Before the
FEDERAL COMMUNICATIONS COMM
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of Sections 22.3(b),	)	**RM:_____**
1.931 and Subpart X of the	)	
Commission's Rules	)	
And Creation of New Rule(s)	)	
To Authorize a Plurality of Technical	)	
Solutions to Eradicate the Unauthorized	)	
Use of Wireless Devices in Correctional	)	
Facilities	)	

PETITION FOR RULEMAKING
Of GLOBAL TEL*LINK CORPORATION

Global Tel*Link Corporation
12021 Sunset Hills Road, Ste. 100
Reston, VA 20190
(703) 955-3915

July 20, 2011

SUMMARY

There is universal agreement that contraband wireless devices in correctional facilities are a serious threat to safety and the maintenance of law and order. There is divided acceptance of the means to counter this threat.

This Petition requests that the Federal Communications Commission issue a Notice of Proposed Rulemaking to openly consider amending its rules and creating new rules that will hasten the development of new and innovative contraband wireless device solutions, and facilitate access to and deployment of currently available technologies.

Managed access systems are generally favorably viewed, yet they are too costly for most deployments and complicated to authorize, given the need to negotiate spectrum sublease agreements with multiple wireless telecommunications carriers. This Petition presents a proposal to amend the Commission's rules to streamline the spectrum lease process so that spectrum lease agreements, when needed, are obtained in a shorter period of time. Additionally, the Petition requests that the Commission revise its rules governing the grant of special temporary authority to specifically consider the importance of timing with respect to contraband wireless device deployments. Petitioner's are aware of the concerns associated with the operation of these systems and the potential impact of operation on commercial wireless networks, and therefore also proposes that the Commission adopt explicit technical operating standards designed to mitigate over-coverage of contraband wireless device system signals. The Petition also discusses obligatory protection of E-911 operations.

Jamming remains a potential solution for many correctional facilities, because it is effective and less expensive than managed access. This Petition argues that the Commission has the authority to exercise discretion and craft rules that would permit the use of jamming technology by correctional facilities under very stringent parameters. Contrary to arguments that have been repeated for years, Section 333 of the Communications Act of 1934 does not prohibit the jamming of illegal wireless device signals in defined settings, nor does it prevent the FCC from authorizing a narrow use of jamming systems. Specifically, Section 22.3(b) can be amended to make this authority clear, and rules can be created that will guard against the possibility of "overjamming."

It is important that any technology deployed to combat contraband wireless devices be operated by a reliable and responsible entity, preferably with experience in telecommunications. To this end, Petitioners recommend that entities seeking to deploy a solution at a correctional facility demonstrate the receipt of regulatory authorizations and certifications at the federal and state levels, to ensure that the entity has familiarity with telecommunications networks and is also accountable for its operations to a regulatory body. Additionally, contraband wireless device operators should demonstrate the approval of the correctional facility administrator where it seeks to deploy a solution, by providing a letter of authorization from the facility administrator and evidence of a contractual agreement with the facility to conduct the deployment.

The recent flurry of state legislation criminalizing the distribution and possession of wireless devices in correctional facilities, and plans in Congress to introduce legislation that would focus on making managed access solutions affordable support the request for Commission action presented here.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of Sections 22.3(b),	)	**RM:_____**
1.931 and Subpart X of the	)	
Commission's Rules	)	
And Creation of New Rule(s)	)	
To Authorize a Plurality of Technical	)	
Solutions to Eradicate the Unauthorized	)	
Use of Wireless Devices in Correctional	)	
Facilities	)	

PETITION FOR RULEMAKING

I. INTRODUCTION

Global Tel*Link Corporation ("GTL"), pursuant to Section 1.401 of the Federal Communications Commission's ("FCC" or "Commission") rules, 47 C.F.R. §1.401, hereby respectfully requests that the Commission issue a Notice of Proposed Rulemaking ("NPRM") to amend certain rules, and create new rules permitting the effective design and deployment of technological solutions to combat the proliferating problem of the unauthorized use of wireless devices[1] by inmates. These rules would be subject to strict and carefully crafted limits that will prevent adverse impact to all radio systems not located on prison property. The serious public safety threat posed by the presence of contraband wireless devices in correctional facilities has been known to the Commission for over four years, and little

[1] "Wireless device," as used in this Petition, means any device, currently available or that could be available in the future, which utilizes licensed frequencies to transmit voice or data communications.

advancement has been made toward adopting rules that would permit the expeditious design and deployment of systems that would enable correctional facilities to substantially reduce or eliminate the use of contraband wireless devices using available technology that is both proven and cost-effective.

On June 14, 2011, the Sullivan County Court in Monticello, New York, ruled that:

> as a matter of law, a cell phone, no matter how a defendant may use it, is inherently **DANGEROUS** because a cell phone or other telecommunications device has a substantial probability that the item itself may be used in a manner that is likely to bring out major threats to a detention facility's institutional safety or security by the defendant, or other inmates, in the facility.[2]

While a growing line of cases serves to increase the penalties for possessing a contraband wireless device in the county or state where the ruling issues, this piecemeal approach to treating the discovery of a contraband wireless device is not the type of wholesale solution that the corrections industry or the public requires.

The Commission recently demonstrated its willingness to consider the permissibility of technologies that impact spectrum-based services in WT Docket No. 10-4.[3] On April 6, 2011, the Commission issued a Notice of Proposed Rulemaking to consider amending its rules to permit the use of signal boosters, despite concerns expressed by the wireless industry.[4] Petitioners submit that the wireless industry's objections in that proceeding are akin to those raised in the debate regarding the use of contraband wireless device solutions, which makes the consideration of contraband wireless device technology ripe for the Commission's review. It is Petitioner's view that interest in adopting this technology has reached critical mass, as states across the country have attempted unsuccessfully to stem the tide of illegal cell

---

[2] *People v. Green*, 2011 Slip Op 21200, June 14, 2011, Sullivan County Court, (3d D) (emphasis in the original). This case joins previous state cases finding that cell phones are not just contraband when in the possession of an inmate, but DANGEROUS contraband. See also, *Malone v. Caruso*, 2011 WL 806617 (W.D. Mich., 2011); *McMullen v. Director, TDCJ-CID*, 2011 WL 1113500 (E.D. Tex., 2011); *Kalasho v. Martin*, 2005 WL 1355065 (e.D. Mich., 2005).

[3] See *In re* Amendment of Parts 1, 2, 22, 24, 27, 90 and 95 of the Commission's Rules to Improve Wireless Coverage Through the Use of Signal Boosters, *Notice of Proposed Rulemaking*, WT Docket No. 10-4, (rel. April 6, 2011)("*Signal Booster NPRM*").

[4] *In re* Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters, *Petition for Declaratory Ruling of CTIA-The Wireless Association*, (RM proceeding pending), Nov. 2, 2007 ("*CTIA Petition*").

phones with tougher statutory penalties, while at the same time cutting edge technology has emerged that provides the best approach to eliminating contraband wireless device use. Most importantly, these technologies can dramatically reduce or eliminate contraband wireless device use while preserving the integrity and availability of cell phone service outside of the grounds and within facilities alike. Petitioners request that the Commission examine the technologies discussed herein and make the determination that preventing criminal activity and protecting public safety are neither inconsistent with, nor threatening to, the Commission's longstanding policies regarding the use of the radio spectrum.

II. PETITIONER BACKGROUND

GTL provides secure, customized, highly-specialized telecommunications services to correctional facilities throughout the United States. GTL serves all types of correctional facilities, from nearly 800 county jails to twenty-eight state Departments of Correction. GTL has been serving the secure telecommunications needs of the corrections industry for over twenty years, during which time its service has evolved from traditional public payphones to sophisticated software-based security systems that not only connect inmates with friends and family by telephone but, just as importantly, assist law enforcement and corrections entities in their attempts to prevent or prosecute illegal activities that may originate within their inmate populations. In many instances, state and county governments look to revenue generated by inmate phone calls to help fund inmate services, counseling and to provide for other facility needs. In this instance, correctional facilities are looking to inmate phone service providers to assist with the deployment of a contraband wireless device solution in addition to traditional telephone services.

Over the last four years, contraband wireless device use has skyrocketed and prisons and law enforcement have been stymied in their efforts to quell the GTL has witnessed the frustration experienced by its customers with the increasing prevalence of illegal wireless devices within their facilities. With smuggled cell phones garnering anywhere from $200-$2,500 each, there is a substantial incentive to smuggle

phones or phone components to inmates. GTL has explored examples of each of the most well-known solutions—detection, jamming and managed access—and has considered the appraisals of each of these solutions as expressed by its correctional facility customers. GTL has deployed the first fully-functioning managed access solution sanctioned by the FCC and the wireless industry, and now has a clearer view of how the provision of managed access systems could be improved.

III. DISCUSSION

A. The Issue of FCC Authorization of Contraband Wireless Device Solutions Is Overripe

The threat posed by contraband wireless devices in correctional facilities has been increasing as rapidly as wireless devices decrease in size. It is time to pen rules. The issue has been raised in Congress, and has produced legislation and law.[5] The issue has been studied by the National Telecommunications and Information Administration ("NTIA") through testing and issuance of a notice of inquiry.[6] The issue has been presented to the Commission in many forms over the course of the last four years; through petitions for forbearance,[7] rulemaking[8] and declaratory ruling,[9] requests for special temporary authority ("STA"),[10]

---

[5] *See generally,* S. 1749, Cell Phone Contraband Act of 2010, Pub. Law 111-225; S. 251, Safe Prisons Communications Act of 2009, 111th Cong., (2009-2010); H.R. 560, Safe Prisons Communications Act of 2009, 111th Cong., (2009-2010). Additionally, several states have either introduced bills or enacted laws that increase penalties for inmate possession of wireless devices, *see* footnote 33. On May 19, 2011, the New Jersey State Assembly issued a Resolution requesting that Congress and the President re-introduce and enact the Safe Prisons Act of 2009, to authorize the FCC to permit the supervisory authority of a correctional facility to operate a jamming system within the facility to prevent, block or otherwise interfere with unauthorized wireless communications by incarcerated individuals. State of New Jersey, Assembly Resolution No. 129, 214th Leg., amended May 19, 2011.

[6] *See generally, In re* Preventing Contraband Cell Phone Use in Prisons, *Notice of Inquiry ("NOI")*, Docket No. 100504212-0212-01, (rel. May 12, 2010).

[7] *See generally, 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 Sections 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.

[8] *See generally, 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, June 12, 2007; *In re* Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users, *Petition for Rulemaking of South Carolina Department of Corrections*, (RM proceeding pending), Aug. 6, 2009; *In re* Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users, *Petition for Rulemaking of the Mississippi Department of Corrections*, WTB Docket No. 09-53, Aug. 21, 2009.

[9] See, *CTIA Petition.*

[10] *See* Letter from Howard Melamed, CEO, CellAntenna Corporation, to Marlene H. Dortch, Secretary, Federal Communications Commission, *Request for Special Temporary Authority* (March 3, 2009)(seeking permission to

and a workshop.[11]

The footnotes delineating the filings and events that have sought the attention of the FCC on the matter of contraband wireless devices is far from exhaustive, yet remarkable in quantity, given its incompleteness and the fact that these filing have essentially produced nothing to advance the efforts of correctional administrators, equipment manufacturers, or the wireless industry toward developing the "tool box" of solutions that is generally believed to be required to sufficiently address the problem on a nationwide scale. Attempts to seek the Commission's blessing to conduct tests and demonstrations of jamming technology through the dutiful filing of STA requests have been denied, or worse, granted and then retracted.[12]

This Commission has yet to act on any of the petitions for rulemaking on these issues submitted since 2007. The lack of action is disappointing at the very least. It may be that the prior petitions sought Commission action on jamming technologies, and at a time distant enough in the past that the operational accuracy and safety of jamming solutions was questionable enough to cause widespread concern over deployment. It is now several years later, and technology has been evolving, specifically in response to the fears and criticisms raised in the interim. Moreover, managed access solutions, which enjoy the

---

demonstrate jamming equipment at Pine Prairie Correctional Center, Pine Prairie, LA); *see also*, Letter from Devon Brown, Director, District of Columbia Department of Corrections, to Kevin Martin, Chairman, Federal Communications Commission, *Request for Special Temporary Authority* (Dec. 16, 2008)(seeking permission to demonstrate jamming equipment at the D.C. Jail).

[11] Public Safety and Homeland Security Bureau Workshop on Combating Contraband Cell Phones in Prisons, September 30, 2010.

[12] *See,* Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Howard Melamed, CEO, CellAntenna Corp., DA-09-622, March 17, 2009, fn. 4 (denying STA request to conduct a limited demonstration of jamming technology at Pine Prairie Correctional Center partially in deference to comments like "the demonstration would be illegal" and that approving the STA request would lead to the widespread use of poorly made jamming devices.); see *also*, Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Devon Brown, Director, District of Columbia Department of Corrections, DA-09-3, Jan. 2, 2009 (granting a STA request to conduct a jamming demonstration, stating "We agree that the proposed demonstration of equipment designed to prevent prisoners' unauthorized wireless telecommunications will benefit public safety."); *but, see also* Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Devon Brown, Director, District of Columbia Department of Corrections, DA 09-354, Feb. 18, 2009 (retracting the previously granted STA approval, finding "that the proposed jamming would violate both the Communications Act of 1934, as amended, ("Communications Act") as well as the Commission's rules.)

support of regulators and industry alike, has now been deployed and studied in operational settings. GTL has hands-on experience, and can assist the Commission in amending and creating rules to ensure that managed access becomes a permanent, efficacious tool in the tool box.

It is significant that on April 6, 2011, the Commission released a Notice of Proposed Rulemaking in WT Docket No. 10-4.[13] This rulemaking concerned signal boosters. Signal boosters shared the stage with cell phone signal jammers as a target of opposition by CTIA.[14] The stated ills associated with the use of signal boosters are notably similar to those voiced with respect to jamming technology.[15] While the Commission has declined to open a rulemaking to address the means to making jamming available as a contraband wireless device solution, it has determined that, while "[m]alfunctioning, poorly designed, or improperly installed signal boosters...may harm consumers by blocking calls, including E-911 and other emergency calls...,"[16] nevertheless, "[w]ell-designed, properly operating, and properly installed signal boosters have the potential to improve consumers' wireless network coverage without harming commercial, private, and public safety wireless network performance."[17] The Commission goes on to state that "[t]he public interest is best served by ensuring that consumers have access to well-designed boosters that do not harm wireless networks."[18] It should not be a stretch to see the same statement can be made about the interests of correctional facility directors and law enforcement personnel.

GTL files this petition with optimism that it will be *the* petition that engenders a rulemaking, and ultimately rules, that will better enable the technological development and rapid deployment of life-saving technology. NTIA notes in its report released pursuant to the *NOI* that "FCC staff is also working to develop a streamlined regulatory process for similar future applications involving managed access

---

[13] *Signal Booster NPRM.*
[14] *CTIA Petition.*
[15] *See, CTIA Petition* at 10-14.
[16] *Signal Booster NPRM* at para. 2.
[17] *Id.*
[18] *Id. at para. 3.*

technology."[19] GTL would like to assist in that development, and submits that the wireless industry needs to join the discussion, as well. Over the course of the last four years, the frightening, frustrating and costly problem of contraband wireless devices in prisons has been illuminated and discussed by all of its stakeholders. It appears that the "talk therapy" has hit a point of diminishing return for everyone except wireless carrier and prepaid phone providers, who continue to earn profits on the sale and illegal use of wireless technology by inmates. Save for the enactment of the Cell Phone Contraband Act of 2010, which does little to nothing to get solutions in place that will prevent tomorrow's witness harassment, drug deal, facility riot or murder, nothing exists to spur the attack on the problem. The issuance of a Notice of Proposed Rulemaking creates an opportunity to encourage progress.

B. The Commission Must Amend Rules and Create New Rules that Address More than One Technological Solution to Unauthorized Wireless Device Use by Inmates

"Any solution to the contraband cell phone problem in prisons needs to address the growing number of telecommunications methods. This includes, for example, the Cellular, PCS, AWS, SMR, WiMAX, 700 MHz and General Mobile Radio bands. Additional methods of telecommunication include satellite, Wi-Fi, and Bluetooth mobile devices."[20] Petitioners seek not only the amendments necessary to permit the testing of jamming, but also seek the amendment and addition of rules to facilitate the improvement and effective deployment of managed access solutions, and the ability to adapt to future advancements in wireless technologies.

It is axiomatic that "[t]here is no single solution that will solve this problem in the wide variety of state and local correction facilities in our county."[21] Cost of deployment, available sources of funding, physical characteristics of specific correctional facilities and their geographic locations, and the extent and magnitude of the contraband wireless device problem at any given facility are all factors that

---

[19] *NOI*, Docket. No. 100504212-0212-01, at 9.
[20] *NOI* at 20.
[21] *In re* Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users, *Petition for Rulemaking of South Carolina Department of Corrections*, (RM proceeding pending), Aug. 6, 2009, at 2.

contribute to the need for a toolbox of solutions. In order to provide the most complete selection of tools, the Commission must consider existing rules that currently bar the deployment of certain solutions, and contemplate the addition of new rules that encourage the testing and future deployment of other solutions.

C. Managed Access

1. The Solution with Support

While there are ongoing disagreements about whether or not the Commission can authorize jamming under current laws and rules, many opponents of jamming have endorsed managed access for use in prisons and jails.[22] With the support of CTIA and many wireless carriers, managed access has already been deployed in pilot locations. However, deployment of managed access systems is not without complications.

Managed access systems work by detouring the signal emanating from a wireless device to the managed access system's base station. There, the signal is either recognized as "authorized" to transmit and therefore connected to the CMRS carrier's network, or it is terminated because the signal is not authorized. In order to function, the managed access system must "broadcast" on all of the frequencies being accessed by the wireless devices within the borders of the location being surveilled. Therefore, the system must be tunable to every frequency available for commercial mobile radio use. As such, it must be scalable and adaptive to address the emergence of each new wireless technology. The speed at which managed access systems can evolve and adapt to address changes in wireless networks is critical to their viability and effectiveness of their operations. While no solution can be one-hundred percent effective at all times, diligent and cooperative communication with carriers regarding network changes or managed access system changes is a critical component of managed access success.

Currently, effective deployment of a managed access system requires cooperation and consent from carriers in the form of a spectrum lease agreement. Before a system can be viably deployed at a

[22] *See, NOI* at 20-22.

correctional facility, the system's operator must determine which CMRS carriers are operating in the area, and create a spectrum leasing arrangement with each. Even if the operator can secure a long-term lease agreement with every carrier, the time involved in negotiating the terms and conditions of each lease agreement prior to making the simple FCC Form 608 filing can create problematic delays in finalizing deployment. In the event that some, or even one, carrier refuses to enter a spectrum lease arrangement with a managed access system operator at a particular location, the managed access system can be defeated by inmates who use that service. CMRS frequencies that are not programmed into the system are points of exploitation that can render the solution ineffective.

For the purpose of simplifying the deployment of managed access systems, Petitioners suggest that the Commission promulgate rules that accomplish the following:

1) A requirement that CMRS carriers must agree to managed access leases of their spectrum if it is technically feasible in a specific installation without undue harm to legitimate CMRS uses, or, a formal determination that managed access systems can be "licensed" pursuant to the private commons provisions of Section 1.9080.[23]

2) A requirement that a CMRS carrier provide notice to managed access system operators within the carrier's service area in advance of making technical changes to the CMRS network that would adversely impact a managed access system's operations so that managed access system settings can be coordinated with the planned CMRS modifications.

3) Explicit quantifiable and reasonable limits on the "over-coverage" of managed access systems.

4) Explicit protection of E-911 performance in the managed access areas absent a specific exemption from the local PSAP.[24]

[23] 47 C.F.R. § 1.9080.

[24] In at least one pilot of managed access technology, the PSAP provider near a South Carolina prison requested that 911 access be blocked within the covered prison, since inmates were tying up 911 lines and operators.

2. Specific Rule Changes--Managed Access

a. Making spectrum accessible

Managed access solutions require access to the spectrum of CMRS carriers. The means by which a managed access system would currently operate on CMRS frequencies is pursuant to a spectrum lease arrangement governed by Subpart X of the Commission's rules. While such means can accomplish the end sought via long-term *de facto* lease agreements with the CMRS carriers serving the geographic location of a correctional facility, the process is replete with shortcomings. The spectrum lease arrangements codified at Sections 1.9001, *et seq.*, were designed to bolster a secondary market in spectrum usage, with commercial interests at heart. As such, the various lease arrangements provided in the rules do not contemplate the need for spectrum access associated with public interest considerations of the contraband wireless device crisis.

Under Section 1.9001, *et seq.*, the spectrum licensee has complete discretion as to whether or not to enter a lease agreement, and can charge the lessee for access. The negotiations leading up to a leasing arrangement can be as protracted as either party wishes to make them. Managed access systems are law enforcements tools needed to safeguard public safety. They are not commercially viable such that their deployment generates revenue, and when they are needed, timely deployment is of the essence. In order to function, access to spectrum MUST be arranged with every CMRS carrier that operates at the location of the correctional facility being served, and ideally, such access should be available for commencement simultaneously. For these reasons, the Commission must either: (1) modify the rules under Section 1.9001, *et seq.*, to require CMRS carriers to timely cooperate in the formation of spectrum leases for managed access systems at no cost; or, (2) declare that managed access systems are suited for a private commons arrangement.

Managed access solutions are effective only when every CMRS carrier serving the geographic location of a particular correctional facility cooperates by providing access to its frequencies. Reluctance or refusal

on the part of even one CMRS carrier diminishes the effectiveness of the system. To this end, it would be optimal to create a subpart of the rules that addresses mandatory cooperation by the wireless industry in much the same way the Communications Assistance for Law Enforcement Act ("CALEA") provisions in Subpart Z guide the telecommunications industry in its mandatory participation in providing call detail to law enforcement and corrections officials.[25] And since managed access systems are imbued with the same public safety and law enforcement objectives as those situations for which CALEA was created, CMRS carriers should be prohibited from imposing a fee for leasing their spectrum.

The Commission must also accommodate a managed access system operator's need for temporary authorization to operate when spectrum lease negotiations with one or more CMRS carriers are delaying a critical deployment. The circumstances associated with these deployments are not exact fits to those addressed by the current special temporary authority ("STA") provisions in Section 1.931 of the Commission's rules.[26] Rather than the "extraordinary" reasons for which STA's are typically sought and granted,[27] STA's might be required for most managed access deployments, especially at locations where there are multiple CMRS carriers with whom the managed access operator must negotiate spectrum lease arrangements. It is important to the efficacy of a managed access system that its deployment be conducted without notice to the prison population it covers. Therefore, public notice requirements in the acquisition of spectrum leases could jeopardize public safety. The Commission can streamline the STA process in these situations by adding a new subsection 1.931(2)(v), indicating that a STA will be routinely approved for the purpose of completing spectrum lease negotiations for a managed access system.

The repeated exercise of negotiating spectrum leases for the same frequencies with the same carriers at different locations around the country (and the commensurate need to request STAs each time) could be avoided if the Commission determined that this spectrum use lent itself to a "private commons"

---

[25] 47 C.F.R. §1.20000, *et. seq.*; Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U.S.C. §§1001-1010 ("To amend title 18, United States Code, *to make clear a telecommunication carrier's duty to cooperate* in the interception of communications for Law Enforcement purposes, and for other purposes.")[emphasis added]
[26] 47 C.F.R. §1.931.
[27] 47 C.F.R. §1.931(a)(2)(iv).

arrangement.[28] "In a private commons arrangement, the licensee or spectrum lessee authorizes users of certain communications devices employing particular technical parameters, as specified by the licensee or spectrum lessee, to operate under the license authorization. A private commons arrangement differs from a spectrum leasing arrangement in that, unlike spectrum leasing arrangements, a private commons arrangement does not involve individually negotiated spectrum access rights with entities that seek to provide network-based services to ends users."[29] It would be most beneficial if the Commission determined that managed access systems require unfettered access to CMRS frequencies on a nationwide basis, albeit under prescribed technical and operational parameters. Petitioners request that the Commission adopt rules that outline the process for entering a private commons arrangement for this limited purpose.

b. CMRS carrier coordination of technical changes

CMRS technology is not static and its rapid evolution provides great benefits to our society and our economy. However, this rapid technological evolution presents a major problem for managed access systems in their role in protecting the public safety.

Of necessity, managed access systems must interact with mobile units located in or near prison property and the CMRS carriers' networks. In some countries, including the whole European Union, the technical nature of CMRS technology is strictly regulated and carriers can only offer standard technologies such as GSM or UMTS. A major strength of FCC spectrum policy over the past two decades has been the absence of such microscopic technical regulation and the freedom for CMRS carriers and their suppliers to innovate rapidly and get new services to the public. Inherent in this freedom is the potential to render managed access systems ineffective, thereby endangering the public, unless some attention is paid to details. The Petitioners do not seek a European Union-like technology monoculture, but rather,

[28] 47 C.F.R. §1.9080.
[29] 47 C.F.R. § 1.9080(a).

reasonable assurances that CMRS networks and managed access systems can practically evolve together to follow changes initiated by carriers to better serve the public.

Ideally, modifications in the carrier's network and the managed access system would be carried out synchronously. Even a simple reconfiguration of cellular sites, without any other networking changes, occurring near a prison with a managed access system, could impact the proper operation of that system. This could entail moving a nearby base station either closer to the prison or further away or changing a power level or antenna pattern. It is essential that such changes be shared with the managed access operator with adequate time to assure that the managed access system is modified in synchronism, if necessary, for a specific change.

Petitioners request that the Commission adopt rules for managed access systems that require that each CMRS operator providing service at prison locations notify the managed access operator or prison administrator in advance of any network changes that are likely to impact the managed access system and that the rules require that CMRS operators negotiate in good faith on the implementation timing of the change.

c. *Limits on over-coverage of managed access systems*

Just as with jamming systems, managed access systems have a finite, but real, risk of over-coverage of the prison area with a resulting potential to impact the general public beyond the secure areas of prison property. This risk is minimal in most prisons, because of large buffer zones; however, in urban jails and prisons with smaller buffer zones, there is a risk of over-coverage. Absent any regulatory standards for how much over-coverage is acceptable, there is a real risk of litigation from members of the general public whose service is impacted, even if the impact is minimal. Therefore, Petitioners request that the Commission adopt explicit standards on how much over-coverage is acceptable and make it clear that such incidental over-coverage is consistent with the CMRS service offered by carriers.

d. Protection of E-911 operations

Petitioners urge the Commission to include in any new rules covering contraband wireless device solutions an explicit statement that E-911 systems may not be compromised by solution operations except in the limited circumstance of authorized jamming systems. Any jamming system should be required to be approved by the PSAP operator whose area covers the prison location. Petitioners believe that the PSAP operator, as a local public safety official, is in the best position to determine whether an E-911 impact serves the public interest in protecting public safety in that specific area, and can assure that all affected public safety organizations are aware of the system that has been authorized.[30]

D. Jamming

1. Not Prohibited by Section 333

Conventional wisdom holds that Section 333 of the Communications Act of 1934, as amended, (the "Act")[31] limits FCC jurisdiction to authorize jamming. Petitioners offer three viable interpretations of the Act that permit the Commission to authorize jamming: (1) Section 333 was not intended to limit the Commission's authorization for jamming; (2) whatever Section 333 means, it applies equally to the FCC and NTIA,[32] and since NTIA has consistently found it can authorize jamming, FCC has the same authority; and, (3) a change to Section 22.3(b)[33] of the Commission's Rules would make the illicit use of wireless devices within correctional facilities generally unauthorized, and therefore jamming would not be prohibited by any reading of Section 333.

---

[30] By law and policy, inmates and staff on prison property do not need mobile access to 911 operators. For decades, prison administrators have developed systems and procedures for dealing with emergencies and for protecting the public, prison staff, and visitors, and inmates. These policies, practices and procedures have been upheld against repeated challenges in state and federal courts.

[31] Pub. L. 101-396, §9, September 28, 1990, 104 Sta. 850; 47 U.S.C. § 333.

[32] *See* Senate Report (Commerce, Science, and Transportation Committee) No. 101-215, 101st Cong., Nov. 19, 1989 (*"The provision in the reported bill also applies to Federal Government radio communications.* Interference to these communications is now covered by 18 U.S.C. §1362. The inclusion of this new provision will provide the FCC with a stronger basis for investigating and seeking prosecution of interference complaints by Federal agencies.")("S.R. 101-215")[emphasis added]

[33] 47. C.F.R. § 22.3(b).

a. Legislative Intent of Section 333

While there are several Commission staff letters written under delegated authority that are consistent with it, Petitioners are not aware of any explicit statement by the Commission staff that the Commission lacks the jurisdiction to authorize jamming or any instance where the Commission, *en banc,* has ever adopted this interpretation of the statute.[34] CTIA has offered that "The Commission cannot ignore Section 333 of the Act or its extensive history of declaring wireless jamming technology illegal,"[35] yet this interpretation ignores the legislative history of Section 333 and the overriding intent of the Act. The legislative history reveals that Congress, in considering this amendment to the Act, did not intend to limit the jurisdiction of the Commission by forbidding it from ever authorizing any jamming. Indeed, it was the Commission that requested this legislation in response to a series of intentional jamming incidents in which the jammer was using a licensed transmitter and thus could not be prosecuted for criminal violation of Section 301.[36] The Senate report summarized the impact of the new legislation by stating, "The reported bill remedies this situation by *giving the FCC the explicit authority* to halt willful or malicious interference..."[37] The provision was meant to confer upon the FCC the discretion to exercise authority, not prohibit the FCC from exercising discretion.

With respect to the Commission's "extensive history of declaring wireless jamming technology illegal," there is an absence of clear evidence that the Commission has *ever* spoken on any interpretation of Section 333. Furthermore, staff interpretations have generally focused on a point of agreement: that under *present* FCC Rules, the sale and use of jammers is not authorized and hence is illegal. None of the

---

[34] We note that many Commission staff actions rejecting prison jamming requests have avoided judging the meaning of Section 333 and focused on the noncontroversial fact that at present no Commission rules authorize jamming and hence the sale of jamming equipment and jamming by the Commission licensees are not legal. *See* Letter from James D. Schlichting, Acting Chief, Wireless Telecommunications Bureau to Devon Brown, Director, District of Columbia Department of Corrections, DA 09-354 (dated Feb. 18, 2009) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-354A1.pdf).

[35] *CTIA Petition* at p.4.

[36] House Report (Energy and Commerce Committee) No. 101-316, October 27, 1989 ("H.R. 101-316").

[37] S.R. 101-215, H.R. 101-316.[emphasis added]

staff documents cited by CTIA explicitly agree with CTIA's contention that Section 333 is a "statutory prohibition...on interference."

CTIA presented this interpretation of Section 333 in its 2007 Petition for Declaratory Ruling.[38] CTIA cited no direct precedent of staff action, no Commission decision and no case law to support this interpretation. Indeed, the *CTIA Petition* relies primarily on a 2005 Public Notice[39] that based its conclusion on the plain language of "47 USC § 302a(b) and Section 2.803(a) of the FCC's rules" – not on a general statement that §333 prohibits Commission authorization of jamming.

A 2011 Public Notice on jamming, issued under delegated authority, stated as follows:

> "As to operation, section 333 of the Communications Act prohibits "willful or malicious" interference to authorized radio communications, and thus prohibits the operation of jammers." [40]

But even this Public Notice fails to adequately support CTIA's requested declaratory language. Even if the language of Section 333 is broader than its original intent, the question of whether illicit CMRS devices within a correctional institution, where their mere possession violates state criminal statutes, have valid FCC authorization (and therefore interference protection under this section) gives the Commission the option of modifying its rules to permit limited jamming.[41] Section 333 is limited in its application to willful or malicious interference with **authorized** radio communications. Obviously, the federal government has not, and could not, "authorize" the use of wireless devices by inmates in federal, state or county correctional facilities where the possession or use of such devices is illegal, as a matter of

---

[38] The Wireless Association, *Petition for a Declaratory Ruling of CTIA* (Nov. 2, 2007) (http://files.ctia.org/pdf/filings/FINAL--CTIA--_Jammers_Petition_for_Declaratory_Ruling.pdf). The Commission has never acted on the "jammer" portion of this petition, which sought a declaratory ruling " that the sale and use of jammers – with the exception of sales to and use by the federal government – is unlawful." The section of the petition dealing with "wireless boosters and repeaters" is now pending in the *Signal Booster NPRM.*

[39] Public Notice, "Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States", DA-05-1776, June 27, 2005 (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-1776A1.pdf).

[40] FCC Enforcement Advisory, "CELL JAMMERS, GPS JAMMERS, and OTHER JAMMING DEVICES", DA 11-249, February 9, 2011 (http://www.fcc.gov/Daily_Releases/Daily_Business/2011/db0209/DA-11-249A1.pdf)

[41] The following states have either laws, or bills introduced, that declare wireless devices to be contraband in the hands of inmates: Alabama, Arizona, California, Georgia, Iowa, Maryland, Mississippi, New York and Texas.

state law or federal policy. Accordingly, the Commission has inherent authority to permit limited jamming in such correctional facility settings. Section 22.3(b) of the Commission's Rules exempts CMRS customers from the Section 301 licensing requirement. Petitioners propose § 22.3(b) be modified so it is clear that where state and local law make CMRS subscriber equipment illegal in corrections facilities, such use is also illegal under federal law.

b. Section 333 applies equally to the FCC and NTIA

NTIA already maintains that it has the jurisdiction to authorize jamming by federal government entities,[42] but that the FCC is forbidden by Section 333 to authorize any jamming.[43] Petitioners believe that this is an erroneous reading of Section 333 and that Section 333 applies to both agencies equally. NTIA offers no explanation or support for its position that Section 333 limits the FCC's jurisdiction but does not limit its own.

Section 333, aptly entitled "Provisions Relating to Radio," applies to all radio uses within the United States. It contains no language limiting its application to the FCC's non-Federal Government jurisdiction. Section 301 of the Communications Act makes no reference to the FCC, but rather simply provides for federal authority over all spectrum use and requires a license for such use.[44] The general radio jurisdiction of the Commission is spelled out in Section 303.[45] Section 305 exempts government radio uses from the Commission's authority granted under Sections 301 and 303, but not from the rest of the Act.[46]

---

[42] NTIA, "Emission Measurements of a Cellular and PCS Jammer at a Prison Facility", NTIA Report TR-10-466, May 2010, at p. 2 (http://www.its.bldrdoc.gov/pub/ntia-rpt/10-466/10-466.pdf).

[43] *NOI* at 26734 ("Currently, the operation by non-Federal entities of transmitters designed to jam or block wireless communications violates the Communications Act of 1934, as amended.")
NTIA, "CONTRABAND CELL PHONES IN PRISONS: Possible Wireless Technology Solutions", ("NTIA Jamming Report") December 2010, at p. 16.
(http://www.ntia.doc.gov//reports/2010/ContrabandCellPhoneReport_December2010.pdf)

[44] 47 U.S.C. § 301.

[45] 47 U.S.C. § 303.

[46] 47 U.S.C. § 305.

Section §305(a) states:

> *Radio stations belonging to and operated by the United States shall not be subject to the provisions of sections 301 and 303 of this title.* All such Government stations shall use such frequencies as shall be assigned to each or to each class by the President. All such stations, except stations on board naval and other Government vessels while at sea or beyond the limits of the continental United States, when transmitting any radio communication or signal other than a communication or signal relating to Government business, shall conform to such rules and regulations designed to prevent interference with other radio stations and the rights of others as the Commission may prescribe. (Emphasis added)

While the statute clearly exempts "[r]adio stations belonging to and operated by the United States" from Sections 301 and 303, and hence the jurisdiction of the Commission, it clearly does not exempt such stations from *all* the provisions of Title III.

Likewise, in 1986, Congress passed a more limited criminalization of jamming dealing only with communications satellites.[47] This Title 18 criminal statute states:

> **§ 1367. Interference with the operation of a satellite**
> (a) Whoever, without the authority of the satellite operator, intentionally or maliciously interferes with the authorized operation of a communications or weather satellite or obstructs or hinders any satellite transmission shall be fined in accordance with this title or imprisoned not more than ten years or both.
> *(b) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States.* [48]
> (Emphasis added)

While 18 U.S.C. 1367(a) criminalizes satellite jamming similarly to the subsequent provisions of Section 333, it clearly provides that certain types of federal agencies are exempt. Yet, four years later, the language of Section 333 has no such exemption. Accordingly, whatever Section 333 means, it applies equally to both NTIA and the FCC. If the agencies believe that the FCC lacks that jurisdiction to authorize jamming to preserve the public safety, than NTIA also lacks that jurisdiction. The logical consequence is that federal law enforcement and intelligence agencies are forbidden use of the same

[47] P. L. 99-508, October 21, 1986, 100 Stat. 1872
[48] 18 U.S.C. 1367

jamming tools that NTIA finds the FCC may not authorize for legitimate state and local government public safety agencies to protect the public.

2. Specific Rule Changes--Jamming

a. Amending Section 22.3(b)

Just as the Commission has inherent, statutory authority to permit limited jamming of "unauthorized" radio communications, the Commission has long recognized its rulemaking authority in this area. Section 22.3(b) is precisely such a rule. It provides:

> Authority for subscribers to operate mobile or fixed stations in the Public Mobile Services, except for certain stations in the Rural Radiotelephone Service, is included in the authorization held by the licensee providing service to them. Subscribers are not required to apply for, and the FCC does not accept applications from subscribers for, individual mobile or fixed station authorizations in the Public Mobile Services, except that individual authorizations are required to operate rural subscriber stations in the Rural Radiotelephone Service under certain circumstances. [49]

This rule was created independent of any statutory mandate, to avoid the absurdity of requiring CMRS customers to obtain a license to use their wireless devices. The Commission is free to amend the rule, in the public interest and to avoid an equal absurdity; providing federal protection to the illegal use of a wireless device . Section 22.3(b) should be amended to provide that the unauthorized use of a wireless device within the defined area of a correctional facility is not a licensed or authorized use for purposes of application of the Commission's rules. This approach is statutorily sound, logical and consistent with Commission rule-making in this area.

b. Prohibition on jamming cannot apply to unauthorized operations under Section 22.3(b)

Section 333 of the Communications Act and the rules that enforce it should only protect communications that are in the first instance lawful. Wireless devices that have been deemed contraband by state or

[49] 47 C.F.R. 22.3(b)

federal law or correctional facility rule cannot be used in a manner that is considered authorized by either the FCC or the carrier from which the service is received. Amending Section 22.3(b) of the Commission's rules would permit the Commission to authorize the jamming of signals from contraband wireless devices.

The modification can be as simple as limiting the authority conferred by Section 22.3 to those mobile and fixed stations that are operated legally. Petitioners request that the Commission propose an amendment to Section 22.3(b) by adding the following text:

"This authority does not apply to the unauthorized or unlawful operation of CMRS devices on correctional facility property."

i. "Overjamming"

Any system providing control of cellular communications inside a prison may have some overreach. This is true for *both* jamming systems and managed access systems. While strength of radio signals in free space decrease with distance from their source following an inverse square law just like optical light, commercial mobile wireless systems operate in a much more complex propagation environment, with reflections from terrain and structures shading some areas, thereby decreasing radio signal strength, while increasing signal strength in other places due to reinforcements from reflections. Even so, radio propagation is no longer the totally unpredictable, random phenomenon that it was when the Commission was formed in 1934. The high efficiency of cellular spectrum reuse has been enabled by software products that remove most of the uncertainty from radio propagation for cellular networks by using advanced propagation computer models that did not exist when cellular service was first authorized in the 1980s.

> In a June 2010 filing at NTIA[50], CTIA introduced the term "overjamming." CTIA wrote: However, because wireless jamming signals cannot be confined to precise geographic boundaries, and because radio waves propagate in a non-linear way, jamming an entire facility will require 'over-jamming' in which the harmful signal extends beyond the walls of the prison facility and

[50] *NOI,* Comments of CTIA, at p. 20-22

into areas where legitimate users may experience harmful interference to their wireless communications.[51]

CTIA justified this conclusion by pointing out that NTIA tests "showed that jammer power was measurable at distances up to 127 m from the building."[52] Petitioners note that while NTIA claimed the jamming signal was "detectable" away from the building, there was no claim that it could cause harmful interference to CMRS services outside the secure area of the prison, nor did the study consider whether the presence of a secure spatial buffer outside the prison building might mitigate the interference.[53]

ii. Mitigation of "Overjamming"

That most prisons have large buffer zones on prison property between prison perimeters and property boundaries is not accidental. Instead, larger buffers are often required for land use protection, security, design, and code requirements. In high-security prisons where CMRS signal denial is most critical, there is generally a large spatial buffer surrounding the secure area where prisoners reside. If this secure area is not available for public access under the terms of valid state or local laws, than CMRS disruption in that area is a matter of state or local law and is not a valid policy concern for the Commission. The buffer serves to demarcate the areas where public CMRS use must remain unfettered and the secure area where CMRS signal denial is essential for public safety. Accordingly, Commission rules should be drafted in a manner that recognizes that urban jails and prisons with small buffer zones are the small exception to the larger norm.

Petitioners recognize the vital important of protecting public CMRS use in areas accessible to the law abiding public and ask that the rules proposed by the Commission make clear that no contraband wireless device solution be authorized for a particular prison unless the design of that installation has been shown to pose a *de minimis* threat to the legitimate use of CMRS devices in publicly accessible areas.

---

[51] *Id.*

[52] NTIA, Emission Measurements of a Cellular and PCS Jammer at a Prison Facility, NTIA Report TR-10-466, (May 2010) at xi (http://www.its.bldrdoc.gov/pub/ntia-rpt/10-466/)

[53] Anecdotal accounts in CTIA's Comments of prison jamming causing massive interference to areas outside prisons in Brazil and India do not include information about whether *any* attempt was made in the jamming design in either case to limit power or coverage area. *NOI,* CTIA Comments at p. 20.

Furthermore, since jamming would impact E-911 operations within the prescribed service area coordinates, it should not be a permissible option unless the E-911 PSAP for that area has agreed in writing that the steps taken to protect public CMRS use and any possible public safety use within the prison are acceptable.

Since there is always a small risk of either jamming or managed access overreach, Petitioners request that the Commission adopt an explicit standard governing the maximum amount of overreach that is acceptable, in addition to a procedure for resolving any conflicts between prison administrators and the CMRS industry.

As an initial proposal, Petitioners suggest a rule mandating that from the border of the prison property where public access is limited and to a distance of 500m from that border, less than 1% of any 100 meter square area be subject to jamming impact or managed access impact on currently available wireless devices. Furthermore, at a distance of more than 500m to 1000m from the border of prison property where public access is limited, no more than 0.1% of any 100 meter square area should be subject to any impact. Beyond 1000m, no impact would be acceptable. In all cases, compliance would be tested by either a random grid of measurements or an evenly-spaced grid of measurements with measurements witnessed by both the local CMRS licensees and the prison administration at a mutually agreed time. Commission staff should be given authority to refuse test requests as repetitious if previous tests have shown compliance and there is no compelling evidence of any changed circumstance.

These rules protect lawful CMRS operations off of prison property. Jamming or managed access deployment would be allowed only if the system was designed to meet written and measurable standards. Impact on E-911 systems at any location could only occur with the advance written consent of the E-911 call center PSAP for that respective geographic area.

E. Provider Certification

It is critical that any contraband wireless device system be evaluated and approved for use by the Office of Engineering and Technology pursuant to current, and possibly new, equipment authorization standards. Additionally, the entity that is responsible for deploying a system at a correctional facility should be verified and accredited by some set of criteria, for the purpose of ensuring that the system will be installed and operated in the public interest, with accountability to the correctional facility, federal and state regulatory agencies, and wireless subscribers. Permitting entities with no known qualifications for interacting with telecommunications networks or law enforcement agencies to install and operate sensitive telecommunications infrastructures such as those required by contraband wireless device systems is reckless and irresponsible. The most carefully vetted contraband wireless device system is rendered a threat to commercial communications and public safety if it installed and operated by an entity with no demonstrated expertise or regulatory authorization.

The Commission should require that entities seeking to deploy a contraband wireless device system at a correctional facility have a Secretary of State authorization, FCC 214 authority and a state Certificate of Public Convenience and Necessity ("CPCN") or its equivalent in the state where the equipment is installed and operated. Each of these authorizations ensures that the system operator has been evaluated by appropriate regulatory authorities and was found to be both financially and technically qualified to engage in telecommunications-related service provision. These authorizations additionally provide commercial wireless consumers with regulatory bodies to whom they can turn in the event that issues arise with the operation of the contraband wireless device system. At the law enforcement and correctional facility level, prospective contraband wireless device system operators should also be required to demonstrate authorization from the correctional facility requesting the system, by means of a contract with the facility to provide contraband wireless device services, and written authorization from the facility administrator indicating approval of the operator.

IV. CONCLUSION

This Petition is the fourth petition of its kind to be filed with the Commission over the course of the last four years. It is an understatement to say that the problem it seeks to address is beyond critical in terms of importance to the public's interest and safety. While none of the previous petitions may have been ripe for action, there have now been multiple demonstrations, pilots and deployments of managed access as a contraband wireless device solution, which has produced valuable information with respect to its operation. The Commission should avail itself of the lessons being learned and find that it is now time to actively address the need to provide the corrections community and the public with tools to combat the serious problem of contraband wireless devices in prisons.

Respectfully submitted,

Dorothy E. Cukier

Dorothy E. Cukier, Esq.
Executive Director, External and Regulatory Affairs
GLOBAL TEL*LINK CORPORATION
12021 Sunset Hills Road, Suite 100
Reston, VA 20190
Phone: 703.955.3915
Facsimile: 703.435.0980
dorothy.cukier@gtl.net

July 20, 2011