Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
	)	
Wireless Service Interruptions	)	GN Docket No. 12-52

To the Chiefs, Public Safety and Homeland Security
and Wireless Telecommunications Bureaus

REPLY COMMENTS OF TECORE NETWORKS

TECORE NETWORKS

7061 Columbia Gateway Drive
Columbia, Maryland 21046
(410) 872-6000

May 31, 2012

TABLE OF CONTENTS

I. Response to Comments

A. CellAntenna Corporation..... 1

B. Global Tel*Link Corporation..... 5

C. Digital Receiver Technology, Inc..... 10

II. California Report on Managed Access..... 11

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
	)	
Wireless Service Interruptions	)	GN Docket No. 12-52

To the Chiefs, Public Safety and Homeland Security
and Wireless Telecommunications Bureaus

REPLY COMMENTS OF TECORE NETWORKS

Tecore Networks ("Tecore") hereby submits these Reply Comments in the above-referenced docket addressing issues related to the intentional interruption of wireless service in the interest of public safety.

I. Response to Comments

The several comments submitted in this proceeding which discuss the interruption of wireless service within the nation's prisons in the interest of public safety are consistent in their identification of the compelling challenge faced by prison officials and the public at large from the increasing proliferation of contraband wireless devices in the hands of prison inmates. Tecore disagrees, however, with certain of the conclusions advanced by these commenters regarding what form the solution to the contraband problem should take.

A. CellAntenna Corporation

In its comments, CellAntenna Corporation ("CellAntenna"), which has vigorously advocated the legalization of jamming technology to address the problem, correctly characterizes the problem for prison officials as "well documented and growing. Regardless of size, location,

security level or design of the correctional facility, most have located and seized contraband wireless devices."[1] CellAntenna correctly notes, further, that prison officials throughout the United States "desperately wish to interrupt wireless service within each correctional facility to render contraband wireless devises unusable."[2] The commenter aptly states the essential merits of addressing the problem of contraband devices through managing access to the commercial networks, noting that "[i]f wireless service is interrupted, contraband wireless devices will not work. If the devices do not work, the threat to public safety occasioned by contraband wireless devices within the zone of the interruption is stopped in its tracks."[3] CellAntenna rightly concludes that interrupting wireless service and rendering contraband devices useless, without the need to detect and confiscate the devices, best serves the public interest because "for so long as the wireless device is unusable, the public is safe from the havoc that a wireless-enabled inmate might wreak on unsuspecting victims."[4] CellAntenna also is correct on the law that there is "no [F]irst [A]mendment right to use a wireless device inside a correctional facility."[5]

CellAntenna, however, has long been an advocate of signal jamming as the solution to the contraband problem, and again advances this solution in its comments. Yet despite its well-known advocacy for jamming, CellAntenna admits in this proceeding – and correctly so – that *managed access* exercises more "discretion" than jamming because it interrupts only *unauthorized* communications – *i.e.*, non-emergency communications from unauthorized users –

[1] *Comments of CellAntenna Corporation* at 3.

[2] *Id.* at 4.

[3] *Id.* at 6.

[4] *Id.* at 7.

[5] *Id.* at 9-10.

whereas jamming is an *all-or-nothing* solution.[6] Tecore welcomes this recognition of the benefits of managed access from the company which, historically, has led the fight for legalizing jamming in the United States.

Yet despite its recognition of the benefits of managed access, CellAntenna advances the position that the interruption of *all emergency 911 communications* within a prison, along with all non-emergency communications, is an acceptable solution, and presents a risk than can be "assumed and managed by the corrections facility."[7] Tecore disagrees. Tecore believes, and has aggressively advocated before the Commission, that the preservation of emergency 911 calling, *even from otherwise unauthorized devices*, serves a critical public policy objective. Because a solution to the contraband cell phone problem exists – managed access – that takes advantage of the "discretion" noted by CellAntenna to both deny unauthorized inmate communications yet safeguard the integrity of all emergency calling, solutions like jamming, that also are not authorized under current law, are unworthy of serious consideration.

Tecore further disagrees with CellAntenna's assertion that the Commission has the legal authority, pursuant to Section 10 of the Communications Act of 1934, as amended (the "Act"), to forbear from enforcing Section 333 of the Act and thereby permit jamming without Congressional action.[8] Section 10 of the Act provides that the Commission may forbear from applying a statutory provision or regulation to a telecommunications carrier or service (or a class of telecommunications carriers or services) if the Commission determines: (1) enforcement is not necessary to ensure that the carrier's charges, practices, classifications or regulations are just,

---

[6] *Id.* at 7.

[7] *Id.* at 9.

[8] *Id.* at 2-3, 10-11.

reasonable and not unjustly or unreasonably discriminatory; (2) enforcement is not necessary to protect consumers; and (3) forbearance from enforcement is consistent with the public interest.[9]

Section 10 was enacted by Congress as part of the 1996 amendments to the Act which largely were deregulatory in nature. In enacting Section 10, Congress specifically noted that the provision was intended to give the Commission the authority to forbear from enforcing statutes and regulations *that are no longer "current and necessary in light of changes in the industry*."[10] Congress found that in order to "improve the [1996 amendment's] deregulatory nature," it needed to give carriers the ability to compel the Commission to exercise its authority "to forbear from regulating."[11] In adopting procedural rules for carriers seeking such forbearance, the Commission noted Congressional intent in enacting Section 10 and made clear that any forbearance request must address each prong of the statute as it applies to the particular provision from which a petitioner seeks relief."[12]

Clearly, CellAntenna's request neither comports with the spirit nor the letter of Section 10. It cannot fairly be said that the prohibition on jamming mandated by Congress through Section 333 of the Act is no longer "current or necessary" in light of changes in the industry. CellAntenna has failed to demonstrate how forbearance in this instance would satisfy this or any of the legs of the three-prong test required in a forbearance request. CellAntenna has failed to show how permitting the deployment of a technology which admittedly blocks the completion of

---

[9] 47 U.S.C. § 160(a). In determining whether forbearance is consistent with the public interest, the Commission must consider "whether forbearance from enforcing the provision or regulation will promote competitive market conditions." 47 U.S.C. § 160(b).

[10] 141 Cong. Rec. S7893 (Jun. 7, 1995) (remarks of Sen. Pressler)(emphasis added).

[11] 141 Cong. Rec. S8069-70 (Jun. 9, 1995) (remarks of Sen. Pressler).

[12] *Petition to Establish Procedural Requirements to Govern Proceedings for Forbearance Under Section 10 of the Communications Act of 1934, as Amended*, WC Docket No. 07-267, Report and Order, 24 FCC Red 9543 (2009) at ¶ 11.

all wireless emergency 911 communications within its coverage zone would be consistent with the public interest, when technologies with more "discretion" are available.

It is important to note that the Commission has previously been presented with specific requests to forbear from enforcement of Section 333, and has to date elected to continue to enforce Section 333, and rightly so.[13]

*B. Global Tel*Link Corporation*

Global Tel*Link Corporation ("GTL"), like CellAntenna and Tecore, finds a compelling need for wireless service interruption at the nation's prisons.[14] With its significant experience with the corrections industry, GTL correctly opines that "there has been an explosion of wireless devices" which has undermined "the attempts of law enforcement and correctional officers to regulate inmate communications in a safe and consistent way" and that U.S. officials "have concluded that only an interruption of wireless service to those devices can fully address the crisis."[15] GTL rightly urges the Commission to take decisive action "with the ultimate goal of comprehensively restoring safety and security to our nation's correctional facilities."[16]

---

[13] *See In re Petition of the GEO Group, Inc. for Forbearance from Application of Sections 302, 303 and 333 of the Communications Act of 1934, as amended, and Section 2.803 and 2.807 of the Commission's Rules to Allow State and Local Correctional Authorities to Prevent Use of Commercial Mobile Radio Services at Correctional Facilities*, Petition for Forbearance, ET Docket No. 08-73, July 31, 2007. Indeed, the Commission has vigorously enforced Section 333, and has refused to permit jamming pursuant to declaratory ruling (*In re Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammer and Wireless Boosters and Repeaters*, Petition for Declaratory Ruling, (RM proceeding pending), Nov. 2, 2007), request for special temporary authority (*Letter from Howard Melamed, CEO, CellAntenna Corporation, to Marlene H. Dortch, Secretary, Federal Communications Commission*, Request for Special Temporary Authority, Mar. 3, 2009), and rulemaking (*In re Amendment of Section 2.807 of the Commission's Rules (47 C.F.R. § 2.807) to Allow the Use of Radio Frequency Jamming Equipment by Local and State Law Enforcement Agencies and Emergency Response Providers*, Petition for Rulemaking, RM-11430, Jun. 12, 2007).

[14] GTL is a provider of authorized inmate telephone services and is the company with which Tecore worked in deploying the Tecore Managed Access solution at the Mississippi State Penitentiary at Parchman, Mississippi. *See Initial Comments of Global Tel*Link Corporation* at 7-8 [hereinafter, "*GTL Comments*"].

[15] *Id.* at 1-2.

[16] *Id*. at 2.

Tecore agrees with GTL's conclusion that "[m]anaged access meets the outstanding needs of correctional facilities to combat inmate wireless calling in a minimally invasive fashion" and provides "a backdrop to prison phone services, which have proven less and less effective with the passage of time" by assuring corrections officials that "any wireless device an inmate manages to obtain will not be able to function, lessening the consequences of an unsuccessful investigation for contraband or a partially-effective jamming system."[17] In addition, GTL properly concludes that managed access systems provide the added benefit of permitting corrections officials "to engage in forensic analysis of the device and call information, a vital tool in law enforcement unavailable with conventional jamming," and benefit from their "innate scalability and adaptability" to suit a broad range of corrections facilities, which means the solution "can be tailored in placement and functionality according to the specific needs and architectural demands" of individual facilities and "can adapt to shifts in spectrum allocation and technological advancement."[18]

GTL's comments also aptly note that the wireless service industry as a whole, which has vigorous opposed and "expressed dismay at the potential side effects of jamming, have praised managed access as a 'promising technological solution'" that addresses the problem of contraband devices yet avoids interference to legitimate wireless users.[19] Citing a study by VComm Telecommunications Engineers, GTL notes that "a managed access system allows calls placed in prisons to be monitored and directed appropriately, while offering important public safety advantages: it allows E911 emergency calls and CALEA calls within and without prison

[17] *Id*. at 20-21.

[18] *Id.* at 21-22.

[19] *Id*. at 22.

facilities, transmits at lower levels than jamming systems to effectuate call capture, and '[c]an intercept Nextel/SMR calls within prisons without interfering with Public Safety radios.'"[20] Indeed, GTL is precisely on point when it states that the long-term technological solution to the problem of contraband wireless devices in prison "must be in the form of economical, scalable and targeted managed access solutions."[21]

Although Tecore pioneered with the Commission the spectrum lease approach to authorizing the operation of managed access systems in prisons within the coverage area of commercial wireless licensees, and has received remarkable cooperation to date from the wireless industry in the testing and deployment of managed access systems, Tecore wholly agrees with the conclusion reached by GTL that it is "necessary for *all* wireless carriers to permit the introduction of wireless interruption technology into the nation's correctional facilities." GTL echoes what Tecore has advocated in this proceeding – that all wireless carriers are "bound to act in the public interest by the terms of their licenses" and therefore "must universally facilitate" the introduction of managed access solutions in the nation's prisons in order to "comprehensively forestall the completion of illicit transmissions from prison cells." Tecore wholeheartedly agrees with GTL that "[i]ndustry reticence over focused interruption of portions of the electromagnetic spectrum, or selective opt-out on the part of particular carriers, will have disastrous consequences." Tecore likewise agrees with GTL that the Commission must act with regard to reluctant wireless carriers "to ensure their cooperation."

---

[20] *Id.* at 22-23. Although Tecore does not agree with their analysis in its entirety, Tecore does agree with GTL in its conclusions that managed access systems are neither a risk (including a liability risk) to emergency communications or to commercial wireless service outside a prison, even in urban settings. *Id.* at 23-25.

[21] *Id.* at 3. GTL acknowledges that in reaching this conclusion, it has "explored alternative solutions to the crisis, including detection and jamming" and that "the benefits of managed access technology" led GTL to work with Tecore in deploying the Parchman system. *Id.* Tecore concurs in GTL's analysis that Section 333 of the Act is not applicable to managed access systems in corrections facilities, and that First Amendment concerns of free speech likewise are not an impediment to the interruption of contraband devices in prisons. *Id.* at 26-28, 32-37.

Where Tecore believes GTL is wrong, however, is in connection with what actions the Commission should take. Indeed, GTL makes a distinctly circular argument in its comments in this regard. GTL advocates for the immediate expansion of the "PROTECT Initiative" to include the deactivation of contraband devices in prison as a principle defense in the fight against contraband devices in prisons.[22] GTL advocates for the availability of managed access systems in prisons (as stated above), but only "to the extent that an expansion of the PROTECT Initiative to correctional facilities proves insufficient."[23] GTL touts the potential effectiveness of the deactivation effort because companies like GTL "can identify the International Mobile Equipment Identity ("IMEI") associated with each mobile device unlawfully used in a prison."[24]

What GTL fails to acknowledge is that *it is precisely a managed access system installed at a prison that will provide prison officials and their contractors, like GTL, with the technical means to identify the IMEIs required for deactivation*. The universal availability of managed access systems is not a long-term "only if" solution, as GTL suggests, but rather is *the immediate solution* that will render contraband devices unusable from day one, whether or not a prison administration elects to take the next step of working with wireless carriers to deactivate the unusable device. Although Tecore does not believe that the deactivation of stolen devices is a bad idea, in point of fact once a device is unusable, the need for deactivation becomes irrelevant, and would be a wasteful application of limited prison resources if applied to contraband devices.

---

[22] *Id.* at 2-4, 39-40. The PROTECT Initiative was recently inaugurated and is designed to create a national database of stolen wireless devices to prevent their reactivation and use by criminals. *See* Remarks of Chairman Julius Genachowski on the Stolen Cell Phones Initiative, Apr. 10, 2012 (*http://transition.fcc.gov/Daily_Releases/ Daily_Business/2012/ db0410/DOC-313512A1.pdf*).

[23] *GTL Comments* at 3.*Id.*

[24] *Id.*

Tecore further disagrees with GTL that the Commission should use its licensing authority over commercial wireless carriers to compel their universal participation in the expanded PROTECT program.[25] If the Commission is inclined to use its licensing authority to create conditions that compel the participation of all commercial wireless carriers licensed in the United States to cooperate with prisons in combating contraband devices, it would be much wiser and more efficient and effective for the Commission to compel all carriers to make spectrum rights available for the operation of managed access systems in prisons (or the provision of managed access directly by the carriers), as Tecore advocates in its comments.

Tecore most strongly disagrees with the portion of GTL's comments wherein it urges the Commission to use its regulatory authority to "require that entities seeking to deploy a wireless interruption system . . . provide their services through an authorized provider of telecommunications services selected by the correctional facility."[26] Tecore agrees that, given the technological complexities of managed access, "[p]ermitting entities with no known qualifications . . . to install and operate sensitive telecommunications infrastructure" would border on the "reckless and irresponsible." However, this does not warrant the requirement that corrections officials be precluded from deploying managed access directly, or through any competent contractor, so long as the system can be effectively deployed and managed. Indeed, the upcoming Maryland deployment of the Tecore Managed Access solution would be precluded under GTL's proposal because the deployment is not being implemented through an inmate telephone service provider. As Tecore has advocated to the Commission in pioneering managed access, the attraction of including an inmate telephone services provider in the equation is that it

[25] *Id.*

[26] *Id.* at 40.

presents a vehicle for funding the deployment, which is useful for cash-strapped corrections departments. Inmate telephone contractors, nor indeed any other corrections contractor, should not be a required part of any deployment. This is an administrative decision best left to each corrections department.

C. Digital Receiver Technology, Inc.

Digital Receiver Technology, Inc. ("DRT"), a wholly-owned subsidiary of aerospace giant Boeing, also filed comments in this proceeding discussing the interruption of wireless services to address the contraband problem in prisons. DRT states that it manufactures "wireless management devices that emulate a base station to detect and manage wireless handsets of concern in a limited geographic area." DRT states that its base station emulation equipment operates "without *significantly affecting* normal [wireless] traffic" and "without a *wide impact* on legitimate wireless communications in the area." DRT touts its solution as a device that can "dramatically *reduce the impact* of wireless service management on legitimate communications."[27] Although Tecore agrees with DRT that corrections officials should have the ability to selectively interrupt wireless services in prisons, Tecore also believes the Commission would have benefitted from DRT explaining in detail in its comments the degree to which its proposed solution to the problem causes *any impact* on legitimate wireless traffic, reduced or otherwise. The DRT comments are lacking in any such details.

In this regard, a report authored by the California Council on Science and Technology ("CCST") on managed access systems, discussed in greater detail in Section II of these reply comments, identified numerous concerns with the managed access system provided by DRT for demonstration to the California Department of Corrections and Rehabilitation ("CDCR"), and

[27] *Comments of the Boeing Company* at 1, 4, 6 [emphasis added].

indeed recommended that California not proceed with the deployment of its chosen managed access system because of these concerns.[28]

II. California Report on Managed Access

Since the deadline for the filing of comments in this proceeding, the CCST[29] issued a report entitled "The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons."[30] Tecore believes it is important to discuss the CCST Report here so that the Commission will have benefit of both the report's assessment of developments in the managed access marketplace, as well as Tecore's thoughts on the portions of the CCST assessment which warrant comment.

In its letter transmitting the results of their study, the CCST stated that they had analyzed "a specific proposed system for managing cell phone access in prisons, Managed Access Systems (MAS)" and were thereby rendered their conclusions regarding "the proposed MAS recently contracted for by the California Department of Corrections and Rehabilitation" – *i.e.*,

---

[28] *See generally* California Council on Science and Technology, *The Efficacy of Managed Access Systems to Intercept Calls from Contraband Cell Phones in California Prisons*, May 2012 (*http://www.ccst.us/publications/2012/2012cell.pdf*)[hereinafter, "*CCST Report*"]. *See also, infra*, at Section II. The CCST Report recognized Tecore and DRT as the only two vendors "of sufficient size to attempt to develop and implement the MAS for the California State Prison system" and concludes that all other "vendors of technologies that might be configured for the MAS … were not considered to have sufficient size of qualifications to be viable enough to include in [its] report. *Id.* at 17.

[29] According to its report, the CCST is an independent non-profit 501(c)(3) organization established in 1988 at the request of the California state government with a mission is to "improve science and technology policy and application in California by proposing programs, conducting analyses, and recommending public policies and initiatives that will maintain California's technological leadership and a vigorous economy." *Id.* at ii.

[30] The study was undertaken by the CCST at the request of several members of the California State Senate who requested that the CCST conduct an assessment of "managed access" technology, a technology which the senators identified as the subject of a pilot study conducted by the CDCR and technology that was "previously tested and/or employed in Mississippi, Maryland and South Carolina prisons." *Id.* at 3-4. It is important to note that the technology reviewed in the CCST study, from DRT, is not the technology "previously tested and/or employed" in Mississippi and Maryland. Tecore's very different technology was tested and deployed in Mississippi and Maryland. This technology has also now been selected for full-scale deployment at Maryland's Metropolitan Transition Center, an urban corrections unit in downtown Baltimore. The technology tested in South Carolina also was not Tecore's technology.

the base station emulation technology developed and made available by DRT.[31] The CCST Report concludes that although "the technology shows promise, but it is not ready for deployment." The CCST characterizes the testing conducted on the DRT technology in California as "preliminary" and "limited in scope and scale," describing it as "essentially a proof of concept trial rather than a full-fledged pilot program that takes into account the complexities of interference from the prison structure itself and surrounding locale."[32]

Unlike the Tecore solution, which the CCST Report correctly identifies as "an intelligent network access controller" and describes as "a small-scale cell phone network that operates exactly as a service provider network such as AT&T or T-Mobile," the DRT system tested in California was not a managed access system at all, but rather was "cell phone test equipment configured to 'act' as a managed access system."[33] The DRT solution "uses test equipment that emulates the base stations and phones as well as the operational radio network controller function" which were "configured to be a MAS capable system."[34] The CCST team found no evidence that the system tested in California "was implemented as a fully operational MAS." Indeed, the entire pilot test conducted at the CDCR lasted just 96 hours and was conducted using just one cell phone of each wireless service provider, each supplied by Shawntec, the inmate telephone provider implementing the test.[35]

---

[31] *Id.* at 1-2. Tecore's proprietary technology does not "emulate" commercial wireless base stations, and operates in conjunction with Tecore's patented multi-technology core.

[32] *Id.* at 1.

[33] *Id.* at 17.

[34] *Id.* at 18.

[35] *Id.* at 22.

Against this backdrop, it is no wonder the CCST concluded the technology is "not mature enough for immediate large-scale deployments," that "[a]lternative options for mitigating Contraband Cell Phones should be considered before adoption of MAS," and that the deployment of managed access in CDCR facilities should be delayed.[36]

Although the CCST project team appeared to understand generally the differences between the technology trialed (and now planned to be installed, despite their recommendation) at California prisons, the team failed to sufficiently distinguish between the numerous deficiencies it found in the solution trialed in California and the Tecore Managed Access solution successfully trialed in Maryland, deployed in Mississippi, and currently being deployed in Maryland. Indeed, the CCST project team did not understand or accurately reflect in its report that the Parchman system is a fully-deployed, fully-operational managed access system, and has been so for nearly two years[37] – it is not "still unproven" or a solution for which "the jury is still out on the ability of this approach to be applicable in a prison environment" as suggested by the CCST.[38]

While it might be true for the solution trialed by California that data is "scarce" due to "the infancy of the MAS marketplace and the early stage of product development,"[39] the Parchman deployment, now nearing the end of its second year of full-scale operation, and the two separate trials of the same solution at Maryland prisons which preceded the Parchman

[36] *Id.* at 6-7.

[37] Although the CCST report correctly identified the Mississippi as the only state that has to date deployed an operational MAS system, it incorrectly characterizes the Parchman system as a "pilot operation" and wrongly states that it was "not fully operational as of November 2011." *Id.* at 15, 18. As a result, it incorrectly states that "there are no prisons anywhere in the United States using a fully functional managed access system to control cell phone use." *Id.* at 1.

[38] *Id.* at 23.

[39] *Id.* at 17.

deployment, provide a robust set of performance data. Far from unproven, in February/March of this year the Parchman system successfully interdicted its 2 millionth call/data transaction. At a December 2011 meeting on the future operation of the Parchman system organized by the Commissioner of the Mississippi Department of Corrections ("DOC"), Christopher Epps, and attended by Tecore, GTL and representatives of the commercial wireless carriers who provide spectrum rights in the area, the Mississippi DOC, GTL and the carriers all confirmed that there were no operational issues – including, perhaps most importantly, carrier interference issues outside the walls of the prison – with the Parchman system.[40]

Further, the CCST Report wrongly states that unresolved operational issues have so far prevented the deployment of managed access systems to the other two Mississippi penitentiaries.[41] On the contrary, the further deployments in Mississippi have been the result of administrative roadblocks and not the result of performance issues with the Parchman system. Tecore encourages the Commission to validate this matter directly with Commissioner Epps and the Mississippi DOC.

Although the CCST Report correctly states that an MAS system can only interrupt communications from devices operating on the same radio technologies on which the MAS system operates, it wrongly concludes that "as new technologies develop there will be a time lag to identify them and to respond with an upgrade in the MAS ability to detect them." It appears that the CCST drew this conclusion from the fact that the IFB stated that the CDCR would give its MAS vendor one year from the commercial availability of a new technology to incorporate

[40] The meeting focused principally on ways in which the operations of the managed access system and the commercial wireless networks can be effectively coordinated in the future as new spectrum and technologies are introduced into the radio environment at Parchman.

[41] *Id*. at 15.

the technology into the MAS solution.[42] The CCST conclusion reflects a fundamental lack of understanding of the pace and manner in which new wireless technologies are developed and commercially deployed, and the real-world evolution of legitimate managed access solutions – *i.e.*, the Tecore Managed Access solution – in the marketplace.

New wireless technologies take years to develop from concept, through standards development and equipment design and manufacture, to testing and final full-scale commercial deployment. New technologies are not "sprung" on the marketplace overnight. Long Term Evolution ("LTE") technology, for example, was first conceived and preliminarily defined before its initial incorporation in 2007-2008 into on-going 3G/4G international standards-setting efforts. Standards setting and equipment development progressed to the point of first testing and trials in 2010. Only now are we seeing commercial deployments of LTE technology, and it is so far very limited.

Vendors who do not cobble together manage access solutions from test equipment and spare parts, but rather like Tecore deploy managed access solutions that leverage their development and deployment of equipment incorporating new technologies which they already will be producing for the wireless industry,[43] are well positioned to stay ahead of the deployment of new technologies and the need to timely evolve their managed access solution. Indeed, the Parchman deployment has already been timely and successfully evolved to address the

[42] *Id.* at 17.

[43] The CCST Report characterizes as a negative the fact that current MAS systems "are not custom designed for use in correctional environments" but rather are miniature cell phone networks. *Id.* Perhaps this is a negative for MAS solutions rigged from test equipment. However, it is a distinct advantage that the Tecore Managed Access solution is a novel application of the existing wireless infrastructure equipment designed, produced and sold by Tecore to commercial and governmental users around the world for 20 years. Although elements of the equipment are custom designed to impede communications rather than enable it, the robust commercial-grade capabilities, scalability and proven performance record of the equipment tested by 20 years of commercial deployments is of great benefit and should be of great comfort to corrections officials. Moreover, the developmental costs which would be associated with solutions custom designed from the ground up can be avoided and do not need to be passed on to cash-strapped corrections departments.

introduction of 3G technology into the radio environment at Parchman. These upgrades were neither "disruptive" or resulted in "long periods of inferior performance" as cautioned by the CCST.[44] The deployment underway in Maryland incorporates iDEN[45], WiMax and 4G/LTE technologies not required to date for the Parchman deployment.

The CCST fails to point out, but it is no less true, that a successful MAS system must operate in all of the radio spectrum bands in which the contraband devices held by inmates can operate. However, just as a legitimate and reliable MAS solution like the one deployed by Tecore is set to keep pace with the evolution of wireless technology, a similar process already exists with the commercial carriers providing spectrum to coordinate their introduction of new radio spectrum into the commercial environment so that the MAS system can continue to interdict contraband devices across all operable frequency bands.

The CCST Report concludes that the "proposed MAS approach … lacks the capability to be simply modified for new cell phone communications technologies" and that "[e]ach and every upgrade of the MAS systems will be tantamount to a complete new installation."[46] While the MAS solution tested in California and proposed for deployment throughout their state prison system may suffer from these deficiencies, it is incorrect to characterize upgrades to the Tecore solution in this manner. Again, Tecore encourages the Commission to hear directly from the Mississippi DOC whether the evolution of the Parchman system was "tantamount to a complete new installation" either in terms of cost or practical impact.

---

[44] *Id*. at 18.

[45] The incorporation of iDEN technology was made more difficult by the proprietary nature of the technology to Motorola Inc. Nevertheless, an iDEN solution is available from and will be first implemented by Tecore at the current Maryland deployment.

[46] *Id*.

The CCST Report reflects the assessment team's misunderstanding of the operation of a properly-deployed managed access system. Again, perhaps their misperceptions stem from the type of solution tested and proposed to be deployed in California. The CCST Report questions the ability of an MAS system to capture text messages, concluding that "[b]ecause texts can be sent very quickly, the efficacy of the MAS in blocking these has not been proven."[47] A properly designed and properly deployed MAS, like the one at Parchman, is equally effective at interdicting voice and data (including text) communications. Since each form of transaction is required to go through the same authentication process with the wireless network, any attempted transaction from an unauthorized user will be blocked. Text messages will be no more successful than voice calls.

Equally misunderstood by the CCST team are communications incoming to the wireless device and those that are outgoing from the device. The report asks the wholly inapposite question of "what would happen if the MAS attempts to block a service provider base station." It is conjectured that if an incoming call could be processed faster than an outgoing call, then the MAS may be incapable of blocking the communication.[48] It is elemental, however, that to receive an incoming call, a wireless device must be turned on. When an unauthorized wireless device within the target area of the Parchman MAS, for example, is turned on, it must be authenticated as a valid user before it can *make or receive* any form of user communication. It is in this process that the unauthorized device gets captured and blocked. At this point it is

[47] *Id.* at 20. The report discussed the relative set up time for a voice call transaction and a text message transaction, as well as the blocking requirements set out in the California IFB, and draws the conclusion essentially that an MAS system will not be quick enough to block text messages and inmates will exploit this limitation.

[48] *Id.* at 20-21.

incapable of any form of incoming or outgoing communication because it cannot reach a network that will allow such transactions.

In addition, the CCST Report questions whether the MAS system "could be effectively managed" by prison officials and the vendor operating the system.[49] Again, this question may have its root in what was noted earlier in the report that the MAS system tested in California "did provide a cell phone blocking function, but it was not automated" and that it was "very manpower intensive and never operated in a standalone mode."[50] As stated above, the Parchman system has now been in full-scale operation for nearly two years, and no operational issues were raised by Mississippi corrections officials, the system operator (GTL) or the wireless carriers providing spectrum rights for the system at the December 2011 meeting with Commissioner Epps. While the system cannot and should not be operated without human involvement, it is false to characterize the Parchman solution as requiring "significant human intervention and operational action" (a criticism leveled at the system trialed in California) or is incapable of effective management.[51] On the contrary, the system is being well managed and is operating superbly.[52]

The CCST Report expresses concern that MAS systems pose substantial threats outside the prison to both normal public communications (including emergency 911 calling) and to communications by public safety officials due to the lack of "the finite systematic radio power

[49] *Id*. at 23.

[50] *Id*. at 18.

[51] *Id*. at 20, 23.

[52] In a January 2012 interview with the Jackson, Mississippi *Clarion-Ledger* newspaper, Commissioner Epps noted that since its installation, the system has blocked about 1.8 million illegal cellphone calls and text messages, and was upgraded to manage 3G technology. Commissioner Epps noted that a single managed access technician had been hired to maintain and monitor the system. *Mississippi prisons crack down on cellphones, Facebook*, ASSOCIATED PRESS, Jan. 20, 2012, http://blog.gulflive.com/mississippi-press-news/2012/01/mississippi_prisons_crack _down. html.

level control capability necessary to prevent interference in real time, "*i.e.*, there is no way to determine if the radio signal it generates could or is causing interference outside the confinement area of the prison." This so-called "RF dispersion" issue, as characterized by the CCST assessment team, "means the MAS system's radiated energy cannot be allowed to propagate beyond the specific physical confines of the prison area." The report concludes that such "RF leakage" might not present a problem at rural prisons, but in more populated settings "could be highly disruptive to cell phone usage by the non-prison population." Such disruption could "greatly reduce the capability of public safety professionals to serve the community's needs or the general public's ability to access a 911 operator."[53]

These conclusions simply do not apply to the Tecore Managed Access solution. The operation of the commercial wireless networks in the area of a prison are not adversely effected simply from "leakage" of the MAS system's RF energy outside the walls of the corrections facility. On the contrary, the Tecore Managed Access solution is designed to operate successfully, and without harmful interference to the desirable commercial operations, when the wireless devices *within* the desire interruption zone are "attracted" to the MAS signal rather than any of the commercial signals in the area, while all devices outside the interruption zone are attracted to a commercial network and ignore the MAS signal. Although the Tecore system's RF design must account for the surrounding commercial network parameters, it is not at all dependent upon "stopping" the MAS systems energy at the prison fence, only preventing its effectiveness to attract and capture wireless devices.

Moreover, since the intrinsic design of the Tecore Managed Access solution permits the completion of all emergency 911 calls, whether coming from contraband or authorized devices,

[53] *Id*. at 18, 19-20.

the risk of failing to complete 911 calls outside the prison walls is non-existent. This is true even in the unlikely event that either one or more commercial networks or the MAS system goes off the air because of equipment failure.

As for public safety communications, since the Tecore Managed Access solution operates solely in the specific radio frequencies licensed to commercial wireless operators, and there is no interference potential to adjacent, harmonic or diverse spectrum, the suggested risk for first responders is equally non-existent.

The CCST Report suggests further that the issues of harmful interference and emergency calling failure pose a significant risk of liability for prison officials and state governments.[54] Contrary to this suggestion, however, the fact is that the operation of the Tecore Managed Access solution as a Private Mobile Radio Service (rather than a Commercial Mobile Radio Service) mitigates the compliance and liability elements of MAS operation. For example, while it has been universally recognized that the ability of the Tecore MAS solution to provide independent and reliable emergency calling for all devices, even if contraband, is of great public interest value and is a necessary element of any proposed solution, it must be remembered that the provision of this feature is for the benefit of the public and not as the result of regulatory compliance requirements.

The CCST Report also wrongly concludes that the future development of applications for wireless devices makes it "likely that the MAS could be bypassed."[55] As with the development of new radio technologies discussed above, the development and commercial availability of new device applications does not occur overnight or in the vacuum. Just as a deployed MAS system

[54] *Id*. at 19.

[55] *Id*. at 20.

can and must evolve to address newly available wireless services, spectrum bands or radio technologies, so too the system can and must evolve to impede newly developed and available applications which might otherwise present inmates with a means of circumventing the MAS solution. The existence of a dynamic wireless marketplace is a reality within which any interruption solution must operate. As a result, MAS solutions are no more or less burdened with technological evolution than alternative methods of addressing the problem of contraband cell phones in prisons.

The foregoing discussion of the many weaknesses in the California report is not meant to suggest that the CCST Report is without merit. In fact, the report very correctly notes that one of the current challenges in deploying MAS solutions to the contraband problem is the fact that operation of the solution requires the legal authority to radiate a signal on the spectrum licensed to the commercial wireless providers in this country, and at present their participation in the solution is wholly voluntary. Tecore agrees with the conclusion drawn by the CCST assessment team that the Commission should "modify existing spectrum owner's [licenses] to require that they provide unobstructed use of their spectrum within the geospatial confines of corrections facilities."[56] In this vein, Tecore reiterates its call for a rulemaking on this very issue, which it outlined in its initial comments in this proceeding.

Respectfully submitted,

TECORE NETWORKS

[56] *Id.* at 19. Tecore does not support the further conclusion drawn by the CCST that the requirement for access to carrier spectrum should include, as well, authority to jam the carrier's spectrum. *Id.* Tecore agrees with the analysis consistently undertaken by the Commission that the FCC lacks legal authority to permit jamming, or to amend the licenses of commercial wireless operators to require them to agree to jamming, under Section 333 of the Communications Act of 1934, as amended. The enforcement of the prohibitions in Section 333 are not subject to forbearance by the Commission, as suggested by a number of commenters.