place corrections personnel in additional dangers beyond the ordinary rigors of a high risk job, as they will have to confront prisoners unwilling to relinquish phones. Please refer to Appendix B for a more detailed comparison of managed access, jamming and cell detection.

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

Tecore is aware of a unique type of managed access technique, as embodied in its Intelligent Network Access Controller. The iNAC forms a radio frequency (RF) umbrella around a precisely defined target area and attracts cellular devices within range. Subscribers are classified into categories and either allowed to access the commercial network or prohibited access on a subscriber-by-subscriber basis. Managed access provides the method for making the decision at the subscriber level rather than at the RF signal level, and therefore the iNAC is able to distinguish the allowed users from those not permitted service. This meets the requirement of service restriction while continuing to allow access to select individuals. This approach also enables the completion of 911 calls while otherwise restricting service. Importantly, by making decisions at the subscriber level, the iNAC is able to restrict an inmate from using an unauthorized subscriber identity module (SIM) card in an authorized device (for example, one stolen from a corrections officer).

[2] Tecore's comments are presented following original portions of the NOI, reproduced and italicized.

The iNAC does not require changes in existing laws in order to be operated. As it uses commercial frequency bands, it requires either a special authorization from the regulatory authority governing use of the spectrum (NTIA: federal facilities; FCC: state and local facilities), or cooperative agreements with the commercial carriers serving the target area.

The principal differentiator of the iNAC is the patented multi-technology controller, capable of addressing commercial carriers, technologies and frequency bands from a common system. The scalability of the platform enables a range of configurations, from a permanent installation to cover a fixed, sizeable area, to a multi-technology rack ready for vehicle mount, to a suitcase model (ideal for a single technology). For more advanced multi-site installations, the iNAC provides centralized control and operations with each location servicing the necessary technologies and frequencies applicable in the area.

To further enhance the public record of technologies to address contraband cell phones in prisons, Tecore respectfully submits a summary report of selected managed access demonstrations and deployments as Appendix C.

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

For managed access, the baseline risk is associated with the issue of RF umbrella bleed outside the borders of the target area. This risk is mitigated by the fact that, unlike jamming, not all communications are prevented. As discussed below, due to the custom nature of each installation, the risk is further reduced by the precise configuration of the necessary antenna system, based on a detailed site survey. During operation, iNAC operators are trained to test and maintain a consistent coverage footprint. By coordinating the deployment with the commercial carriers in the area, the coverage of the iNAC is managed and monitored as if it were effectively another cell site in their network. As a failsafe, built into the agreements with each of the commercial carriers is a procedure for any carrier to notify the iNAC operator of anomalies in RF activity. This procedure includes methods for correction starting with shutdown of the specific frequency band at issue until resolved. Finally, due to the nature in which the iNAC interacts with the commercial networks serving the area, a call already in progress outside the prison perimeter will not be impacted adversely by the iNAC.

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

As the iNAC is built using FCC approved cellular and wireless infrastructure, the existing equipment is capable of operating within the bounds of the spectrum licensed to each of the carriers. The operating frequencies of the iNAC are precisely tuned and managed in coordination with the commercial network. As such, the iNAC poses no more risk to the public safety and government use of spectrum than the existing commercial equipment deployed in the area providing commercial wireless service.

The RF umbrella can be precisely tuned to the frequency bands and channels used by the commercial carriers serving the target area, thereby avoiding interference with public safety or government frequency bands. Furthermore, the controller can be configured to support the

Communications Assistance for Law Enforcement Act (CALEA), enabling the government to intercept, monitor and record communications under court warrant or applicable law.

While the iNAC equipment has FCC compliant filtering built into the solution, most jamming equipment has a cost curve that rises sharply in correlation with increased accuracy and precision of filtering and tuning required for this type of application.

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

The unique approach of the iNAC managed access solution provides the flexibility to adjust the system to the coverage, capacity, and carriers operating in a given area. A key element of the system deployment is matching the proper RF distribution method with the coverage requirements of the institution. While this may vary greatly from one site to the next, the iNAC can be deployed to cover an entire facility, a specific building or a single floor.

Unlike solutions that operate at low power and provide a minimal coverage footprint per device thus requiring a high number of installation points in the facility, the iNAC can be deployed using standard cellular antenna systems, operate at macro power levels and provide the necessary coverage footprint. For smaller areas requiring a minimal footprint, the same solution can be deployed using milliwatts of power and common technology solutions such as distributed antenna systems. In either deployment scenario, a consistent operation and solution is provided for the prison(s).

The opportunity for sabotage, disablement or interference of the iNAC is very low since, unlike jamming or cell detection, the deployed components are not usually installed where inmates or other unauthorized individuals may have access to them. The iNAC can be located in a secure area locally or remotely to add another level of security. The antenna system is usually located on a local water tower or other structure where access is very limited and secure.

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

The iNAC establishes an RF umbrella designed to precisely cover the target area. Prior to each deployment, a site survey is conducted to optimize the configuration of the system. The borders of the target area, as well as the technologies and frequency bands of the serving commercial network operators, are accounted for. The footprint is optimized through the use of power control, directional antennas, and repeaters to limit the coverage of restricted area to the building or campus where the iNAC is to operate. The process of the site survey and installation follows standard industry practices for the installation of a cell site in the network.

How disruptive is the installation process?

The iNAC solution has been designed to be minimally disruptive in terms of installation since access to general inmate population areas is typically not required. The iNAC can be installed within a week, by professionals under contract. The installation occurs during hours acceptable to the prison administration. Following installation, personnel designated by the prison administration are trained on system operation, which typically takes several hours

depending on the level of technical background of the personnel. The process has also been designed to be minimally disruptive to the commercial carrier networks. Tecore has been working with the carrier community for over a year on developing agreements and test and verification processes to ensure there is no adverse impact to the normal operation of their networks.

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?

Handheld two-way radios operate on a frequency band outside the frequncies used by the commercial carriers and therefore operate as they do today without interference. As described previously, the iNAC includes a feature to enable calls to 911 even from unauthorized subscribers.

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? How quickly can they be upgraded?

The iNAC has a unique ability for upgrade to new technologies and generations. When new technologies and/or frequencies are added to the commercial wireless infrastructure, these are incorporated into the iNAC as an additional access technology. This is possible because the solution is based on Tecore's patented multi-technology iCore platform, which is the first and only core network to process the family of 3GPP and 3GPP2 wireless technology standards on a common architecture. New technologies can therefore be addressed significantly through software upgrade to the controller, and the addition of radio access modules. Similar to the installation process, the iNAC can be upgraded within a day.

2. Devices and Frequency Bands

Many types of wireless mobile devices are available to consumers from a plethora of commercial carriers (e.g., push-to-talk, cell phones, smart phones, personal digital assistants). These devices operate, consistent with FCC rules, in a number of frequency bands depending upon the types of services and capabilities/features that the wireless carriers offer. To eliminate contraband cell phone use in prisons, techniques must be identified that have the capability to thwart the use from the gamut of devices and spectrum bands/frequencies in which these phones operate. These devices and associated frequency bands are: Cellular (824-849/869-894 MHz); PCS (1850-1990 MHz); AWS (1710-1755/2110-2170 MHz); and SMR (806-824 and 851-869; 896-901 and 935-940 MHz). Additionally, spectrum bands, such as the 698-806 MHz (700 MHz) band, 2110-2170 MHz, and the 2500-2690 MHz band, will soon offer newer, faster, and more bandwidth-intensive features to the public. Further, other devices that operate in such radio services as the Family Radio (462.5625-467.7125 MHz band) and General Mobile Radio (462 – 467 MHz band) Services present possible avenues for illegal or unauthorized communications by inmates. While the range of these two services is relatively small, both use handsets for two-way voice communication and could be attractive to inmates in urban environments. Undoubtedly, any of these devices could find their way to prison inmates as well. What other frequency bands could be used by technologies that inmates could acquire with which to communicate?

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? Specifically, which frequency bands does each approach currently best address, and which could they best address in the future? How can the technologies prevent an inmate from communicating with a device employing proprietary technology (e.g., SMR radios)? 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? What will be necessary to extend the capabilities of the technologies to new bands (new hardware or software, new antennas, agreements, etc.)?

The scope of all potential devices and technologies that can be used for illicit communication is very broad. Practically speaking, however, Tecore believes that the vast majority of contraband devices are in the widely commercially available cellular technologies. There are three drivers for this state:

- Cellular devices are becoming ever more compact in size, making it easier to smuggle them into restricted areas;

- Pricing of devices as well as service plans have essentially made cellular communication a commodity affordable to almost all income levels; as part of this issue, prepaid service requiring no commitments or contracts has made tracing the purchase of the device more difficult; and

- The devices interact with network equipment that is far outside the facility, and as such inmates can use them to communicate with minimal chance of detection by corrections personnel.

To further support these points, consider that while satellite telephony could theoretically be used, satellite telephones are neither compact nor inexpensive enough to be as widely adopted as cell phones. Short range communications – whether Specialized Mobile Radio (SMR) radios or even Wi-Fi devices – are also less likely to be used, due to the fact that the other end of the communication (other radio, or access point) would need to be located in or sufficiently near the facility so as to increase the risk of detection by personnel.

Accordingly, managed access solutions focus on the core group of cellular technologies that are widely commercially available. Within these technologies, all protocols and frequency bands are addressed. As new protocols and frequency bands – for example, Long Term Evolution (LTE) or 700 MHz – reach a point of critical mass in terms of device availability and pricing, managed access technology will evolve to address them.

3. Interference to Other Radio Services

Avoiding interference to authorized cell phone reception – as well as other radio services outside the cell phone bands – is a critical element in evaluating the various technologies. The longstanding radio spectrum regulation principle, embodied in the Communications Act of 1934, is to preclude harmful interference and not to block access to or receipt of information transmitted wirelessly.22 In addition to producing emissions in specific bands and within specific areas to deny service, jamming systems also produce unwanted signals outside of their

intended operating bands and are not naturally confined to a prescribed area. These signals have the potential to produce interference to other radio services operating in numerous frequency bands (including Federal Government operations) and outside of the prison facility.

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? 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?

What jammer system parameters (e.g., power levels, modulation, antennas) can be used to control out-of-band (OOB) and unwanted emissions? Which of these parameters have the greatest impact on the effectiveness of the jammer transmitter? Swept frequency techniques are often employed in jamming systems. What other jamming techniques can be employed to disrupt wireless communication systems? Are filters commercially available that could be used to reduce the OOB and unwanted emission levels from jammer transmitters? Commenters should provide details on the specifications for the filter (e.g., manufacturer, model number). Will jamming multiple frequency bands simultaneously affect the emission characteristics of the jammer transmitter (e.g., generation of intermodulation products)?

NTIA also seeks comment on other techniques that cell phone jammers can implement to reduce interference to other radio services. Can spectrum sensing be used in conjunction with jamming techniques to reduce the transmit duty cycle of the jammer transmitter? Are there variable strength cell phone jammers that are capable of dynamically adjusting their strength? What are the factors that can vary the signal strength of the jammer if it is putting out too much power?

The emissions from jammer transmitters can potentially cause interference to receivers beyond the intended jamming area. A critical parameter necessary to assess the potential impact to a receiver is the interference protection criteria (IPC). There are currently no industry-adopted or Federally-mandated standards for in-band interference from other systems to wireless mobile handset receivers. How should the IPC for these handsets be established? What IPC values should be used for assessing potential interference to these handset receivers?

An approach to regulating jammer transmitters could be to establish a distance at which the jammer signal must be below a specified level necessary to protect in-band and out-of-band receivers. An alternative approach could be to specify maximum allowable equivalent isotropically radiated power (EIRP) limits necessary to protect in-band and out-of-band receivers as a function of frequency. 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? 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. How should the effect of multiple

jammer transmitters and antennas be taken into consideration? Are there other approaches that can be used to regulate jammer systems?

The impact of jamming signals would also depend on the prison environment. 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? 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. The variations in the measured jammer transmitter signal levels could likely be due to propagation effects and building attenuation losses that will be different at each facility and for each jammer installation.

Furthermore, depending on the relative signal levels, it can be difficult to differentiate between the measured jammer transmitter signal and the cellular and PCS signals. 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?

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? 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? Can restrictions be placed on the jammer transmitter antenna height to minimize the potential for interference outside of the area that is being jammed? 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? Can down tilting the antennas be used to minimize the jammer transmitter signal level at the horizon? What restrictions can be placed on the antennas without impacting the effectiveness of the jamming system?

Each prison is unique in size, location and structure. Jammer set-up configurations cannot be applied broadly to all jammer systems in all locations. The variations in the jammer transmitter signal levels outside of the facility depend on a number of factors such as building structures, antenna deployment, and background signals. These factors could have an effect on the ability to measure accurately jammer transmitter emission levels. Given all of the possible variations in a jammer system installation, will operators need to conduct on-site compliance measurements at each facility? What techniques should be used to measure the emissions of a jammer system? Is it possible to accurately measure the jammer transmitter signals in the presence of other background signals? How shall an operator, in its request for authorization of such equipment, be required to demonstrate that it meets any interference protection requirements?

Do other technologies or approaches have the potential to interfere with other authorized radio services within the same bands or adjacent bands? If so, under what conditions and how can an operator mitigate interference? In some of the bands identified above, public safety frequencies are interleaved or operate in close proximity with frequencies used by mobile devices, for instance in the 800 MHz SMR and 700 MHz bands. How will internal and external

land mobile systems, including systems used by the prisons themselves, as well as other public safety operations, be protected? 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?

Tecore believes that jammers are not the optimal solution to address contraband cell phone use, primarily because they prevent legitimate and emergency communications from occurring.

Tecore commends NTIA's tests of jammers[3] as part of a broader initiative to investigate how various technologies can be used to address law enforcement and corrections requirements. However, these tests cannot be considered conclusive because:

- the limited deployment (in a confined geographic area) for field measurements was not sufficient to warrant definitive assessments of the aggregate interference to in-band or out-of-band receivers if multiple jammers were deployed in the facility;

- laboratory and field measurements were only conducted for one type of jammer, which cannot be applied broadly to all jamming products;

- testing involved measurements of the relative signal strengths of jamming systems compared to out-of-band (LMR, GPS) and in-band (cellular, PCS) transmissions, but effectiveness of the jamming on unwanted communications was out of scope;

- jamming signals were detectable in contention with commercial cellular signals up to a distance of 127 meters (139 yards) outside the perimeter of the prison where the field measurement was performed, creating a significant area where legitimate communications could be adversely affected by the jammer.

In addition to the significant uncertainties remaining in the interference potential of jamming technology, the inherently complex and dynamic nature of the commercial cellular and public safety communications infrastructure will further impede attempts to mitigate interference. The following characteristics of wireless networks will be important considerations and challenges in such attempts:

- the large range of narrow frequency bands utilized by the different commercial service providers, including but not limited to technologies deployed in 700 MHz, 800 MHz, 850 MHz, 1700 MHz, 1950 MHz and 2100 MHz, with channels as narrow as 200 kHz;

- the diversity of technologies being used in those bands, with different attributes for addressing interference;

[3] NTIA Technical Memorandum 10-468, *Initial Assessment of the Potential Impact From a Jamming Transmitter on Selected In-Band And Out-of-Band Receivers*, Drocella, Edward F., May 2010; and NTIA Report TR-10-466, *Emission Measurements of a Cellular and PCS Jammer at a Prison Facility*, Sanders, Frank K. and Johnk, Robert T., May 2010.

- the variation in distances of base stations from the prisons, resulting in variation of the signal level for each network;

- the continually adjusting area of coverage of a cell site based on cellular activity at different times of the day; and

- the variation in signal receive sensitivities of cellular devices.

Tecore invites NTIA to test the iNAC managed access system to establish a common frame of reference for technologies to address contraband cell phones in prisons. As noted in an earlier response, the iNAC is built using FCC-approved equipment that has been specified, built and approved by the FCC for operation as cellular infrastructure in each of the commercial bands and technologies. We propose that these tests be conducted under conditions that would result in a more complete assessment of managed access than was possible for jamming. Specifically:

- the ability for a single iNAC to cover an entire prison will enable NTIA to draw conclusions about the impact of this technology in a real-world deployment;

- the availability of data on devices, subscribers and calls will provide insights into the effectiveness of this technology in solving the critical problem of eliminating contraband cell phone use;

- the capability of the system to permit 911 calls and support CALEA will demonstrate how this technology addresses critical aspects of public safety and law enforcement.

4. Protecting 911 Calls and Authorized Users

The preservation and protection of calls to 911 from cell phones is a paramount concern as more consumers rely on mobile devices. The number of cell phones calling 911 has been steadily increasing as more consumers are using them. The National Emergency Number Association estimates that wireless telephone users account for nearly half of the calls to 911. Jamming radio signals in and around prisons cannot differentiate between normal cell phone traffic and 911 calls. Managed access systems, however, can be selective and designed to ignore 911 calls (i.e., letting them connect to the network), and detection systems typically use passive devices that do not affect transmission or reception. 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? Are there any other technologies identified that can protect 911 calls and how do they do so?

Wireless consumers expect their wireless calls to be completed without being dropped or busy. In and around prisons, consumers and public safety officials, as authorized users of the system, will expect their wireless devices to communicate. How are authorized users allowed to make calls with the technologies described? 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)? Are calls handed off to the carrier cell site and network? 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?

This issue goes to the very heart of why Tecore Networks developed the managed access approach, and why we believe it is the optimal solution to preventing use of contraband cell phones.

Tecore's principal line of business entails enabling, not disabling, cellular communications. In supplying core and radio access networks to commercial carriers worldwide, we have developed a broad perspective on the benefits afforded to the general public from this technology, and on the issues facing the carriers. While we have no doubt that the issue of contraband cell phones is a national threat to public safety that must be eliminated, we also know that brute-force measures will have undesirable consequences. Denying legitimate, mission-critical or emergency use of the cellular networks is not only inadvisable, it is also unnecessary.

In a managed access system, separate policies are readily defined for authorized subscribers, unauthorized subscribers, and calls to 911. These policies are set by the iNAC operator, and may need to comply with state or local laws and regulations. These policies are also approved in advance by the commercial carriers. Authorized subscribers and calls to 911 can therefore be allowed access to the network while unauthorized subscribers are denied. These policies and lists of authorized or unauthorized subscribers can be revised in real time – pursuant to the appropriate security measures – by the iNAC operator.

Additionally, the compliant interface to the Public Safety Access Point (PSAP) can be provided directly from the iNAC for the PSAP per the E911 standards. Where required this includes reconnect capabilities for E911 calls that require a reconnect from the PSAP to the device.

5. Cost Considerations

The cost of preventing cell phone use in prisons is a factor that must be considered and varies according to the type of technology, area to be covered, and additional features. What factors impact the cost of implementing each of the technologies as described above? Are there on-going or recurring costs associated with each? To what extent will installation costs vary in light of the particular characteristics of each prison (e.g., geographic setting)? What characteristics are most likely to affect costs? 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.)? Are there typical costs or a range for each, and if so, what are they? Is training required for prison staff to properly operate the equipment? What staff costs are associated with each technology?

There are three primary drivers of cost of a managed access system:

- The number and types of technologies and frequency bands utilized by commercial networks serving the target area.
- The size and topology of the target area to be covered
- The suite of features (e.g., CALEA support) included with the controller.

Given the significant variability in all of these drivers from one prison to the next, it is difficult to provide firm costs without at least some preliminary information to determine the three cost drivers listed above. The availability of different-sized iNAC configurations – from a suitcase at the low end to a macro cell site at the high end – supports a wide range of facility types as well as department budgets. The ability of the iNAC to operate over a wide area also means that costs can be spread over multiple facilities in some geographic areas. The iNAC operating expenses can further be minimized if it is deployed centrally at a managed access facility.

6. Locating Contraband Phones

In order to completely eradicate contraband cell phone use, the cell phone must be physically located and removed, which can be labor-intensive. Inmates may use them for a short period of time and turn them off and then move them, making the devices more difficult to locate.

Tecore does not believe it is effective to require contraband cellular devices to be physically located and removed. This approach entails additional resources and time from the prison administration. Managed access is designed to assure the prevention of unauthorized communications without requiring the retrieval of devices, which is manpower-intensive. The iNAC effectively turns contraband cell phones into paperweights.

In addition, confiscating a cell phone does not necessarily disable communications: the critical component allowing communications on many phones is the subscriber identity module (SIM) card, which sets the device phone number and calling plan, is the size of a postage stamp, can be easily removed from the phone and hidden, and can be used on any compatible device.

Neither the brevity of the communications attempt, nor the use of modified equipment (as in the SIM card example above) will have any impact on the iNAC's ability to block unwanted communication.

How do managed access and detection technologies locate a cell phone caller? What software and hardware is needed? How accurate are detection technologies? 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)? Do managed access and detection technologies have the capability of providing intelligence-gathering information for prison officials, and if so, what type of information? What other means are necessary to physically locate the phones once a position is known?

As stated previously, Tecore does not believe it is cost effective to require contraband cellular devices to be physically located and removed from the prison. With respect to intelligence gathering capabilities, the iNAC can provide the type and detail of information available from a commercial network operator. Information about the device identity, activity record including numbers dialed and text messages sent, along with the capability for CALEA compliant interfacing to Law Enforcement Agencies.

7. Regulatory/Legal Issues

The Communications Act of 1934 established the FCC and set specific rules on wireless radio services. Both the operation of mobile wireless devices, and effective means and solutions to deny the use of them have regulatory and legal implications. The FCC has primary responsibility for regulating spectrum issues for the types of systems typically used within the State and local prisons and jails (for example, private internal radio communications and commercial systems used by prison staff). NTIA, on behalf of the President, authorizes the use of the radio frequencies for equipment operated by Federal entities, including the BOP.

While the Communications Act prevents the FCC from authorizing jamming or other acts of intentional interference to the radio communications of authorized stations, those same provisions do not apply to the Federal government itself. Therefore, NTIA is not limited in its authority to permit jamming at Federal prison facilities. 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. 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? 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?

Physical Interdiction

The traditional solution of physical interdiction – *i.e.,* preventing unauthorized devices from entering a prison – presents the potential for First Amendment freedom of speech and Fourth Amendment search and seizure issues, at least among those non-prisoners who may be subject to physical search and confiscation of devices upon entering a prison and the subsequent denial of communications while in the prison. The fact that visitors and other unauthorized holders of devices voluntarily enter the prison, and thereby effectively consent to the denial of these rights would seem to undercut the potency of any Constitutional argument with physical interdiction. The denial of these rights to the prisoners themselves would seem to fall within the scope of the other freedoms and rights taken legally from prison inmates as a result their incarceration.

The limited effectiveness of physical interdiction has resulted in the widespread introduction of wireless devices into prison facilities. Prison officials have been forced to devote significant resources to the location and removal of contraband devices from within their facilities. Such confiscation would seem to implicate the same Constitutional rights as above, and with the same analysis of the legal limitation of these rights for prisoners.

Cell Detection/Confiscation

Cell detection – which uses a variety of technologies to identify the existence and location of operating devices within the prison – works as an adjunct to traditional confiscation efforts. This solution "listens" for devices and guides prison officials in wresting unauthorized devices away from prisoners who are using them. The ultimate success of the solution in

preventing the *continued use* of contraband devices, however, is only as good as the ability of prison administration to physically locate and confiscate the devices detected. Because the solution is "passive" (i.e., it does not involve radio transmission by the detection equipment or any interdiction of radio signals), it does not require compliance with any law or administrative rule that regulates the licensing or operation of radio transmitting stations or interference between radio stations. However, the solution involves the interception of radio transmissions from a device to locate and identify the device within the prison, and as a result implicates a number of Federal statutes.

The so-called "Pen/Trap Statute" – 18 U.S.C. §§ 3121 *et seq.* – states that "no person may install or use a pen register or a trap and trace device without first obtaining a court order." 18 U.S.C. § 3121(a). A ''pen register'' is a device which records or decodes the "dialing, routing, addressing or signaling information" transmitted by a device and a "trap and trace device" captures similar information incoming to the device. 18 U.S.C. §§ 3127 (3)-(4). Wireless service providers are exempted from this prohibition in the operation and maintenance of their wireless networks. 18 U.S.C. § 3121(b)(1). Since the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that a person has no reasonable expectation of privacy in the telephone numbers he dials, the legal hurdle for such surveillance is generally very low. A much different analysis has applied to the collection of location information however.

Cell site information – *i.e.,* identification of the specific cell site or sites a device transmitted to and received from during a wireless call – has been determined to be "signaling information" within the scope of this prohibition. *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 463-64 (D.C.Cir.2000). Section 103(a)(2) of the Communications Assistance for Law Enforcement Act ("CALEA"), explicitly restricts court orders under the Pen/Trap Statute from requiring wireless service providers to make available "any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2). The legislative history of CALEA makes it clear that "the authority for pen registers and trap and trace devices *cannot be used to obtain tracking or location information,* other than that which can be determined from the phone number." *See* H.R.Rep. No. 103-827(I), at 17 (1994) [emphasis added].

A series of Federal court cases have upheld the protection of cell site information, including especially capturing of information in combination to allow law enforcement the ability to triangulate the location of a subscriber in real time to within a few hundred yards. Review of the case law across the nation, however, demonstrates that the law in this area is not at yet settled. Nevertheless, the cases do make clear that the collection and use of subscriber location information will always require a court order based on a showing of probable cause. *See. e.g., In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information,* 407 F.Supp.2d 134 (D.D.C.2006); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747 (S.D.Tex.2005); *In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information,* 396 F.Supp.2d 294 (E.D.N.Y.2005)*; In the Matter of an Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone*

Numbers and the Production of Real Time Cell Site Information, 402 F.Supp.2d 597 (D.Md.2005).

In the case before the District Court in Maryland, the judge rejected the government's suggestion that most cell phone users realize they can be located within a few hundred yards any time their phones are turned on and therefore consent to the tracking of their movement, noting that most subscribers reasonably expect privacy – at least in nonpublic places. *Id.* at 605. To this later point, a recent decision by the Supreme Court of Georgia, the court held that a person traveling along a parkway in his vehicle had no expectation of privacy, and as a result the sending of a signal by the wireless carrier to his phone to locate it at the request of police did not violate the Fourth Amendment right against unreasonable search and seizure, because the warrantless monitoring of the cell phone revealed the same information that could have been obtained through visual surveillance. *Devega v. State*, 286 Ga. 448 (2010). Whether a reasonable expectation of privacy exists in a prison among prisoners (and all others, including authorized users who would also be located through detection technology) is an open question.

Jamming

Jamming technology requires the transmission of radio signals with the intent of interrupting and interfering with (*i.e.*, "jamming") the successful completion of communications on the targeted radio frequencies. Section 333 of the Communications Act of 1934, as amended (the "Communications Act") – the principle Federal statute governing the commercial operation of radio communications, including commercial wireless networks and devices (cellular, PCS, etc.), in the United States – speaks directly to this technology, stating:

> No person shall *willfully or maliciously interfere with or cause interference to any radio communications* of any station licensed or authorized by or under this chapter or operated by the United States Government.

47 U.S.C. § 333. The FCC noted in *In re Imposition of Forfeiture Against Capitol Radiotelephone Inc., et al.,* 9 FCC Rcd 6370, 6380 (ALJ 1994) *aff'd* 11 FCC Rcd 2335 (1996), that the "express language" of the provision makes it clear that the target of the law is any "deliberate act with actual intent to cause interference to a licensee's transmissions." The FCC asserted that its conclusion is supported by the legislative history of the section which makes clear that the purpose of the statute is to prohibit "actions that are expressly designed to cause interference" including "intentional jamming." H.R. Rep. No. 101-316, at 13 (1989). *See also In re Jack Gerritsen,* 20 FCC Rcd 19256, 19259 (EB 2005). FCC decisions distinguish intentional interference, which is prohibited and which will subject the offender to sanction, from occasional unintentional interference incidental to operating in a saturated radio environment. *See, e.g., In re Cordell Engineering, Inc.,* 14 FCC Rcd 7440, 7443-44 (WTB 1999)*; In re Imposition of Forfeiture Against Capitol Radiotelephone Inc., et al.,* 11 FCC Rcd 2335 (Rev. Bd. 1996).

The FCC has had a number of opportunities to consider specifically cell phone disruption technologies and their compliance with the Communications Act. In Office of Engineering and Technology and Compliance and Information Bureau Warn Against the Manufacture, Importation, Marketing or Operation of Transmitters Designed to Prevent or Otherwise Interfere

with Cellular Radio Communications, *Public Notice*, 15 FCC Rcd 6997 (OET, CIB 1999), the FCC's Office of Engineering and Technology (OET) and Compliance and Information Bureau (CIB) issued a Public Notice stating that Sections 301, 302(b) and 333 of the Communications Act (47 U.S.C. §§ 301, 302(b) and 333) and Sections 2.803, 2.1203 and 22.377 of the FCC's rules (47 C.F.R. §§ 2.803, 2.1203 and 22.377) do not permit such jamming devices to be manufactured, imported, marketed or operated in the United States.[4] The Commission reiterated these prohibitions in Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States, *Public Notice*, 20 FCC Rcd 11134 (EB, OET, WTB 2005). A 2006 judicial challenge to the constitutionality of anti-jamming prohibitions was dismissed on jurisdictional grounds. *CellAntenna Corp. v. FCC*, Case No. 06-CV-60430-HUCK (S.D.Fla.2006).

The Commission has denied a number of recent requests to operate – even on a very limited, demonstration basis – cell phone jamming technology. The District of Columbia Department of Corrections (DCDOC) recently sought approval to host a demonstration of jamming equipment at a D.C. jail. Despite being "cognizant of the substantial threat to public safety posed by the use of contraband mobile phones by inmates in prisons and other correctional facilities"[5] and stating that the "demonstration of equipment designed to prevent prisoners' unauthorized wireless telecommunications will benefit public safety,"[6] the FCC's Wireless Telecommunications Bureau (WTB) nevertheless refused to grant operating authority for the jammers on the grounds that it would violate Sections 302 and 333 of the Communications Act and Section 2.803 of the FCC's rules.[7] A similar request to demonstrate jamming technology *for just fifteen minutes* at a Louisiana correctional facility was denied on the same grounds.[8]

The FCC has made it abundantly clear that it will not authorize – *but rather will sanction* – parties who market products that violate the anti-jamming restrictions. *See, e.g., Monty Henry*, DA 08-1202, 23 FCC Rcd 8293, 8294 (May 27, 2008)("[t]he main purpose of cell phone, GPS

[4] Statutory Section 301 states that persons operating or using radio transmitters must be licensed or authorized under the FCC's rules and Section 302(b) prohibits the manufacture, importation, sale, offer for sale, or use of devices that fail to comply with the FCC's regulations. Rule Section 2.803 regulated the marketing of radio frequency devices generally, Section 2.1203 regulates the importation of devices capable of causing interference, and Section 22.377 governs the certification of public mobile radio transmitters.

[5] Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau, to Devon Brown, Director, District of Columbia Department of Corrections, 24 FCC Rcd 2060 (2009)(the "February Letter").

[6] Letter dated January 2, 2009, from Joel D. Taubenblatt, Deputy Chief, Wireless Telecommunications Bureau, to Devon Brown, Director, District of Columbia Department of Corrections, 24 FCC Rcd 23 (2009)(the "January Letter").

[7] WTB initially granted the operating authority in the January Letter, *supra*. However, the demo was called off and the grant of one-day authority became moot after the Cellular Telecommunications Industry Association (CTIA) sought reconsideration and review of the grant by the full Commission, and an order blocking the grant in Federal court. A subsequent request from the DCDOC to demonstrate jamming at the D.C. jail on February 20, 2009 was denied by WTB in the February Letter, *supra*. In denying the grant, WTB noted that its earlier action had failed to fully consider all of the relevant legal issues.

[8] Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, to Howard Melamed, CEO, CellAntenna Corporation, 24 FCC Rcd 3246 (2009).

and other wireless jammers is to block or interfere with radio communications. Such use is clearly prohibited by section 333 of the Act . . ."); *Victor McCormack*, DA 08-1193, 23 FCC Rcd 8264 (May 22, 2008); *Mr. Jean Pierre de Melo*, 22 FCC Rcd 20957 (Dec. 6, 2007); *Curtis King*, 22 FCC Rcd 19162 (Nov. 1, 2007); *Shaker Hassan*, 20 FCC Rcd 10605 (June 9, 2005).

Despite the public interest benefit that will undeniably result from the resolution of the contraband cell phone issue, the FCC has made it clear that the use of jammers for this purpose would require a change of law. Indeed, the efforts to enact the Safe Prisons Communications Act of 2009 (S.251 and H.R.560) reflect the understanding of Congress as well that the FCC will require special statutory authority to allow the operation of jammers in prisons, even on an experimental or temporary basis.

Jamming technology is further hamstrung by the fact that the technology is an "all-or-nothing" solution. The technology blocks *all* subscribers in the areas covered by the jamming signals. It does not selectively permit the completion of calls by authorized users, and more importantly does not allow for the completion of emergency 911 calls or the collection of intelligence under CALEA authority. From a public policy standpoint, the public safety benefit of curtailed contraband cell phone use in prison would need to be weighed against the threat to public safety posed by the wholesale blocking of emergency communications.

Managed Access

By contrast to jamming, Tecore's iNAC managed access solution operates within the current legal and regulatory framework. After extensive consultation with the FCC, Tecore's request for authority to first demonstrate managed access at a Maryland correctional facility was approved and the technology successfully demonstrated. Tecore's request was supported by CTIA and the four carriers operating in the prison area (AT&T Mobility, Sprint, T-Mobile and Verizon Wireless), who each agreed in writing to the coordinated use of their spectrum. The FCC made clear its view that the coordinated and carefully designed use of spectrum pursuant to Commission operating authority is a critical element in the compliance of the solution with the existing language of the Communications Act. Unlike third party solutions which interpose "noise" into the radio frequency environment, the iNAC managed access solution works under leased authority in concern with and as an authentication tool for the licensed wireless spectrum.

In its report on this first demonstration at the Jessup, Maryland, prison, the Maryland Department of Public Safety and Correctional Services (MDPSCS) noted that Tecore's managed access technology was the only solution operated pursuant to FCC authority. *See* Maryland Department of Public Safety and Correctional Services, *Overview of Cell Phone Demonstration*, at 5 (www.dpscs. state.md.us/publicinfo/media/pdf/FinalReport_2008-09-10.pdf). In December 2009, when Maryland officials sought a more thorough[9] demonstration of technologies over a several day operational window, Tecore's managed access was again successfully authorized and demonstrated. For this extended demonstration, Tecore's operating authority came by way of a combination of a renewed and extended Special Temporary Authority (STA) (File No. 0211-EX-RR-2009) and short term *de facto* spectrum leases signed with the carriers and filed with the FCC. (Lease IDs 00006037-6040). The MDPSCS report on the expanded demonstration

[9] The September 3, 2009, demonstration lasted less than two hours.

similarly reflects that Tecore was the only participant to obtain prior FCC approval for the operation of its equipment. Maryland Department of Public Safety and Correctional Services, *Non-Jamming Cell Phone Pilot Summary*, Jan. 20, 2010, at 2. (www.dpscs.state.md.us/media/Cell-Phone-Pilot-Summary_Final.pdf).

As the foregoing demonstrates, the FCC views managed access under applicable communications law *very differently* from jamming. Jammers have been consistently recognized as prohibited by the Communications Act. Meanwhile, Tecore has successfully operated *within* the existing law to demonstrate its technology, attract users, and forge a working relationship with wireless carriers to implement the solution through the coordinated use of spectrum pursuant to long-term leases of spectrum. Operating pursuant to spectrum leases, the solution satisfies Section 301 of the Communications Act and does not offend either Section 302(b) or 333 of the Act or the Commission's rules. Tecore's managed access solution does not interfere with carrier signals, it works in coordination with them to introduce an additional authentication layer into the radio environment.

Unlike cell detection, managed access is effective without the collection of subscriber location data. Whether or not contraband devices are located or confiscated by prison officials, they are rendered ineffective by the managed access signal. Fourth Amendment issues regarding unreasonable search and seizure, and constitutional privacy protections, are not implicated. Moreover, while the iNAC solution affords the ability to gather intelligence under CALEA as may be authorized by court, the typical operation of the iNAC does not require the collection or accessing of private subscriber data or communications content.

Under the rules promulgated by the FCC for the construction and operation of wireless networks pursuant to the spectrum licenses issued by that agency, wireless providers have certain build-out and coverage requirements. Nevertheless, carriers are not required to provide service to all people in all places within the geographic areas they serve. These licensees are free to tailor their networks according to their own network designs. Clearly, wireless providers are legally permitted to restrict their coverage in certain areas – indeed, intelligent frequency reuse requires it. While all of the carriers in the area of a prison could, in theory, re-tool their networks to eliminate coverage of the prison, managed access working in conjunction with these carriers accomplishes the same goals in a more intelligent and cost effective manner.

8. Technical Issues

The identification of technical issues is another factor in investigating and evaluating contraband cell phone use in prisons. Are there any technical issues to be considered for the technologies identified above? For example, the actual range of a jammer depends on its power, antenna orientation, and the local environment (size and shape), which may include hills or walls of a building (that could be made of a variety of materials) that block the jamming signal.

How accurate are the location technologies? Does each site need specific RF engineering for each of the approaches?

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

In a managed access system, separate policies are defined for authorized subscribers, unauthorized subscribers, and calls to 911. These policies are set by the system operator, and may need to comply with state or local laws and regulations. These policies are also approved in advance by the commercial carriers. Authorized subscribers and calls to 911 can therefore be allowed access to the network while unauthorized subscribers are denied. These policies and lists of authorized or unauthorized subscribers can be revised in real time – pursuant to the appropriate security measures – by the iNAC operator.

The iNAC can be configured to match the rules and laws for privacy and operations in a given jurisdiction. Information that is stored can be limited to the extent permitted by the law.

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?

At the RF level the technology and solution provided by the iNAC is driven by the technology deployed by the operator and how they have approved the operations of the solution within their network infrastructure. This is consistent with the iNAC managed access solution providing a coordinated method of operations with each of the operators and technologies.

Technologies that do not differentiate the type of access method are going to be sub-optimal. Jamming, for example, is a blunt instrument which prevents legitimate, mission-critical and emergency communications while addressing contraband cell phone use. Detection does not immediately prevent cell phone use, requires further resource and time to take devices out of service, and does not address cell phones that are off or are separated from their Subscriber Identity Module (SIM) cards. In contrast, managed access does account for the type of access method used by devices, in order to force devices to register with the system and be scrutinized to determine whether each subscriber should be allowed or denied access to the network.

Tecore's managed access solution, the iNAC, has the advantage of a patented multi-technology controller, capable of addressing the commercial carriers, technologies and frequency bands from a common system.

Text-messaging continues to increase as a form of communication from hand-held wireless devices. Wireless hand-held devices in the possession of prison inmates afford them this option as an alternative to talking. 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?

Generally there is not a need to differentiate between voice and text messaging. For purposes of jamming or detection technologies, voice and text messaging use the same frequency bands. For the purpose of managed access, voice and text messaging use the same access technology.

Note that text messaging and broadband (so-called 3G) data are two different services. In the case of 3G voice/data, it is a separate access technology than 2G voice or 2.5G data, and also

often uses different frequency bands. Managed access addresses 3G voice/data differently than 2G voice or 2.5G data. Once again, the iNAC's multi-technology architecture supports all of these access technologies in a common system.

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

Given the iNAC's baseline functionality, the brevity of the communication attempt, or the use of modified equipment (as in the SIM card example above), do not affect the effectiveness of the managed access approach. All unwanted communications will be prevented.

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?

Long-Term Evolution and 700 MHz are simply incremental access methods (the former a technology, the latter a frequency band) that are being introduced into the wireless marketplace, in a continuous evolution that has been occurring since the advent of cellular communications. The technologies and frequency bands currently supported by the iNAC were all introduced at different points in that evolution. As LTE matures (specifically, as devices become commonplace, compact and inexpensive) enough to become a concern for prison officials, it will be available as another access method addressed by the iNAC.

Note that all technology solutions will need to adapt and be upgraded to emerging technologies and frequency bands, so regardless of the solution adopted, periodic maintenance and upgrades should be included in the deployment plan.

CONCLUSION

The problem of contraband cell phones in prisons is pervasive and growing. While forceful countermeasures are required, the corrections community and vendors should be careful about the ramifications of technology solutions under consideration. Jammers can block inmates' calls, but they also prevent legitimate and necessary communications from prison personnel, doctors, nurses and lawyers on the premises, as well as calls to 911. Detection locates the devices but requires corrections personnel to retrieve them, which not only adds to their resource burden, but also means that calls can occur until the devices are confiscated.

In contrast, managed access can truly be considered "the best of both worlds." In a managed access solution, all calls, text messages, e-mails and other cellular communications would flow through a centrally deployed system known as the Intelligent Network Access Controller (iNAC). Communications through authorized devices, or to 911, would be permitted to connect to the commercial cellular networks, while unauthorized devices would be denied access. Additionally, device and call data can be logged for law enforcement forensic analysis.

Corrections administrations get what they want: the ability to prevent contraband cell phones from working, without expending scarce time and effort to retrieve the devices. Regulators are also satisfied: managed access has been found to be legal with respect to existing

U.S. communications law, especially as it has been supported through working in conjunction with the major cellular carrier networks.

In addition to providing comments to the NOI, Tecore Networks respectfully invites NTIA to conduct testing of managed access technology to further enhance the public record on technology solutions to the problem of contraband cell phones in prisons.

Respectfully submitted,

TECORE NETWORKS

By: /Bruce K. Portell/
Bruce K. Portell
Chief Operating Officer

Appendix A: Tecore Networks Corporate Background

Introduction

Tecore Networks has supplied core and radio access networks to mobile operators and government agencies around the globe. In this regard, Tecore is a member of an elite group of companies supplying the infrastructure that serves over 4.5 billion subscribers. The company has developed and patented several innovations in cellular technology, been recognized by major industry groups including the GSM Association and CTIA, and achieved the prestigious ISO 9001:2008 quality certification. Tecore has delivered turnkey systems worldwide, including core and radio access networks based on the major standards – starting with 2G GSM and CDMA, and evolving to 3G UMTS and 4G LTE.

Tecore is headquartered in Columbia, Maryland, and has an Advanced Radio Technology Center in Melbourne, Florida.

Patents

U.S. Patents No. 6,912,230 / 7,733,901. Multi-protocol wireless communication apparatus and method. A scalable, multi-protocol mobile switching center in a wireless communications network provides communications control for digital and analog wireless communications devices including devices that operate according to GSM and IS-41 standards. The hardware and software architecture of the switching center is designed so that processing that is unique to a particular protocol is performed at the lowest possible level, and remaining processing can use generic procedures. The switching center incorporates a home location register and visitor location register that are used in conjunction with software applications to determine the protocol of mobile communications devices using the wireless communications network. The mobile switching center can be used to provide a large scale distributed wireless network or a small scale wireless network. The switching center can also be used as an adjunct to a private branch exchange to provide in-building wireless services and call control. Graphical user interfaces make the wireless communications network easy to maintain.

U.S. Patent No. 7,460,866. Position location for airborne networks. A wireless communications system, and a corresponding method, for use with an aircraft, includes airborne pico cell base stations mounted on the aircraft, the base stations capable of communication with wireless devices used by subscribers on the aircraft via using switching/transaction processing equipment located optionally on the aircraft or in the ground network with one or more ground-based networks. The system includes aircraft location equipment, in communication with the base stations, that determine the aircraft's location, including latitude, longitude, altitude, and other relevant data. Finally, the system includes a wireless communications enable/disable module that receives the aircraft's location and enables and disables wireless communications through the base stations based on the aircraft's location.

Industry Firsts, Innovations and Awards

In addition to patents, Tecore Networks has developed a track record of industry firsts and distinctive capabilities.

2010	Scalable Evolved Packet Core — Available as Software Upgrade to 3G Networks
2009	All-IP 3G Radio Network Controller — First To Interface with Other Vendors' NodeBs
	Intelligent Network Access Controller (iNAC) demonstrated and deployed in prisons around the U.S., registering hundreds of call and message attempts per hour on average, with contraband devices being denied while authorized devices are simultaneously permitted to complete calls.
	ISO 9001:2008 Certification
2008	UMTS Mobile Switching Center — On ATCA, mTCA and Server Platforms
	Achieved USDA "Rural Development Accepted" and "Buy American" status
	Participated in and passed the DoD Interoperability Communications Exercise (DICE)
2007	GSMA Global Mobile Award — Over-the-Air Prepaid Roaming
	Launch FarSite Extended Range GSM Base Station (4x Standard Range)
2006	GSMA Global Mobile Award — Adaptive Array for GSM / GPRS / EDGE
	Launch of Rapid / Rural Deployment System
2002	ISO 9001:2000 Certification
1999	Launch of First Multi-Technology Core Network
1998	GSMA Global Mobile Award — GSM Infrastructure (First Technical Win by A North American Company)
	First Scalable CDMA Core Network
1997	First Scalable GSM Core Network

Appendix B.

Comparison of Managed Access, Jamming and Cell Detection			
	Managed Access	Jamming	Cell Detection
Immediately prevents unwanted communications before they can occur	✓	✓	
Allows calls to 911[10]	✓		✓
Allows authorized or mission-critical use of commercial networks	✓		✓
Complies with U.S. Communications Act (1934)[11]	✓		N / A
Does not require personnel to retrieve devices to terminate communications	✓	✓	
Addresses not only cell phones, but SIM cards as well[12]	✓	✓	
Device, subscriber and call data can be made available for forensic analysis	✓		
Supports Communications Assistance for Law Enforcement Act (CALEA) to enable monitoring or recording of communications for lawful intercept	✓		
Equipment has few physical points of presence, in restricted-access areas[13]	✓		

[10] Certain jamming systems can detect the initiation of a 911 call, and switch off the jamming transmission to allow such a call to connect to the commercial network. During that period, other devices including contraband cell phones may also have access to the commercial network.

[11] As cell detection technology only receives but does not emit radio signals, compliance with the Communications Act is not applicable.

[12] Many cell phones include a subscriber identity module (SIM) card that holds the telephone number, account information and contact list for a subscriber. The SIM card is the size of a postage stamp, can be easily removed and concealed, and can be inserted into a compatible device to allow calls again.

[13] Jamming systems are typically deployed at low power to minimize potential interference; this results in a higher number of jamming devices to cover a correctional facility, often in general-access areas. Cell detection technology requires a high number of transceivers to be placed throughout the facility to enable accuracy of the triangulation methodology. In both cases, the equipment is often accessible, and at risk of being damaged or turned off, by inmates or corrupted personnel. In contrast, managed access equipment requires only a few components that are located in a central secure facility (controller) or at hard-to-reach points such as a water tower (antennas). The high power of the system (from milliwatts to 100 watts) allows coverage of an entire facility from such few points of presence.

Appendix C. Summary Report of Selected Managed Access Demonstrations and Deployments

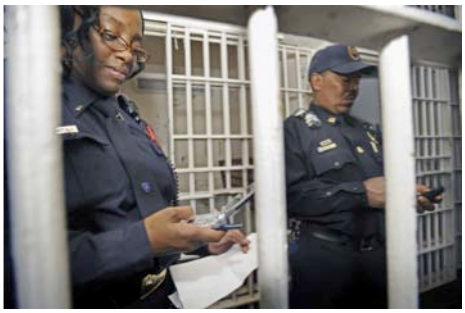
1.0 PILOT DEMONSTRATION FOR THE STATE OF MARYLAND

To demonstrate the product capabilities and the compatibility with the U.S. wireless infrastructure, Tecore participated in a coordinated demonstration of the iNAC solution at the Jessup Correctional Facility in Maryland. The focus of the pilot program was to demonstrate the iNAC capabilities for both GSM and CDMA across multiple operators and frequency bands. The demonstration was carried out during a two day period on September 2-3, 2009. During this timeframe, the operation of the iNAC provided targeted operations on an isolated area of the prison. The iNAC functionality was demonstrated to block unwanted devices from access while allowing other devices to continued access to the commercial network.

The targeted coverage area was the first two floors of an uninhabited cell block approximately a 250 ft x 50 ft structure. Tecore parked the iNAC Mobile Unit in the courtyard in front of the targeted building. The antennas and coverage were directed toward the building and adjusted to provide the iNAC service within the cell block. The targeted cell block was situated approximately one quarter mile from external access to the prison. Additionally the Jessup facility operates under a no cell phone policy within the prison area. The location of the front entrance to this section of the prison is 39° 8'42.00"N, 76°46'47.56“W.

iNAC Mobile Unit

During this demonstration, Tecore executed a set of test cases provided by the Maryland Division of Corrections. The tests validated the effectiveness of the system to block access for unwanted devices across the four major operators. Voice, text, E911 access, and CALEA Lawful Intercept were all demonstrated as part of the exercise. All tests specified by the Maryland DoC passed. When the demonstration concluded, the iNAC was powered down and the devices used all returned to the commercial network.



Maryland corrections personnel participating in demonstration, as photographed by *The Baltimore Sun*

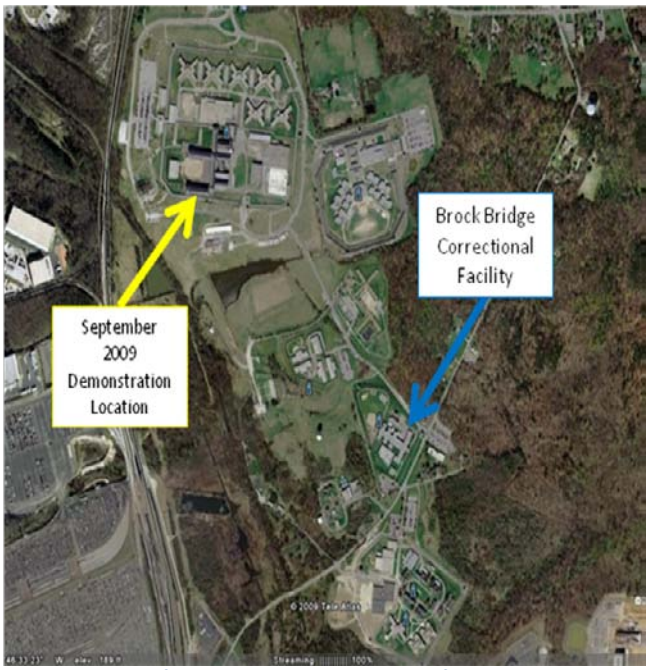
The demonstration was operated with the authorization of a Special Temporary Authority (STA) license granted by the FCC for this purpose as well as coordination of system configuration and coverage footprint with each of the four participating carriers (AT&T, T-Mobile, Verizon, Sprint).

2.0 TRIAL FOR THE STATE OF MARYLAND

To demonstrate the product capabilities and the compatibility with the U.S. wireless infrastructure, Tecore provided a coordinated trial of the iNAC solution at the Brock Bridge correctional facility in Jessup, Maryland. The focus of the trial was to demonstrate the iNAC capabilities for both GSM and CDMA across multiple operators and frequency bands. The trial was carried out during the four-day period of December 15-18, 2009. During this timeframe, the operation of the iNAC provided targeted operations within a fenced in area of the prison. The designated cellblock is currently inhabited with approximately 650 inmates.

This trial expanded on the previous one-day demonstration (described previously) provided in September at another location in the Jessup facility. At the September exercise, Tecore provided a successful trial of the managed access functionality.

The target of the December pilot was to show the effectiveness and applicability of the Tecore iNAC solution to address the issues of illegal cell phone usage within the prison environment for an extended period (multiple days). The functionality included the ability to catch and hold as well as catch and release standard wireless devices from the carrier networks.



Aerial view of demonstration set up for Brock Bridge Correctional Facility

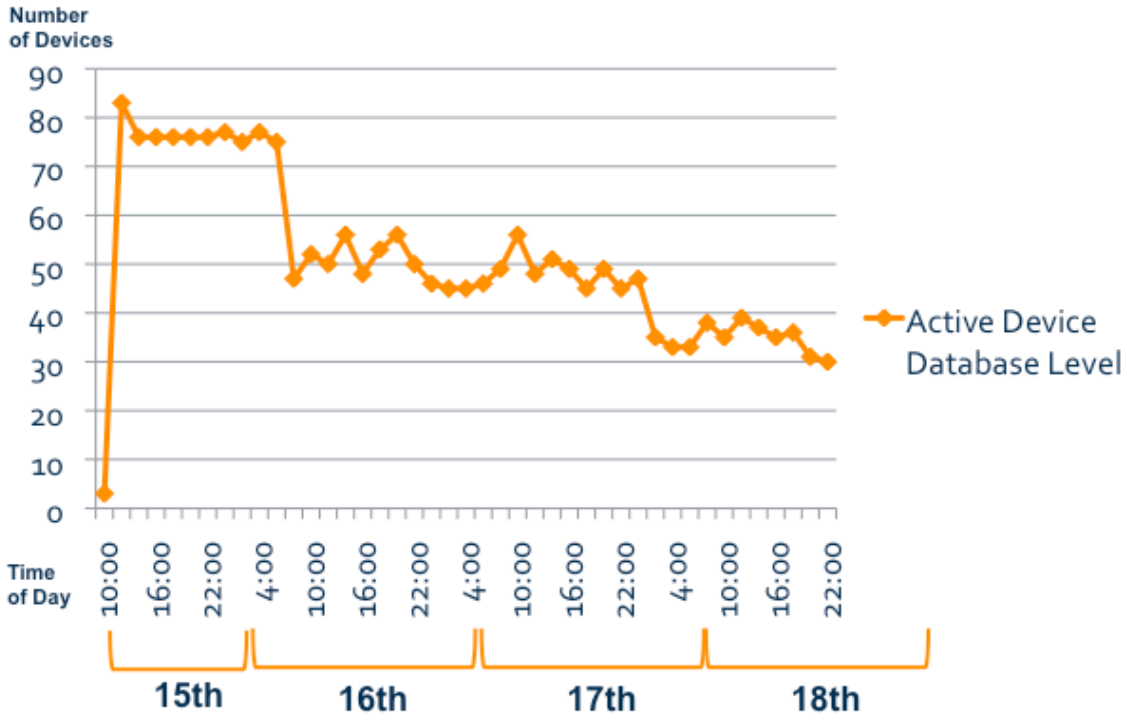
Tecore's coordination of spectrum with the operator community resulted in an effective trial of the technology. The trial was executed under a combination of a Special Temporary Authority (STA) issued from the FCC as well as a coordinated sublease of spectrum from the carriers as applicable. The participating carriers included AT&T, T-Mobile, Verizon, and Sprint.

The trial took place at the Brock Bridge facility in Jessup, Maryland. The target coverage area was the inmate housing area in an 85,000 sq. ft. facility. The structure footprint is approximately a 265 ft x 160 ft. The communications equipment for this trial system was contained in the Tecore iNAC Mobile Unit. Tecore parked the communications van in the parking lot location to provide coverage of the targeted facility. The antennas and coverage were directed toward the building and adjusted to provide the iNAC service within the fenced area. The entire Jessup facility operates under a no-cell phone policy within the prison area. The location of the front entrance to this section of the prison is 39° 8'4.06"N, 76°46'26.79"W.

2.1 iNAC ACTIVITY LEVELS

The chart below shows the level of active devices on the iNAC system during the period of the trial. The data was collected after the audit on the system was executed to remove any devices with an inactivity period of

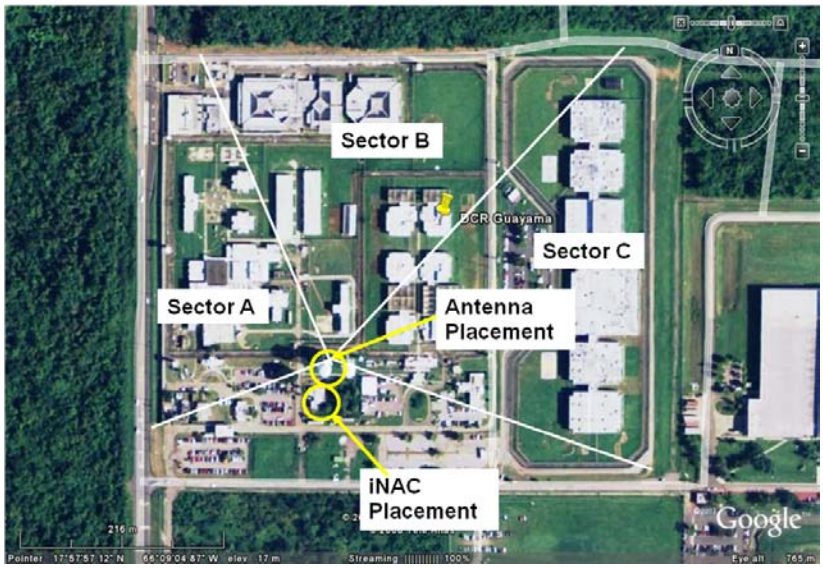
longer than 2 hours. An expected trend during the operation of the system is a downward step of utilization, as the illegal devices can no longer be used within the facility. The data observed over the three and one half day period followed this trend as evidenced below.



3.0 PERMANENT SYSTEM DEPLOYMENT

The iNAC technology has been successfully deployed and implemented in a prison facility in the Caribbean. The system has been in operation for over a year and has proven to be an effective alternative solution to the jamming equipment that was previously installed. The system deployment is coordinated across nine (9) operators and provides blanket coverage for the facility that is ¼ mile x ¼ mile. The Warden and corrections officers utilize one of the commercial operators as their in-house communications system. So the iNAC provides a combination of positive users who are allowed access to the commercial network as well as unknown and negative users who are accepted to and held on the iNAC signal. The prison is divided into three primary regions (Administration, Minimum Security and Maximum Security). All of these areas are covered by the INAC utilizing multiple antennas. The prison layout is shown in the picture below.

In the diagram, Sector A is the Administration buildings, Sector B is primarily Minimum Security and Sector C is primarily Maximum Security.



Aerial view of iNAC deployment in Maximum Security Prison

The iNAC solution replaced the 20+ low power jammers that were previously installed at the facility. Due to the low power output and the need to control the jamming footprint, many of these were installed in accessible locations. The iNAC replaced this equipment with three (3) standard sectorized antennas mounted to a water tower and two repeaters (used in the Super Max facility). This reduction in RF equipment and inaccessibility has reduced the opportunities for sabotage and vandalism of the equipment. The iNAC-controlled equipment is installed in a secured 10x10 shelter outside the accessible areas of the complex and is remotely monitored via an IP connection.

A typical day for this iNAC can see upwards of 1,000 call attempts and other access attempts to the network. Many of these call attempts are from inmates trying to call 611 (customer service) to complain about their service problems.