

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities)	GN Docket No. 13-111
)	
CellAntenna Corp. Request for 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)	RM-11430
)	
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)	ET Docket No. 08-73
)	
CTIA—The Wireless Association Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters)	WT Docket No. 10-4
)	
South Carolina Department of Corrections Request for Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users)	PRM09WT
)	
Mississippi Department of Corrections Request for Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users)	PRM09WT
)	
Global Tel*Link Corp. Request for Amendment of Sections 22.3(b), 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)	PRM11WT
)	

CellAntenna Corp. Request for Amendment of) PRM11WT
Section 20.5 of the Commission’s Rules, 47)
C.F.R. § 20.5, to Categorically Exclude Service to)
Wireless Devices Located on Local, State, or)
Federal Correctional Facility Premises)

To: The Commission

**COMMENTS OF THE
ALARM INDUSTRY COMMUNICATIONS COMMITTEE**

The Alarm Industry Communications Committee (“AICC”), on behalf of its members, hereby submits the following comments on the *Notice of Proposed Rulemaking*¹ (“NPRM”), released May 1, 2013, in the above-captioned proceeding. As detailed below, AICC and its members support the Commission’s efforts to facilitate technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide. However, a wide variety of wireless alarm systems may be installed and operating in the vicinity of correctional facilities, and communications from these wireless alarm systems must be protected from capture, blocking and/or harmful interference. AICC therefore vigorously opposes any use of radio signal jamming equipment in prisons and other protected facilities. By nature, jammers cannot differentiate between contraband devices and legitimate devices, including devices used for alarm signaling/monitoring and those used for 9-1-1 calls. Instead, AICC supports the use of managed access systems which are authorized by the FCC and operated pursuant to individual lease agreements with each wireless provider licensed to provide service where the correctional facility is located. When operated and configured correctly, managed access systems using low power base stations should cause less interference to or disrupt service to wireless devices operating legitimately outside of the target facility. AICC recommends certain protocols, discussed below, to help minimize the chance of any interference or call capture.

¹ See In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, *Notice of Proposed Rulemaking*, GN Docket No. 13-111, *et. al.*, FCC 13-58, 28 FCC Rcd 6603, 78 FR 36469 (June 18, 2013) (“NPRM”).

With respect to the Commission's NPRM proposals, AICC supports the FCC's efforts to streamline the spectrum leasing process for managed access systems used in correctional facilities, with minor changes to ensure that the alarm industry (via AICC) and local alarm companies (identified in the Yellow Pages) receive prior written notice before a managed access system is tested or put into service. That way, the performance of nearby wireless alarm systems may be monitored while the managed access system is being optimized, and any "whitelist" programming that may be necessary to safeguard wireless alarm operations in the vicinity of the prison can be completed while the installation contractors are on hand. The managed access lessee should also be required to provide prior written notice of its proposed operations to households and businesses located within a reasonable proximity to the correctional facility, depending on the size and power of the managed access system, as well as annual notifications thereafter to these same households and businesses so long as the managed access system is operational. And because the pool of individuals and businesses with authorized wireless devices that may be impacted by a managed access system is likely to change from time to time, AICC believes the public interest would be further served if the FCC and/or the Bureau of Prisons created and maintained a web site database with the name and location (including street address and lat/long) of all managed access systems that are operational. In this way, up-to-date information about managed access networks and those responsible for their ongoing operation and maintenance will be readily available to wireless alarm installers and other potentially affected members of the public at all times. AICC leaves open the possibility that alternative protocol may accomplish the notice and call capture prevention requirements of the alarm industry and others, upon study of these needs and the specific operating characteristics of managed access systems.

I. Statement of Interest

AICC is comprised of representatives of the Central Station Alarm Association (CSAA), Electronic Security Association (ESA), Security Industry Association (SIA), Bosch Security Systems, Digital Monitoring Products, Digital Security Control, Telular Corp, Stanley Convergent (alarm division, formerly known as Honeywell Monitoring), Honeywell Security, Vector Security, Inc., ADT, AES-

IntelliNet, Alarm.com, Bay Alarm, Intertek Testing, RSI Videofied, Security Network of America, United Central Control, AFA Protective Systems, Vivint (formerly APX Alarm), COPS Monitoring, DGA Security, Security Networks, Universal Atlantic Systems, Axis Communications, Interlogix, LogicMark, Napco Security, Alarm Detection, ASG Security, Protection One, Security Networks, Select Security, Inovonics, Linear Corp., Numerex, Tyco Integrated Security, FM Approvals, and the Underwriters Laboratories.

ESA and CSAA, representing the alarm monitoring and installation industry sector, collectively have 2434 member companies providing alarm service to the public. Together with these trade association members, AICC member companies protect a wide range of sensitive facilities and their occupants from fire, burglaries, sabotage and other emergencies. Protected facilities include government offices, power plants, hospitals, dam and water authorities, pharmaceutical plants, chemical plants, banks, schools and universities. In addition to these commercial and governmental applications, alarm companies protect a large and ever increasing number of residences and their occupants from fire, intruders, and carbon monoxide poisoning. Alarm companies also provide medical alert services in the event of medical emergencies. Because wireless signal jamming and managed access technologies pose a threat of interference to alarms and alarm monitoring operations that rely on wireless signaling, AICC and its members have a significant interest in the outcome of this proceeding. As the Commission is aware, the alarm industry has deployed millions of wireless alarm devices that use data signaling over commercial cellular networks to send alarm signals to the central station, which can then notify the appropriate authorities to respond to the fire, home invasion, excessive carbon monoxide level or medical emergency that has been detected.

II. Notice of Proposed Rulemaking

With the understanding that signals from commercial and private wireless alarm systems must at all times be protected from capture, blocking and/or harmful interference, AICC and its members support the Commission's efforts to streamline its spectrum leasing rules to facilitate the deployment of managed

access systems in correctional facilities. Managed access systems are relatively new, and AICC is encouraged that corrections officials and organizations across the country have been working with the FCC to determine how best to implement available technologies in accordance with the law and without jeopardizing the wireless service to public safety and law enforcement users. Alarm companies also play a vital role in protecting the safety of persons and property, and it is respectfully submitted that the Commission and corrections officials should consider the protection of wireless alarm communications as an important part of this proceeding. Among the most serious public policy concerns related to radio signal jamming and managed access systems is the potential for harm to public safety and private property through the unintentional blocking or capture of signals from wireless alarm systems located near prison facilities where jammers or managed access systems are deployed. Similar concerns exist relating to the unintentional jamming or capture of legitimate calls to 911 from wireless devices used by prison guards or members of the public in close proximity to the prison.

Managed access systems – *i.e.*, low power micro-cellular private networks that have been optimized to capture all voice, text and data communications within a protected correctional facility and that cross-check device identifying information against a “whitelist” of authorized devices – are far more preferable to AICC and its members than radio signal jammers which indiscriminately block all wireless communications on affected spectrum bands and which pose a significant threat to authorized communications outside of a correctional facility, such as 9-1-1 calls and alarm monitoring and signaling operations. Managed access systems are authorized by the FCC in accordance with its policies and rules and the Communications Act of 1934, as amended (the “Act”), and with the full knowledge and supervision (in accordance with the Commission’s Rules) of the underlying CMRS licensees, in their capacity as spectrum lessors. Thus, managed access systems provide multiple layers of oversight, and lease arrangements can facilitate appropriate supervision of managed access lessees. This can help to ensure that signal capture and blocking is limited to areas within the protected facility, and that there is little or no harmful interference to wireless users outside of the protected facility.

Still, because of the fluid nature of RF signals, which propagate differently depending on the weather, the environment and time of day (among other factors), even the most carefully designed and maintained managed access system has the potential of interrupting or interfering with wireless operations outside of the controlled facility. AICC appreciates that the FCC is soliciting comment on procedures for operators of managed access systems to notify the public of their operations and methods to address any impact on nearby consumer (and commercial) wireless services.

a. Streamlining the Lease Authorization Process for Managed Access Systems

Provided that the alarm industry and local alarm companies receive adequate notice in advance of any testing or operation of a managed access system, AICC and its members support the Commission's proposals to streamline its normal *de facto* transfer and spectrum manager leasing procedures to eliminate unnecessary burdens on proposed managed access lessees. It is appropriate for managed access system operators to have individualized lease negotiations with each wireless provider, so each will understand the exact geographic locations where operations on its network may be compromised, and the affected companies can have appropriate contact persons identified and established procedures for resolving interference concerns. Adding an alarm company prior notification/coordination requirement to the managed access lease application would be appropriate because it would make alarm companies aware that a managed access system is being proposed in a particular location and, if they have wireless alarm operations in the vicinity, give them the opportunity to monitor alarm operations while the managed access system is being installed and fine-tuned. That way, if signal capture or blocking is a concern, the alarm company and managed access system operator can work out an appropriate solution, which may involve adding network identification for the alarm system into the managed access system "white list." Managed access operators should be required to create a streamlined procedure for adding alarm device and other legitimate users in the vicinity of the prison to the white list. The prior notice should be sent no less than 30 days before any on-air testing of the managed access system. Identifying alarm companies that should receive this prior notice could be streamlined by using AICC as a clearinghouse for its members, and the Yellow Pages to identify any other companies that may have local wireless alarm

operations and that may not be AICC members. Delivery of the notice should be via certified mail, return receipt requested, or by other readily verifiable means. It would then become the responsibility of any alarm company with wireless operations in the vicinity of the managed access system to evaluate the performance of its customers' systems and confirm there is no signal capture, blocking and/or harmful interference; and/or to make arrangements with the managed access operator to add alarm devices to the white list. Even more desirable, managed access system manufacturers should work with alarm device manufacturers to determine if there is a way to allow managed access systems to recognize alarm signals and avoid capturing them without individual notice/white list modification being necessary. Is there some aspect of alarm data signals that would allow the access system to automatically allow the signals to pass?

To ensure that the integrity of other nearby consumer wireless services (including private alarm monitoring operations) , the managed access lessee should also be required to provide prior written notice of its proposed operations to households and businesses located within a reasonable proximity to the correctional facility, depending on the size and power of the managed access system, as well as annual notifications thereafter to these same households and businesses so long as the managed access system is operational. This notification should include an express warning, in bold face type, that “wireless alarms and alarm monitoring systems operated in proximity to a protected correctional facility may be adversely impacted and coordination with the correctional facility’s managed access system may be necessary.” And because the pool of individuals and businesses with authorized wireless devices that may be impacted by a managed access system is likely to change from time to time, AICC believes the public interest would be further served if the FCC and/or the Bureau of Prisons created and maintained a web site database with the name and location (via street address and lat/long) of all managed access systems that are currently operational. This way, up-to-date information about managed access networks and those responsible for their ongoing operation and maintenance will be readily available to wireless alarm installers and the public at all times. Correctional facilities should also include this information on their web site, as well as instructions for local businesses and homeowners as to who they should contact in the

event of signal capture, blocking or harmful interference to wireless operations outside of the protected facility.

Provided that the managed access lessee complies with reasonable prior notification/coordination procedures designed to protect the integrity of wireless alarm operations, and includes a certification in its STA request and/or managed access lease application confirming its compliance, AICC would not object to the Commission's proposed rule changes designed to facilitate streamlined processing of managed access lease applications. Applications or notifications for managed access leases should not be deemed to have met completeness standards unless and until an appropriate "alarm company notification" certification has been provided, and all relevant fields and certifications on the FCC Form 608 have been completed. Otherwise, managed access lease proposals that are confined to a correctional facility and not intended for the provision of commercial service to the public, are private services that should be presumptively treated as PMRS, and these arrangements do not raise spectrum aggregation, competition or Designated Entity (DE) eligibility concerns.

The Commission's rules and procedures for immediate lease approval or processing were designed to streamline review of those leases that presumptively do not raise public interest concerns.² However, since any capture, blocking or interference with wireless alarm operations would clearly be contrary to the public interest, the Commission should not seek to use immediate lease approval for managed access systems, or grant any managed access lease application, unless and until alarm company and nearby household and business notification obligations have been met. These minor procedural changes proposed by AICC are appropriate under the circumstances, are minimally burdensome, and are consistent with the Commission's intent in providing immediate lease approval procedures.

² See *Second Secondary Market Report and Order*, 19 FCC Rcd at 17512, ¶ 15 (explaining that leases that "do not potentially raise certain specified public interest concerns" should be granted pursuant to the application and immediate grant procedures).

