

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

FILED/ACCEPTED

AUG - 1 2007

Federal Communications Commission
Office of the Secretary

In the Matter of)

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)

Docket No.

PETITION FOR FORBEARANCE

Mitchell F. Brecher
GREENBERG TRAUIG, LLP
800 Connecticut Avenue, NW
Suite 500
Washington, D.C. 20006
(202) 331-3100

Attorney for The GEO Group, Inc.

July 31, 2007

Table of Contents

Summary ...	
Introduction 2
The Relevant Statutes and Rules.....	5
GEO's Forbearance Request Meets Each Prong of the	7
Statutory Standard for Exercise of the Commission's Forbearance Authority..... 7
a. Enforcement of the Federal Government Limitation on the Prohibition against Interference with Cellular Telephones at State and Local Correctional Facilities is not Necessary to Ensure that Charges, Practices, Classifications, or Regulations for, or in connection with, Telecommunications Service are Just and Reasonable and are not Unjustly or Unreasonably Discriminatory8
b. Enforcement of the Federal Government Limitation on the Prohibition against Interference with Cellular Telephones at State and Local Correctional Facilities is not Necessary for the Protection of Consumers.....	10
c. Forbearance from Enforcement of the Federal Government Limitation on the Prohibition Against Interference with Cellular Telephones at State and Local Correctional Facilities would be Consistent with the Public Interest.....	13
Conclusion 17

Summary

Pursuant to Section 10 of the Communications Act, The GEO Group, Inc. petitions the Commission to forbear from application or enforcement of Sections 302, 303, and 333 of the Act, sections 2.803 and 2.807 of the Commission's rules, and such other provisions of the Act and the rules as necessary to allow state and local correctional authorities and those entities (such as GEO) which operate correctional facilities pursuant to contracts with state and local correctional authorities to utilize devices to prevent the use of wireless devices, including cell phones and data transmission devices at correctional facilities and jails. Although the Act generally prohibits interference or "jamming" of radio communications, Section 302(c) allows the Commission to adopt regulations which permit interference by the federal government. By this petition, GEO asks the Commission to forbear from enforcement of the federal government limitation such that state and local governments may similarly interfere with radio communications at correctional facilities and jails.

This petition meets each prong of the statutory three-part test for forbearance. Enforcement is not necessary to ensure just and reasonable charges, practices, classifications or regulations for or in connection with telecommunications services; forbearance is not necessary to protect consumers; and forbearance will serve the public interest.

Despite the fact that inmate possession and use of cell phones and other wireless devices is prohibited at virtually all correctional facilities and jails, all too often such devices make their way into the hands of inmates, despite these prohibitions and despite the best efforts of correctional authorities to prevent them from reaching inmates. Inmate possession and use of cell phones has impeded public safety, undermined law enforcement, enabled inmates to conduct criminal activities while incarcerated and to intimidate members of the public, law enforcement and judicial personnel. Descriptions of how cell phones have been used to engage in such

unlawful and dangerous conduct at correctional facilities and jails are contained in three affidavits prepared by officials at GEO-operated facilities. Those affidavits are attached to this petition. Promotion of law enforcement and public safety objectives has long been a critical aspect of the Commission's public interest responsibilities. Indeed, it has evaluated public safety and law enforcement concerns in considering other forbearance petitions.

Accordingly, the Commission should conclude that each prong of the forbearance standard has been met, and it should promptly grant this petition so that state and local correctional authorities and those who operate correctional facilities and jails pursuant to contract with state and local correctional authorities can more effectively prevent unlawful cell phone use and thereby improve public safety, correctional management and law enforcement efforts with such facilities.

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

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

EXHIBIT B

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)

NOTICE OF PROPOSED RULEMAKING

Adopted: April 29, 2013

Released: May 1, 2013

Comment Date: (30 days after date of publication in the Federal Register)

Reply Comment Date: (45 days after date of publication in the Federal Register)

By the Commission: Commissioner Pai issuing a statement; Commissioner McDowell not participating.

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION	1
II. BACKGROUND	4
A. Contraband Wireless Devices in Correctional Facilities	4
B. The Commission's Role.....	7
C. Other Federal Efforts.....	10
D. Current Technologies	13
1. Managed access	14
2. Detection.....	16
3. Jamming.....	18
E. Petitions.....	21
III. NOTICE OF PROPOSED RULEMAKING.....	24
A. Streamlining Authorization of Leases for Managed Access Systems for Use in Correctional Facilities	24
1. Overview and Regulatory Environment for Managed Access.....	26
2. Proposed Rules to Streamline Managed Access Spectrum Leasing Procedures.....	36
i. Streamlined Lease Application Approval and Lease Notification Processing	38
ii. PMRS Presumption.....	45
iii. Compliance with Sections 308, 309, and 310(d) of the Act	47
iv. Streamlined Special Temporary Authority Request Processing	50
3. Other Proposals	52
B. Detection	53
1. Overview and Regulatory Environment for Detection Systems	53
2. Disabling Contraband Wireless Devices through Improved Coordination.....	56
i. Identifying Contraband Devices	61
ii. Requesting Termination of Service to Contraband Devices	65

iii.	Action by CMRS Licensess	70
C.	Applicability of Prohibitions on Intercepting and Publishing Communications and on the Use of Pen Register and Trap and Trace Devices	74
D.	Other Technological Solutions.....	77
IV.	PROCEDURAL MATTERS	78
A.	<i>Ex Parte</i> Rules	78
B.	Filing Requirements.....	79
C.	Initial Paperwork Reduction Act Analysis.....	80
D.	Initial Regulatory Flexibility Act Analysis.....	81
V.	ORDERING CLAUSES	82
	APPENDIX – A	
	APPENDIX – B	

I. INTRODUCTION

1. In this *Notice of Proposed Rulemaking (Notice)*, we take steps to facilitate the development of multiple technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide.¹ Prisoners' use of contraband wireless devices to engage in criminal activity is a serious threat to the safety of prison employees, other prisoners, and the general public. Through this *Notice*, we seek to remove barriers to the deployment and viability of existing and future technologies used to combat contraband wireless devices.

2. We propose a series of modifications to the Commission's rules to facilitate spectrum lease agreements between wireless providers and providers or operators of managed access systems used to combat contraband wireless devices.² Those proposed modifications are:

- Revising the Commission's rules to immediately process *de facto* lease agreements or spectrum manager lease agreements for spectrum used exclusively in managed access systems in correctional facilities, and streamlining other aspects of the lease application or notification review process for those managed access systems in correctional facilities.
- Forbearing, to the extent necessary, from the individualized application review and public notice requirements of Sections 308, 309, and 310(d) of the Communications Act of 1934, as amended (the Act), for qualifying managed access leases.³
- Establishing a presumption that managed access operators provide a private mobile radio service (PMRS),⁴ streamlining the process for seeking Special Temporary Authority

¹ In this *Notice*, "contraband wireless device" refers to any wireless device, including the physical hardware or part of a device – such as a subscriber identification module (SIM) – that is used within a correctional facility without authorization by the correctional authority. We use the phrase "correctional facility" to refer to any facility operated or overseen by federal, state, or local authorities that houses or holds prisoners for any period of time.

² See *infra* Parts II.D.1 and III.A.1 for a description of managed access systems. For purposes of this *Notice*, "managed access" and "managed access systems" are used generically to refer to a system or systems used to combat contraband wireless devices by capturing transmissions to and from wireless devices within correctional facilities.

³ See 47 U.S.C. §§ 308, 309, 310(d).

(STA) to operate a managed access system, and seeking comment on whether to establish a requirement that managed access providers provide notice to nearby households and businesses prior to activation of a managed access system.

3. We also propose to require wireless providers to terminate service, if technically feasible, to a contraband wireless device if an authorized correctional facility official notifies the wireless provider of the presence of the contraband wireless device within the correctional facility.⁵ We seek comment on the elements of the proposed notification and termination process, including who should be authorized to transmit a termination notification to the wireless provider, the form of such termination notice, and any safeguards necessary to ensure that service to legitimate wireless devices is not inadvertently terminated. We seek comment on the implication of our proposals on detection and managed access system operators' compliance with or liability under Section 705 of the Act and federal law governing the use of pen registers or trap and trace devices.⁶ Finally, while we are limiting our proposals to managed access and detection solutions, we nevertheless invite comment on other technological approaches for addressing the problem of contraband wireless device usage in correctional facilities.

II. BACKGROUND

A. Contraband Wireless Devices in Correctional Facilities

4. Prisoners in federal, state, and local correctional facilities increasingly use wireless devices to engage in criminal activity while incarcerated, which poses a serious security challenge to correctional facility administrators, law enforcement authorities, and the general public.⁷ For example, prisoners can use contraband wireless devices “to arrange the delivery of contraband drugs or other goods, transmit information on prison staff to or from non-inmates, harass witnesses or other individuals, or potentially coordinate an escape.”⁸ The U.S. Government Accountability Office (GAO) reports several instances of contraband wireless devices being used to conduct criminal activity: an inmate in a federal correctional facility was caught running an identity-theft ring using a contraband cell phone; a death row inmate in a Texas facility used a contraband cell phone to threaten a state Senator and his family; an inmate in a Maryland facility used a contraband cell phone to order the murder of a state witness; and a New Jersey state inmate used a contraband cell phone to order the murder of his girlfriend who testified against him at trial.⁹ These are just a few examples that make clear that prisoner possession of wireless

(...continued from previous page)

⁴ A PMRS is “neither a commercial mobile radio service nor the functional equivalent of a service that meets the definition of commercial mobile radio service” and is not subject to common carrier obligations. *See* 47 C.F.R. §§ 20.3, 20.9.

⁵ *See infra* Parts II.D.2 and III.B.1 for a description of detection technologies.

⁶ 47 U.S.C. § 605(a) (prohibiting generally, except as authorized under Chapter 119, Title 18 of the U.S. Code, any person “receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio” from divulging or publishing the “existence, contents, substance, purport, effect, or meaning” to another person); 18 U.S.C. § 3121 (prohibiting the use of pen register and trap and trace devices without a court order, subject to several exceptions including when a provider of a communications service obtains the consent of the user). *See also infra* Part III.C.

⁷ *See* U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Cell Phones Behind Bars at 1 (December 2009) (NIJ Bulletin), *available at* <https://www.ncjrs.gov/pdffiles1/nij/227539.pdf>.

⁸ U.S. GOVERNMENT ACCOUNTABILITY OFFICE, REPORT TO CONGRESSIONAL COMMITTEES, BUREAU OF PRISONS: IMPROVED EVALUATIONS AND INCREASED COORDINATION COULD IMPROVE CELL PHONE DETECTION, GAO-11-893 at 23 (Sept. 2011) (GAO Report), *available at* <http://www.gao.gov/new.items/d11893.pdf>.

⁹ *Id.* at 23-24.

devices is a serious threat to the safety and welfare of correctional facility employees and the general public.

5. Inmate use of contraband wireless devices has grown within the federal and state prison systems parallel to the growth of wireless device use by the general public.¹⁰ In federal institutions and prison camps, GAO reports that the number of cell phones confiscated by the Federal Bureau of Prisons (BOP) grew from 1,774 in 2008 to 3,684 in 2010.¹¹ While not all states track or report data on the use of contraband wireless devices, the data that has been reported demonstrates significant growth. For example, California correctional officers seized approximately 261 cell phones in 2006; by 2011, correctional officers discovered more than 15,000 contraband wireless devices.¹² Further, a test of an interdiction technology in two California State prisons detected more than 25,000 unauthorized communication attempts over an 11 day period in 2011.¹³ A similar interdiction system permanently installed in a Mississippi correctional facility reportedly blocked 325,000 communications attempts in the first month of operation, and as of February 2012, had blocked more than 2 million communications attempts.¹⁴

6. Congress, the Federal Government, and state and local correctional administrators recognize the need to address the proliferation of contraband wireless devices in correctional facilities.¹⁵ A number of states are conducting trials and investing in technologies that will enable them to combat contraband wireless device use in correctional facilities.¹⁶ At least 23 states and the District of Columbia have enacted legislation that officially designates – or allows local authorities to designate – wireless devices in correctional facilities as contraband, and in some cases provides penalties for possession of contraband wireless devices within correctional facilities.¹⁷

¹⁰ See U.S. DEPARTMENT OF COMMERCE, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, CONTRABAND CELL PHONES IN PRISONS: POSSIBLE WIRELESS TECHNOLOGY SOLUTIONS at 3 (Dec. 2010) (NTIA Report), available at http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf. The NTIA Report was issued subsequent to a Notice of Inquiry seeking comment on technologies used to combat contraband cell phone use without negatively affecting other wireless users. See Preventing Contraband Cell Phone Use in Prisons, 75 Fed. Reg. 26733 (May 12, 2010) (NTIA NOI).

¹¹ GAO Report at 20 tbl.3.

¹² California Department of Corrections and Rehabilitation, Fact Sheet: Contraband Cell Phones in CDCR Prisons and Conservation Camps, at 1 (2012) (CDCR Fact Sheet), available at <http://www.cdcr.ca.gov/Contraband-Cell-Phones/docs/Contraband-Cell-Phone-Fact-Sheet-January-2012.pdf>; NTIA Report at 3.

¹³ CDCR Fact Sheet at 2.

¹⁴ Wireless Service Interruptions, GN Docket No. 12-52, Comments of Tecore Networks at 10 (filed Apr. 30, 2012) (Tecore Wireless Service Interruption Comments). See *infra* note 18 for a discussion of the Commission's wireless service interruption proceeding.

¹⁵ See *infra* Parts II.B-C, D.1.

¹⁶ See, e.g., *infra* Part II.D.1 (describing trials of managed access systems in several states).

¹⁷ See Ariz. Rev. Stat. Ann. § 13-2501, 2505 (2010); Ark. Code Ann. § 5-54-119 (2009); Cal. Penal Code § 4575 (2007); Colo. Rev. Stat. Ann. § 18-8-204 (2005); Conn. Gen. Stat. § 53a-174b (2010); 11 Del. C. § 1256 (2008); Fla. Stat. Ann. § 944.47 (West 2008); O.C.G.A. § 42-5-18 (2008); 720 Ill. Comp. Stat 5/31A-1.1 through 1.2 (2011); LA. Rev. Stat. Ann. § 14:402 (2010); Md. Code Ann., Criminal Law § 9-417 (2007); Mich. Comp. Laws Ann. §§ 800.283a, 285 (2006); Miss. Code Ann. §§ 47-5-193, 195 (2008); Nev. Rev. Stat. Ann. § 212.165 (West 2007); N.C. Gen. Stat. Ann. § 14-258.1 (West 2009); N.D. Cent. Code Ann. § 12-44.1-21 (West 2009); 18 Pa. Cons. Stat. Ann. § 5123 (West 2002); Okla. Stat. Ann. Tit. 57 § 21 (West 2009); R.I. Gen. Laws Ann. § 11-25-14.1 (West 2011); Tenn. (continued...)

B. The Commission's Role

7. The Commission has taken several steps to facilitate efforts by state authorities to address contraband wireless device use in correctional facilities.¹⁸ The Commission has granted special temporary authorizations and experimental special temporary authorizations to allow testing of managed access technologies, which utilize wireless base stations located within a correctional facility to capture and block transmissions to or from unauthorized devices.¹⁹ In 2010, the Commission approved spectrum leases between CMRS providers and a managed access provider for the deployment of a managed access system in the Mississippi State Penitentiary in Parchman, Mississippi.²⁰ In 2012, the Commission approved spectrum leases between CMRS providers and several managed access providers for managed access system deployments in the Metropolitan Transition Center in Baltimore City, Maryland;²¹ the Lieber Correctional Institution in Ridgeville, South Carolina;²² the Stiles Unit in Beaumont, Texas;²³ and the

(...continued from previous page)

Code. Ann. § 39-16-201 (2006); Tex. Penal Code Ann. § 38.11 (2011); D.C. Code §§ 22-2603.01-03 (2011); W. Va. Code § 61-5-8 (2009); Wyo. Stat. Ann. § 6-5-213 (2007).

¹⁸ The Commission is currently in the process of examining issues related to the intentional interruption of wireless service by government entities for public safety reasons. See Commission Seeks Comment on Certain Wireless Service Interruptions, GN Docket No. 15-52, *Public Notice*, 27 FCC Rcd 2177 (2012). The Commission sought comment on past practices and precedents, the bases for interrupting service, risks of interrupting service, the scope of and authority to interrupt, and legal constraints on interrupting wireless service. *Id.* at 2179-82. The Commission explicitly excluded “practices expressly prohibited by statute or regulation, such as signal jamming” from the scope of its inquiry. *Id.* at 2178. Four commenters to that proceeding addressed issues implicated in this proceeding, and we incorporate those comments into this proceeding. See Wireless Service Interruptions, GN Docket No. 12-52, Comments of CellAntenna Corp. (filed Apr. 30, 2012) (CellAntenna Wireless Service Interruption Comments); Wireless Service Interruptions, GN Docket No. 12-52, Comments of Global Tel*Link Corp. (filed Apr. 30, 2012) (GTL Wireless Service Interruption Comments); Wireless Service Interruptions, GN Docket No. 12-52, Reply Comments of Global Tel*Link Corp. (filed May 30, 2012) (GTL Wireless Service Interruption Reply Comments); Wireless Service Interruptions, GN Docket No. 12-52, Comments of the Texas Department of Criminal Justice (filed Apr. 16, 2012) (TDCJ Wireless Service Interruption Comments); Wireless Service Interruptions, GN Docket No. 12-52, Reply Comments of Tecore Networks (filed May 30, 2012) (Tecore Wireless Service Interruption Reply Comments); Tecore Wireless Service Interruption Comments.

¹⁹ See, e.g., Tecore Government Services, Special Temporary Authorizations, Call Signs WQMH278, WQMH382, WQMH383, WQMH384, WQMH385, WQMH386, and WQMH387; ShawnTech Communications, Experimental Special Temporary Authorizations, Call Signs WE9XNZ, WE9XRO, WG2XFD (ShawnTech Experimental STAs); Screened Images, Experimental Special Temporary Authorization, Call Sign WF9XUR (Screened Images Experimental STA); Blind Tiger Communications Experimental Temporary Authorization, Call Sign WG9XED (Blind Tiger Experimental STA). See *infra* Parts II.D.1 and III.A.1 for a more thorough description of managed access technologies.

²⁰ Tecore Government Services, Lease IDs L000007637, L000007704, L000007705, L000007706, L000007707, L000007734, and L000009517 (Tecore Parchman Leases).

²¹ Tecore Government Services, Lease IDs L000009924, L000009925, L000009926, L000009927, L000009929, L000009930, L000010050, L000010076, L000010077, L000010078, L000010079, and L000010080 (Tecore Baltimore Leases).

²² ShawnTech Communications, Lease IDs L000009174, L000009484, L000009485, L000009486, L000009487, L000009513, L000009514, L000009515, and L000009516 (ShawnTech Lieber Leases).

²³ ShawnTech Communications, Lease IDs L000009813, L000009878, L000010035, L000010038, L000010274, L000010276, and L000010280 (ShawnTech Stiles Leases).

McConnell Unit in Beeville, Texas.²⁴ We discuss these trials and deployments in further detail below in Part II.D.1.

8. FCC staff has also engaged in extensive outreach regarding the availability of new technologies to combat contraband wireless devices. This outreach includes regular interaction with state corrections officials and organizations from across the country, including the American Correctional Association (ACA) and the Association of State Correctional Administrators (ASCA), equipment and solution vendors, wireless providers, and federal agency partners including the Department of Justice's National Institute of Justice (NIJ), Federal Bureau of Prisons (BOP), and the National Telecommunications and Information Administration (NTIA).

9. On September 30, 2010, the Commission held a public workshop in partnership with NIJ and ASCA to discuss technologies currently available to combat contraband wireless device use and to address the statutory and public policy concerns related to radio signal jamming and managed access.²⁵ The discussion also focused on how to implement available technologies in accordance with the law and without jeopardizing the wireless service to public safety and law enforcement users.²⁶ This *Notice* continues our efforts to examine the Commission's appropriate role in facilitating the use of various technical solutions to combat contraband wireless devices.²⁷

C. Other Federal Efforts

10. Other federal agencies and Congress also recognize the serious problem of contraband wireless device use in correctional facilities, have studied the problem, and have taken steps to deter such use. In December 2010, NTIA, pursuant to Congressional direction and in coordination with the Commission, BOP, and NIJ, issued a report detailing the specific problem of contraband wireless device use in correctional facilities.²⁸ NTIA believes that "contraband cell phone use by prison inmates to carry out criminal enterprises is intolerable and demands an effective solution" and "[p]rison officials should have access to technology to disrupt prison cell phone use in a manner that protects nearby public safety and Federal Government spectrum users from harmful disruption of vital services, and preserves the rights of law-abiding citizens to enjoy the benefits of the public airwaves without interference."²⁹

11. In 2010, Congress enacted legislation that classified wireless devices as "prohibited objects" within federal prisons.³⁰ A federal inmate who possesses a wireless device or anyone who

²⁴ ShawnTech Communications, Lease IDs L000009814, L000009877, L000010036, L000010037, L000010038, L000010275, L000010277, L000010278, and L000010279 (ShawnTech McConnell Leases).

²⁵ An archived video of the workshop, written remarks, presentations, statements, briefing sheet, and a transcript are available through the Commission's Website at <http://www.fcc.gov/events/workshopwebinar-contraband-cell-phone-use-prisons>. See Public Safety and Homeland Security Bureau to Hold Workshop/Webinar on Contraband Cell Phone Use in Prisons, *Public Notice* (Sept. 13, 2010) (Workshop Public Notice).

²⁶ Workshop Public Notice at 1.

²⁷ The Commission has also undertaken an examination of rates for interstate interexchange inmate calling services. See Rates for Interstate Inmate Calling Services, FCC 12-167, WC Docket No. 12-375, *Notice of Proposed Rulemaking*, 27 FCC Rcd 16629 (2012).

²⁸ See NTIA Report at 4.

²⁹ *Id.* at 1.

³⁰ Cell Phone Contraband Act of 2010, Pub. L. No. 111-225, 124 Stat. 2387 (2010) (codified at 18 U.S.C. § 1791). Other objects that federal prisoners are prohibited from possessing include but are not limited to firearms, ammunition, weapons, controlled substances, and U.S. or foreign currency. 18 U.S.C. § 1791(d).

provides a wireless device to an inmate is subject to a possible penalty of up to one year in prison, a fine, or both.³¹ According to the bill's sponsor, Senator Dianne Feinstein, the bill is intended to end criminal activity perpetrated by prisoners using wireless devices in prisons and "punish those who would profit from smuggling cell phones and other wireless devices into [U.S.] federal prisons."³² The legislation also required GAO to conduct a study of cell phone use by inmates and state and federal efforts to prevent prisoners or others from smuggling wireless devices into prisons.³³ The GAO report, released in September 2011, examined the proliferation of contraband wireless devices and federal and state efforts to combat contraband wireless devices,³⁴ and recommended actions for the Attorney General "[t]o help BOP respond more effectively to contraband cell phone challenges."³⁵

12. BOP and NIJ are actively examining solutions to combat contraband wireless devices in correctional facilities. As NTIA reports: "Over the past 15 years, BOP has evaluated a large number of cell phone interdiction technologies."³⁶ NIJ continues to examine solutions to combat contraband wireless devices, convened a plenary panel as part of its annual conference, and co-sponsored with the Commission the contraband wireless device webinar in September 2010.³⁷ Additionally, NIJ's National Law Enforcement and Corrections Technology Center "assists state, local, tribal, and federal correctional agencies, as well as law enforcement and criminal justice agencies, in addressing technology needs and challenges, such as contraband cell phones."³⁸

D. Current Technologies

13. Technological solutions available to correctional facility administrators to combat contraband wireless devices generally fall into three categories: managed access, detection, and radio signal jamming.³⁹ Each of these categories is described below. We seek comment on specific proposals regarding managed access and detection technologies outlined in Part III, and seek comment generally on

³¹ Pub. L. No. 111-225, sec. 2, 124 Stat. at 2387; 18 U.S.C. § 1791(b)(4). Specifically, whoever "in violation of a statute or a rule or order issued under a statute, provides to an inmate of a prison a prohibited object, or attempts to do so; or being an inmate of a prison, makes, possesses, or obtains, or attempts to make or obtain, a prohibited object; shall be punished as provided in [18 U.S.C. § 1791(b)]." 18 U.S.C. § 1791(a). Section 1791(b) of Title 18 establishes punishments for violations of Section 1791 based on the type of prohibited object involved in the violation. 18 U.S.C. § 1791(b).

³² Press Release, Senator Dianne Feinstein, House Approves Feinstein Measure to Prohibit Cell Phones in Prisons (July 21, 2010), available at <http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=f6796124-5056-8059-7669-f0a81a3a664a>.

³³ Pub. L. No. 111-225, sec. 3, 124 Stat. at 2387-88.

³⁴ See GAO Report at 19-32. The GAO report also examined BOP telephone rates and the impact of a rate reduction for inmate calls. *Id.* at 12-18.

³⁵ *Id.* at 33. The recommended actions include evaluation plans for testing and deploying technologies to combat contraband wireless devices, such as managed access, detection, and jamming, as described below. *Id.* at 33-34.

³⁶ NTIA Report at 10. BOP has developed a set of four basic requirements through which it evaluates a given interdiction technology. BOP requires any technology used to combat contraband wireless devices to "work without impacting or collecting information from the general public;" "have no legal restrictions;" "work with all cellular phone protocols;" and have reasonable equipment and installation costs. *Id.*

³⁷ *Id.* at 11.

³⁸ GAO Report at 9.

³⁹ See *id.* at 10; NTIA Report at 1.

other technological solutions that are consistent with the statutory framework that has limited the use of jamming technologies.⁴⁰

1. Managed Access

14. Managed access systems are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks.⁴¹ Managed access systems utilize base stations that are optimized⁴² to capture all voice, text, and data communications within the system coverage area, which would be a correctional facility in the instant case.⁴³ When a wireless device attempts to connect to the network from within the coverage area of the managed access system, the system cross-checks the identifying information of the device against a database that lists wireless devices authorized to operate in the coverage area.⁴⁴ Authorized devices are allowed to communicate normally (*i.e.*, transmit and receive voice, text, and data) with the commercial wireless network,⁴⁵ while transmissions to or from unauthorized devices are terminated.⁴⁶ The managed access system may also provide an alert to the user notifying the user that the device is unauthorized.⁴⁷ The systems provide operational flexibility to the correctional facility administrators by allowing them to disable devices without having to physically remove them.⁴⁸

15. A correctional facility or third party at a correctional facility may operate a managed access system if authorized by the Commission.⁴⁹ This authorization has to date involved agreements with the wireless providers serving the geographic area including the correctional facility and lease applications approved by the Commission.⁵⁰ A number of deployments and trials have been conducted or are ongoing, as listed below.

⁴⁰ See 47 U.S.C. §§ 301, 302a(b)-(c), 333; 47 C.F.R. §§ 2.803(a), 2.807(d).

⁴¹ See NTIA Report at 19.

⁴² See *id.*; CTIA NTIA NOI Comments at 10; Tecore NTIA NOI Comments at 3. The systems are scalable, so it is possible to deploy a system that covers only a portion of a correctional facility. See Tecore NTIA NOI Comments at 4. This might be preferable due to budgetary constraints or operational need.

⁴³ See AT&T NTIA NOI Comments at 10-11. The systems can also reportedly adapt to accommodate changing technologies and protocols, such as LTE. See Tecore NTIA NOI Comments at 5-6, 20.

⁴⁴ NTIA Report at 19; AT&T NTIA NOI Comments at 11; CTIA NTIA NOI Comments at 11. Identifying information can include phone number, serial number, or subscriber identity module (SIM) information. See AT&T NTIA NOI Comments at 11; CTIA NTIA NOI Comments at 11.

⁴⁵ See NTIA Report at 19; CTIA NTIA NOI Comments at 11; MDOC Petition at 6-7; Verizon Wireless NTIA NOI Comments at 9.

⁴⁶ See NTIA Report at 19; CTIA NTIA NOI Comments at 11; MDOC Petition at 6-7.

⁴⁷ See CTIA NTIA NOI Comments at 11; MDOC Petition at 6-7. The system may also route the call to a designated official point of contact. See MDOC Petition at 6-7.

⁴⁸ See AT&T NTIA NOI Comments at 13; T-Mobile NTIA NOI Comments at 8-9; Tecore NTIA NOI Comments at 12.

⁴⁹ See 47 C.F.R. §§ 1.9001-1.9080. The Commission's spectrum leasing rules implicated by managed access systems are discussed in detail *infra* Part III.A.1.

⁵⁰ See ShawnTech Lieber Leases; ShawnTech McConnell Leases; ShawnTech Stiles Leases; Tecore Baltimore Leases; Tecore Parchman Leases.

- *California.* The California Department of Corrections and Rehabilitation (CDCR) has conducted trials of managed access systems at two state prisons.⁵¹ Based on the results of the trials, the California Technology Agency issued an Invitation for Bids for a prime contractor to provide a pay telephone system for inmates and wards and a managed access systems in correctional facilities across the state.⁵² The CDCR awarded the contract in April 2012 to Global Tel*Link (GTL), and its managed access operator has received experimental authorization to test a managed access system in nine facilities.⁵³
- *Maryland.* The Maryland Department of Public Safety and Correctional Services (DPSCS) conducted an in-depth analysis of contraband cell phone interdiction technologies in 2009.⁵⁴ Maryland DPSCS conducted trials of various non-jamming technologies at a decommissioned correctional facility in Jessup, Maryland, and a real-world study of non-jamming technologies in three commissioned correctional facilities.⁵⁵ Maryland DPSCS subsequently issued a Request for Proposals for the installation of managed access and detection systems in all of its prisons, and granted a contract to Tecore Networks (Tecore) to install a managed access system in the Metropolitan Transition Center in Baltimore City, Maryland.⁵⁶

⁵¹ See CDCR Fact Sheet at 2.

⁵² California Technology Agency, Office of Technology Services, Bid #IFB 11-126805 – Inmate Ward Telephone System and Managed Access System Services (rel. July 20, 2011) (IFB), <http://www.dts.ca.gov/stnd/calnet-inmate-ward.asp>. The IFB notes that not all facilities will use a managed access system. *Id.* Section 1 at 2.

⁵³ Press Release, CDCR, CDCR Awards System-wide Telephone Contract That Will Restrict Cellular Phones in Prisons (Apr. 16, 2012), available at http://cdcrtoday.blogspot.com/2012/04/cdcr-awards-system-wide-telephone_16.html; Screened Images Experimental STA. The California Council on Science and Technology (CCST), an independent organization that advises on science and technology policy in California, released a report on the efficacy of managed access in May 2012. CAL. COUNCIL ON SCI. AND TECH., THE EFFICACY OF MANAGED ACCESS SYSTEMS TO INTERCEPT CALLS FROM CONTRABAND CELL PHONES IN CALIFORNIA PRISONS (May 2012) (CCST Report), available at <http://www.ccst.us/publications/2012/2012cell.pdf>. The CCST recommended that alternative interdiction methods be examined before statewide adoption of managed access, including methods to intercept contraband devices rather than relying on technology to block communications, and recommended that CDCR conduct a one-year managed access pilot program prior to awarding a managed access contract. CCST Report at 7, 13-15. CCST also raised several concerns it has regarding managed access, including the lack of operational experience due to the relative infancy of the technology, the possibility of systems capturing authorized devices outside of a correctional facility, difficulties in upgrading systems to add new wireless technologies, and the ability of the systems to capture text and incoming calls in practice. CCST Report at 17-21. Tecore responded to CCST's report in its reply comments in the Commission's wireless service interruption proceeding. See Tecore Wireless Service Interruption Reply Comments at 11-21. Tecore asserts that the CCST report "reflects the assessment team's misunderstanding of the operation of a properly-deployed managed access system." Tecore Wireless Service Interruption Reply Comments at 17.

⁵⁴ See Maryland DPSCS, Cell Phone Detection/Jamming Demonstration, available at http://www.dpscs.state.md.us/media/Cell_phone_detection_flashvideo.shtml.

⁵⁵ See Maryland DPSCS, Overview of Cell Phone Demonstration (2009), http://www.dpscs.state.md.us/publicinfo/media/pdf/FinalReport_2008-09-10.pdf; Maryland DPSCS, Non-Jamming Cell Phone Pilot Summary (2010), available at http://www.dpscs.state.md.us/media/Cell-Phone-Pilot-Summary_Final.pdf.

⁵⁶ See Maryland DPSCS, Request for Proposals: Cell Phone Interdiction Project Solicitation Number: DPSCS Q0011008, available at http://collaboration.asca.net/system/assets/attachments/2020/MD_DOC_Cell_Phone_Detection_RFP_Amended_mb_edits_9_21_2010_2_.pdf?1296010779; Press Release, Maryland DPSCS, Cellular (continued....)

- *Mississippi.* In 2010, the Mississippi Department of Corrections deployed a managed access system at the Mississippi State Penitentiary, a maximum security prison in Parchman, Mississippi.⁵⁷ In its first month of operation, the system blocked a total of 325,000 call and message attempts, and has prevented more than 2 million calls and text messages through February 2012.⁵⁸
- *South Carolina.* South Carolina has conducted trials of a managed access system at its Lieber Correctional Institution in Ridgeville, South Carolina.⁵⁹ The Commission has approved several spectrum leases sought by ShawnTech Communications (ShawnTech) for a permanent installation at the Lieber Correctional Institution, and the system is operational.⁶⁰
- *Texas.* The Texas Department of Criminal Justice announced in late 2012 that it would install managed access systems in two state correctional facilities.⁶¹ The Commission has approved a number of spectrum leases for ShawnTech for the managed access installations.⁶²

2. Detection

16. Detection systems are used to detect contraband devices within a correctional facility by locating, tracking, and identifying radio signals originating from a device.⁶³ Detection systems use passive, receive-only technology and do not transmit radio signals.⁶⁴ As stated in the NTIA Report:

For accurate position location in an environment such as within a prison facility, detection technology triangulates a cell phone signal and requires correctional [facility] staff to physically search a small area (such as a prison cell) and seize the identified cell phone. This may involve placing direction-finding antennas or sensors (connected wire-line or wirelessly) to a computer to

(...continued from previous page)

Detection Through Managed Access Coming to Maryland Prison System (rel. Apr. 23, 2012), *available at* http://www.dpccs.state.md.us/publicinfo/news_stories/press_releases/20120423a.shtml; Tecore Baltimore Leases.

⁵⁷ Press Release, Mississippi Department of Corrections, “Operation Cell Block”: Commissioner Epps Shuts Down Illegal Inmate Cell Phone Usage (Sept. 8, 2010), *available at* http://www.asca.net/system/assets/attachments/1535/MS_Illegal_Cell_Phone_Press_Release.pdf?1291917909.

⁵⁸ Tecore Wireless Service Interruption Comments at 10.

⁵⁹ See Letter from Leigh Blackwell, Assistant Attorney General, South Carolina Office of the Attorney General, to Jon Ozmint, Director, South Carolina Department of Corrections (Dec. 15, 2010), <http://www.scag.gov/wp-content/uploads/2011/03/ozmint-j-os-9173-12-15-10-use-of-cell-phones-by-inmates-in-scdc.pdf>; see also Jessica Mulholland, *Combating Contraband Cell Phones in Prisons*, GOVERNING, Nov. 16, 2010, *available at* <http://www.governing.com/topics/technology/Combating-Contraband-Cell-Phones-in-Prisons.html>. See ShawnTech Experimental STAs.

⁶⁰ See ShawnTech Lieber Leases.

⁶¹ See Mike Ward, Prison Cell Phone Blocking to Start, Postcards: Texas Government and Politics Blog, Statesman.com (posted Sept. 4, 2012), http://www.statesman.com/blogs/content/shared-gen/blogs/austin/politics/entries/2012/09/04/prison_cellphone_blocking_to_s.html/.

⁶² ShawnTech McConnell Leases; ShawnTech Stiles Leases.

⁶³ NTIA Report at 27.

⁶⁴ *Id.*

identify a cell phone call and locate the origin of the call. Additionally, hand-held cell phone detectors are able to scan frequencies within correctional facilities and detect the location of the caller.⁶⁵

17. Detection systems can locate a device with an accuracy of within three to five meters.⁶⁶ Systems are usually capable of detecting across multiple frequencies, and can easily be programmed to add frequencies.⁶⁷ Because detection systems rely on passive receive-only technology, they do not pose an interference threat to wireless operations.⁶⁸

3. Jamming

18. Radio signal jamming is the purposeful disruption of electronic devices, equipment, or systems via radio frequency interference.⁶⁹ A radio signal jamming device transmits on the same radio frequencies as wireless devices and base stations, disrupting the communication link between the device and the network base station, and rendering any wireless device operating on those frequencies unusable.⁷⁰ When used to disrupt wireless devices, radio signal jammers cannot differentiate between contraband devices and legitimate devices, including devices making 911 calls.⁷¹ Radio signal jammers block all wireless communications on affected spectrum bands.⁷²

19. The Act prohibits any person from willfully or maliciously interfering with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government.⁷³ Because radio signal jammers are used to willfully interfere with radio communications of such licensed or authorized stations, jammers are not permitted under the Commission's rules.⁷⁴ Similarly, the manufacture, importation, marketing, sale, or operation of radio signal jamming devices within the United States is prohibited, except for the sale to or use by the Federal Government.⁷⁵

⁶⁵ *Id.*

⁶⁶ *See id.* at 29; ITT NTIA NOI Comments at 18.

⁶⁷ NTIA Report at 27-28.

⁶⁸ *Id.* at 28.

⁶⁹ *See id.* at 13.

⁷⁰ *Id.* Interference is caused by "radiation, re-radiation, or reflection of electromagnetic spectrum." *Id.*

⁷¹ *See id.* at 14-16.

⁷² *See id.* at 14. Radio signal jammers may be unable to block all frequencies that may be used by prisoners, including Wi-Fi signals. *Id.*

⁷³ 47 U.S.C. § 333.

⁷⁴ *See, e.g.*, 47 C.F.R. § 2.915(a)(1) (providing, as a required element for granting an application for equipment certification, that the Commission find that the equipment be "capable of complying with pertinent technical standards of the rule part(s) under which it is to be operated"); *Id.* § 2.919 (requiring denial of certification application if Commission is unable to make the requisite Section 2.915(a) findings). Note that in none of the FCC rule parts has the Commission authorized the operations of jammers or prescribed technical standards for their operation. *See also* 47 U.S.C. § 302a (authorizing Commission to promulgate regulations that govern the interference potential of devices that are capable of emitting a sufficient amount of RF energy to cause harmful interference to radio communications); 47 U.S.C. § 333 (prohibiting willful or malicious interference to any radio communications or any authorized station).

⁷⁵ *See* 47 U.S.C §§ 301, 302a(b)-(c), 333; 47 C.F.R. §§ 2.803(a), 2.807(d).

20. Aside from the statutory constraints, wireless providers have indicated a preference for managed access solutions over jamming solutions,⁷⁶ on the grounds that managed access “can effectively prevent unauthorized communications without disrupting legitimate users.”⁷⁷ Wireless providers point to benefits of managed access over jamming solutions including the coordination and leasing process that occurs between the managed access provider and relevant licensees, and to system design that utilizes low power base stations optimized to prevent interference or the unintentional disruption of service to wireless devices operating legitimately outside of the target facility.⁷⁸

E. Petitions

21. Several entities – including state correctional agencies, equipment manufacturers, and others – filed petitions seeking Commission action on various issues regarding technological solutions to combat contraband wireless devices. Some petitioners urge Commission action with respect to the use of radio signal jammers in state and local correctional facilities.⁷⁹ In 2007, CellAntenna filed a petition for rulemaking to allow signal jamming equipment to be sold to and used by emergency response providers, including state and local law enforcement agencies.⁸⁰ The GEO Group filed a petition seeking forbearance from application or enforcement of Sections 302, 303, 333 of the Act and Sections 2.803 and 2.807 of the Commission’s rules to allow state and local correctional authorities and correctional facility operators to utilize radio frequency jamming devices to prevent the use of wireless devices in correctional facilities.⁸¹

⁷⁶ See AT&T NTIA NOI Comments at 1-2; CTIA NTIA NOI Comments at 9-13; Sprint Nextel NTIA NOI Comments at 1; T-Mobile NTIA NOI Comments at 7-9; Verizon Wireless NTIA NOI Comments at 9-10.

⁷⁷ T-Mobile NTIA NOI Comments at 8. See also AT&T NTIA NOI Comments at 11-12; CTIA NTIA NOI Comments at 12; Sprint Nextel NTIA NOI Comments at 1; Verizon Wireless NTIA NOI Comments at 9-10.

⁷⁸ See AT&T NTIA NOI Comments at 11-12; Sprint Nextel NTIA NOI Comments at 1-2; Verizon Wireless NTIA NOI Comments at 9.

⁷⁹ 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 (filed June 5, 2007) (CellAntenna 2007 Petition); Petition for Declaratory Ruling Regarding the Unlawful Sale and Use of Cellular Jammers and Wireless Boosters and Repeaters, *Petition for Declaratory Ruling*, WT Docket No. 10-4 (filed Nov. 2, 2007) (CTIA Petition); 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 (filed July 31, 2007) (The GEO Group Petition); Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission’s Rules and Creation of New Rules(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities, *Petition for Rulemaking*, PRM11WT (filed July 20, 2011) (GTL Petition); Request for Authorization of Managed Access Systems Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users, *Petition for Rulemaking*, PRM09WT (filed Aug. 21, 2009) (MDOC Petition); Letter from Michael W. McManus, Deputy General Counsel, Texas Department of Criminal Justice, to Kathryn S. Berthot, Chief, Spectrum Enforcement Division, Enforcement Bureau, FCC (Oct. 22, 2008) (TDCJ Letter); Request for Authorization of CMRS Jamming Within Correctional Institutions in Order to Improve Public Safety Under Conditions that Protect Legitimate CMRS Users, *Petition for Rulemaking*, PRM09WT (filed Aug. 6, 2009) (SCDC Petition). The SCDC Petition was co-signed by corrections officials of state and regional prison systems from 31 states and the District of Columbia. SCDC Petition at App.A.

⁸⁰ CellAntenna 2007 Petition at 3. CellAntenna also filed comments in response to the Commission’s proceeding examining wireless service interruptions, in which CellAntenna argued the Commission should forbear from applying Section 333 in order to allow correctional facilities to interrupt contraband wireless devices. CellAntenna Wireless Service Interruption Comments at 11.

⁸¹ The GEO Group Petition at 1. The Commission subsequently informed The GEO Group that because it is not a telecommunications carrier nor a class of telecommunications carriers the petition would not be deemed granted if
(continued...)

The South Carolina Department of Corrections (SCDC) seeks rule changes to make wireless devices in correctional facilities unauthorized devices under the Commission's rules if their possession is prohibited by state or local law, arguing that this would circumvent the statutory prohibition against willful and malicious interference against licensed or authorized stations.⁸² GTL included a similar request in its petition, which also seeks rule changes regarding managed access systems as discussed below.⁸³ The Texas Department of Criminal Justice sent a letter to the Commission's Enforcement Bureau seeking information on whether a process exists for it to be certified or permitted by the FCC to purchase and use radio signal jammers in prisons.⁸⁴ CTIA—The Wireless Association filed a petition opposing the use of radio signal jammers and seeking a declaratory ruling that the sale of radio signal jammers, except to federal users, is unlawful.⁸⁵

22. Two petitioners seek rule changes to facilitate the deployment of managed access systems.⁸⁶ In 2009, the Mississippi Department of Corrections (MDOC) filed a petition for rulemaking to amend the Commission's rules to make the possession or use of a radio frequency device in a correctional facility illegal, and to authorize the operation of managed access systems to prevent unlawful device use.⁸⁷ More recently, GTL filed a petition seeking to require wireless carriers to agree to technically-feasible spectrum leases necessary for a managed access system, and other rule changes.⁸⁸

23. In September 2011, CellAntenna filed a petition for rulemaking requesting rule changes that would require wireless carriers to terminate service to unauthorized wireless devices operating within correctional facilities.⁸⁹ CellAntenna proposes specific rules providing for a plan of detection and CMRS provider termination of service to identified contraband wireless devices.⁹⁰

(...continued from previous page)

the Commission failed to take action within the statutory period for action on petitions for forbearance. Letter from Julius P. Knapp, Chief, Office of Engineering and Technology, FCC, to Mitchell F. Brecher, Greenberg Traurig, LLP, ET Docket No. 08-73 (July 31, 2008).

⁸² SCDC Petition at 12-13.

⁸³ GTL Petition at 19-23; *infra* Part III.A.3.

⁸⁴ See TDCJ Letter. TDCJ also filed comments in response to the Commission's proceeding examining wireless service interruptions, in which TDCJ argued that "the use of a wireless service managed access solution at a correctional facility for the purposes of preventing unauthorized wireless service usage from the facility is an acceptable method of wireless service interruption." TDCJ Wireless Service Interruption Comments at 1.

⁸⁵ See CTIA Petition at 6-10. CTIA's petition also sought a declaration regarding the use of wireless signal boosters, which the Commission addressed in a separate proceeding. See 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, WT Docket No. 10-4, *Report and Order*, 28 FCC Rcd 1663 (2013).

⁸⁶ See MDOC Petition; GTL Petition.

⁸⁷ MDOC Petition at 11-12.

⁸⁸ GTL Petition at 9. GTL also urges the Commission to require licensees to provide spectrum to managed access providers on fair and economical terms in reply comments it filed in response to the Commission's proceeding examining wireless service interruptions. See GTL Wireless Service Interruption Reply Comments at 9-12.

⁸⁹ See Amendment of 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, *Petition for Rulemaking*, PRM11WT, at 8 (filed Sept. 2, 2011) (CellAntenna 2011 Petition).

⁹⁰ *Id.*

III. NOTICE OF PROPOSED RULEMAKING

A. Streamlining Authorization of Leases for Managed Access Systems for Use in Correctional Facilities

24. Managed access systems “permit[] calls by known users (*i.e.*, prison-authorized cell phone numbers) by handing them off to the network, but prevent others by denying access to the network.”⁹¹ The Commission has previously applied its existing spectrum leasing rules and procedures to allow the operation of managed access systems by entities that lease the necessary spectrum from spectrum licensees.⁹² Nonetheless, for the reasons discussed below, these rules and procedures are sufficiently time-consuming and complex that they can delay deployment of managed access systems, and therefore unnecessarily discourage their use. Below we set forth an overview of the existing spectrum leasing rules and procedures and propose to streamline the Commission’s spectrum leasing rules and processes to permit the more timely deployment of managed access systems. We seek comment on the proposals below, including the costs and benefits.

25. Throughout the *Notice*, where we seek comment on the costs and benefits of a proposal, we ask that commenters take into account only those costs and benefits that directly result from the implementation of the particular rules that could be adopted, including any proposed requirement or potential alternative requirement. Commenters should identify the various costs and benefits associated with a particular proposal. Further, to the extent possible, commenters should provide specific data and information, such as actual or estimated dollar figures for each specific cost or benefit addressed, including a description of how the data or information was calculated or obtained, and any supporting documentation or other evidentiary support.

1. Overview and Regulatory Environment for Managed Access

26. Managed access providers that have deployed systems have sought licensee consent and Commission authorization prior to operation of the systems, because they use base stations that transmit and receive signals on licensed frequencies.⁹³ Thus far, wireless providers and managed access providers have used spectrum lease agreements to negotiate the transfer of rights and have sought approval or provided notification of such agreements under the Commission’s spectrum leasing rules.⁹⁴ This approach requires negotiation of individual lease agreements with each wireless provider licensed to provide service where the correctional facility is located, and thus likely requires multiple lease negotiations and lease approvals or notifications for a single correctional facility. The number of leases is compounded where the provider seeks to deploy systems in multiple correctional facilities in different geographic locations served by multiple wireless providers. Additionally, as discussed below, the managed access lessee will likely

⁹¹ NTIA Report at 19.

⁹² See ShawnTech Lieber Leases; ShawnTech McConnell Leases; ShawnTech Stiles Leases; Tecore Baltimore Leases; Tecore Parchman Leases.

⁹³ See 47 U.S.C. § 301 (requiring a license for the “transmission of energy or communications or signals by radio”); *id.* § 310(d) (requiring application to the Commission for the transfer of any rights under a license to another party, such as a managed access provider).

⁹⁴ See ShawnTech Lieber Leases; ShawnTech McConnell Leases; ShawnTech Stiles Leases; Tecore Baltimore Leases; Tecore Parchman Leases; 47 C.F.R. §§ 1.9001-1.9080. An effective managed access solution requires leasing agreements from all licensees providing service to the target area. GTL Petition at 10-11. The lessee may be the correctional facility, a local or state agency, a managed access provider, or some other third party.

seek to modify its regulatory status from commercial mobile radio service (CMRS)⁹⁵ to PMRS, which requires additional filings and results in processing delays.

27. Given the current lease processing challenges and transaction costs involved in the deployment of managed access systems, we seek to streamline our filing requirements and application processing mechanisms, particularly with respect to our leasing rules as applied to managed access systems in correctional facilities. Below is an overview of our current relevant rules and processes followed by proposed modifications.

28. *Leasing Procedures Applicable to Managed Access.* Under current rules, lessees and licensees have three spectrum lease options: long-term *de facto* leases, short-term *de facto* leases, and spectrum manager leases.⁹⁶ The leases carry different rights and responsibilities for both the licensee and the lessee, with *de facto* leases vesting greater rights and responsibilities in the lessee than spectrum manager leases.⁹⁷

29. The Commission's rules require that the parties to a *de facto* lease file an application for approval of the lease with the Commission.⁹⁸ Parties to a spectrum manager lease must file a notification of the lease with the Commission and can commence operations without prior Commission approval after a short period.⁹⁹ The Commission's rules provide for expedited processing (by the next business day) for short-term *de facto* lease applications, and for long-term *de facto* lease applications and spectrum manager notifications that meet certain conditions.¹⁰⁰ To be accepted for processing, any application or notification

⁹⁵ CMRS is a mobile service that is provided for profit; interconnected; and "available to the public, or to such classes of eligible users as to be effectively available to a substantial portion of the public;" or the functional equivalent of CMRS. 47 C.F.R. § 20.3. See also 47 U.S.C. § 332(c)(1).

⁹⁶ 47 C.F.R. §§ 1.9020 (spectrum manager lease), 1.9030 (long-term *de facto* lease), 1.9035 (short-term *de facto* lease). See Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets, *Report and Order and Further Notice of Proposed Rulemaking*, 18 FCC Rcd 20604, 20624, 20671, ¶¶ 41, 160 (2003) (*First Secondary Market Report and Order*).

⁹⁷ Under a spectrum manager lease, the licensee "is directly and primarily responsible for ensuring the spectrum lessee's compliance with the Communications Act and applicable Commission policies and rules." 47 C.F.R. § 1.9020(b)(1). Under *de facto* lease arrangements, the licensee "retains *de jure* control of the license while *de facto* control of the leased spectrum is transferred to the spectrum lessee for the duration of the spectrum leasing arrangement." *Id.* §§ 1.9030(a), 1.9035(a). See also *id.* § 1.9010 (establishing the *de facto* control standard). Also, under *de facto* lease arrangements, the "primary responsibility for ensuring compliance with Commission policies is transferred to spectrum lessees." See *First Secondary Market Report and Order*, 18 FCC Rcd at 20664, ¶137; See also 47 C.F.R. § 1.9030(c)(1).

⁹⁸ 47 C.F.R. §§ 1.9030(a), (e), 1.9035(a), (e).

⁹⁹ *Id.* § 1.9020(e)(1). Under general notification procedures, spectrum manager leases for more than one year must be filed at least 21 days prior to the date of operation. Spectrum manager leases of one year or less must be filed at least 10 days prior to the date of operation. *Id.* § 1.9020(e)(1)(ii). We note that under immediate approval processes, acceptance of the notification will be reflected in ULS on the next business day following the day the application is filed, and spectrum manager lessees may operate upon acceptance consistent with the terms of the leasing arrangement. *Id.* § 1.9020(e)(2)(ii).

¹⁰⁰ *Id.* §§ 1.9020(e)(2), 1.9030(e)(2), 1.9035(e). See Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets, *Second Report and Order, Order on Reconsideration, and Second Further Notice of Proposed Rulemaking*, 19 FCC Rcd 17503, 17512, ¶ 14 n. 42 (2004) (*Second Secondary Market Report and Order*) ("[U]nder the immediate approval process, spectrum leasing parties must submit qualifying applications and include the requisite filing fees. The [Wireless Telecommunications] Bureau will then process the application overnight and . . . indicate in our Universal Licensing System (ULS) that the application has (continued....)

must be “sufficiently complete,” including information and certifications relating to a lessee’s eligibility and qualification to hold spectrum, and lessee compliance with the Commission’s foreign ownership rules.¹⁰¹ *De facto* applications must also be accompanied by the requisite filing fee.¹⁰²

30. Long-term *de facto* lease applications and spectrum manager notifications must meet three additional criteria for immediate approval or processing.¹⁰³ First, the license cannot involve spectrum that may be used to provide an interconnected mobile service and that would result in a geographic overlap with licensed spectrum “in which the proposed spectrum lessee already holds a direct or indirect interest of 10 [percent] or more.”¹⁰⁴ Second, the licensee cannot be “a designated entity or entrepreneur subject to unjust enrichment requirements and/or transfer restrictions under applicable Commission rules.”¹⁰⁵ Finally, the lease arrangement cannot “require a waiver of, or declaratory ruling pertaining to, any applicable Commission rules.”¹⁰⁶

31. Under these rules, managed access systems involving more than one lease will not be afforded immediate approval or processing for long-term *de facto* applications or spectrum manager notifications subsequent to the first approved application or accepted notification. Because lessees of spectrum used in managed access systems require spectrum leases from multiple carriers covering a common location, subsequent applications will always be removed from expedited processing because they will result in a geographic overlap with spectrum held by the lessee that may be used to provide an interconnected mobile service.¹⁰⁷

32. If a long-term *de facto* lease application is not subject to immediate approval, the application is placed on public notice generally within one week of filing¹⁰⁸ and petitions to deny may be filed within 14 days of the initial public notice date.¹⁰⁹ The Commission will take action to approve or deny the lease application or issue another public notice indicating the application will undergo further

(...continued from previous page)

been approved.”). Applications and notifications are filed on FCC Form 608, “FCC Application or Notification for Spectrum Leasing Arrangement.” 47 C.F.R. § 1.913(a)(5).

¹⁰¹ 47 C.F.R. §§ 1.9020(e)(2)(i), 1.9030(e)(2)(i), 1.9035(e).

¹⁰² *Id.* §§ 1.9030(e)(1)(i), (e)(2)(i), 1.9035(e)(1). *See also id.* § 1.9020(e)(1)(i). We note that governmental entities are not required to pay filing fees. *See id.* § 1.1116(f) (“For purposes of this exemption a governmental entity is defined as any state, possession, city, county, town, village, municipal corporation or similar political organization or subpart thereof controlled by publicly elected or duly appointed public officials exercising sovereign direction and control over their respective communities or programs.”).

¹⁰³ *Id.* §§ 1.9020(e)(2)(i)(A)-(C), 1.9030(e)(2)(i)(A)-(C). All short-term *de facto* applications are processed via immediate approval procedures. *See id.* § 1.9035(e).

¹⁰⁴ *Id.* §§ 1.9020(e)(2)(i)(A), 1.9030(e)(2)(i)(A).

¹⁰⁵ *Id.* §§ 1.9020(e)(2)(i)(B), 1.9030(e)(2)(i)(B).

¹⁰⁶ *Id.* §§ 1.9020(e)(2)(i)(C), 1.9030(e)(2)(i)(C). Short-term *de facto* lease applications must also meet this requirement. *Id.* § 1.9035(e)(1).

¹⁰⁷ *See id.* § 1.9020(e)(2)(i)(A), 1.9030(e)(2)(i)(A).

¹⁰⁸ *Id.* § 1.9030(e)(1)(ii) (explaining the general approval procedures, including for public notice, which are effective if the applicant does not meet the conditions under Section 1.9030(e)(2) of the Commission’s rules for immediate approval); *First Secondary Market Report and Order*, 18 FCC Rcd at 20668-69, ¶ 151 n.320 (“The Wireless Telecommunications Bureau currently expects to list leasing applications on weekly public notices.”).

¹⁰⁹ 47 C.F.R. § 1.9030(e)(1)(iii).

review no later than 21 days after the initial public notice date.¹¹⁰ While spectrum manager leases that are disqualified from immediate processing are not subject to as thorough review as long-term *de facto* leases, the licensee is required to file the notification at least 21 days in advance of operation if the lease term exceeds one year, or ten days if the lease term is for one year or less.¹¹¹

33. *PMRS Classification of Managed Access.* Managed access operators typically lease spectrum from wireless service providers that offer service on a CMRS basis and are regulated as CMRS providers under the Act and the Commission's rules.¹¹² CMRS providers are subject to common carrier obligations,¹¹³ which include the obligation to provide service upon reasonable request, at just, reasonable, and non-discriminatory rates.¹¹⁴ When a CMRS provider enters into a spectrum lease arrangement with a managed access provider, the managed access provider is also presumed to be providing CMRS.¹¹⁵ However, because managed access systems are configured to operate solely within the confines of a correctional facility and are not intended to provide service to the public, they may qualify as PMRS,¹¹⁶ exempting them from common carrier obligations.¹¹⁷ Changing regulatory status requires the managed access provider to file a separate application for each lease that has been approved. In addition, for leases in certain services (*e.g.*, Personal Communications Service), the modification application must be placed on a 30 day public notice.¹¹⁸ The requirement that a separate modification application be filed to change the regulatory status may therefore further delay deployment of a managed access system.

34. *Special Temporary Authority.* The Commission has authority under Section 309(f) of the Act to grant a STA if it finds "there are extraordinary circumstances requiring temporary operations in the public interest and that delay in the institution of such temporary operations would seriously prejudice the public interest."¹¹⁹ Under current rules, an applicant must file a STA request at least ten days prior to the applicant's proposed operation,¹²⁰ and STA requests for spectrum that is licensed on a market basis – such as PCS and 700 MHz – must be filed manually.¹²¹ Additionally, unless the STA application falls into one of several exemptions, it must be placed on public notice.¹²²

35. We seek to facilitate the prompt deployment of managed access systems by reducing unnecessary filing burdens and barriers to expedited processing, including for modification of the lessee's

¹¹⁰ *Id.* § 1.9030(e)(1)(iv)-(v). The Commission has 90 days to take action on an application requiring further review. *Id.* § 1.9030(e)(1)(v).

¹¹¹ *Id.* § 1.9020(e)(1)(ii).

¹¹² 47 U.S.C. § 332(c)(1); 47 C.F.R. § 20.9.

¹¹³ *See* 47 U.S.C. § 332(c)(1).

¹¹⁴ *Id.* §§ 201-202.

¹¹⁵ *See* 47 C.F.R. §§ 1.9020(d)(6), 1.9030(d)(6), 1.9035(d)(1).

¹¹⁶ *See id.* §§ 20.3, 20.9.

¹¹⁷ *See id.* § 20.9.

¹¹⁸ *Id.* § 20.9(b).

¹¹⁹ 47 U.S.C. § 309(f).

¹²⁰ 47 C.F.R. § 1.931(a).

¹²¹ Market-based licensees that file STA applications manually also have to file a simultaneous waiver of the electronic filing requirement. *See id.* § 1.913(b), (d) (requiring electronic filing, and permitting manual filing of Form 601 for several wireless services, excluding PCS).

¹²² *Id.* § 1.931(a)(2).

regulatory classification to PMRS and for applications for STA. Through streamlined regulatory processes, stakeholders will be better equipped to combat the use of contraband wireless devices in correctional facilities. Below we outline several proposed rule changes that could expedite the lease application or notification process for managed access systems. We seek comment on the proposed changes and other proposals on the record.

2. Proposed Rules to Streamline Managed Access Spectrum Leasing Procedures

36. We propose rule and procedural changes to facilitate a streamlined application process for spectrum leases entered into exclusively to combat the use of unauthorized wireless devices in correctional facilities, which we believe is in the public interest. 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.¹²³ The proposed rules and procedural changes below are consistent with this intent. Contraband wireless devices in correctional facilities are a threat to the safety and welfare of correctional facility workers, other prisoners, and the general public,¹²⁴ and managed access is an important option in combating their use.¹²⁵ The proposals we outline below seek to balance the need to minimize regulatory barriers to deploying managed access systems in correctional facilities with the need to maintain an effective lease review process and the need to protect legitimate wireless users. We seek comment on the costs and benefits of the proposed rule and process changes, including the extent to which they will reduce barriers to the deployment of managed access systems.

37. We propose to immediately process qualifying lease applications or notifications for managed access systems in correctional facilities, and to exercise our forbearance authority as necessary to implement this proposal.¹²⁶ We also propose to reduce the need for multiple application filings by creating a presumption that managed access services in correctional facilities are PMRS. Finally, we propose to streamline the process for seeking STA for managed access operators seeking to use leased spectrum prior to obtaining a more permanent system authorization.

i. Streamlined Lease Application Approval and Lease Notification Processing

38. We propose to modify the Commission's rules and procedures to make qualifying leases for managed access systems in correctional facilities subject to immediate processing and approval. Specifically, we propose to immediately process long-term *de facto* lease applications and spectrum manager notifications for managed access systems, even in cases where grant of multiple lease applications would result in the lessee holding geographically overlapping spectrum rights or where the license involves spectrum subject to designated entity unjust enrichment provisions or entrepreneur transfer restrictions.¹²⁷ Under this proposal, grant or acceptance of qualifying managed access leases

¹²³ 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).

¹²⁴ See *supra* Part II.A.

¹²⁵ See *supra* Part II.D.1.

¹²⁶ Under existing rules, which would apply to managed access leases as proposed herein, interested parties may petition for reconsideration of the grant or acceptance within 30 days of the public notice announcing the application was granted or accepted. 47 C.F.R. § 1.106(f).

¹²⁷ See 47 C.F.R. §§ 1.9020(e)(2)(i)(A), 1.9030(e)(2)(i)(A).

would be indicated the following business day on the Commission's Universal Licensing System (ULS).¹²⁸ The accepted lease would then be effective upon the date set forth by the licensee and lessee in the lease application or notification.¹²⁹ We seek comment on the specific rule changes necessary to implement this proposal below.

39. *Completeness Requirement.* We propose to require applications or notifications for managed access leases to meet the completeness standards set forth in our existing spectrum leasing rules.¹³⁰ Under our proposed process, licensees and lessees would continue to file Form 608,¹³¹ and would be required to complete all relevant fields and certifications on the form.¹³² If an application or notification is sufficiently complete but the responses or certifications raise questions regarding the lessee's eligibility or qualification to hold spectrum, we propose that the application or notification will not be eligible for immediate approval or processing consistent with the Commission's current processes.¹³³ We seek comment on this proposal, including on the costs and benefits.

40. *Competition.* We propose to immediately process lease applications or notifications for managed access systems in correctional facilities regardless of whether the approval or acceptance will result in the lessee holding or having access to geographically overlapping licenses that may be used to provide an interconnected mobile service.¹³⁴ Our rules requiring more lengthy case-by-case review of leases that would result in the lessee holding geographically overlapping spectrum are intended to focus on leases that "potentially raise competition concerns."¹³⁵ In the managed access context, however, we believe such review is unnecessary because managed access systems intended solely to combat contraband wireless devices in correctional facilities do not raise the same competitive concerns as multiple licenses leased in the same geography to provide a CMRS.¹³⁶ Managed access providers are not offering service to the public, and will generally contract directly with a correctional facility to be the sole managed access provider. We seek comment on this proposal and analysis.

¹²⁸ ULS is the Commission's online database and filing system for applications and fees for most radio services. See FCC, ULS, <http://wireless.fcc.gov/uls/index.htm?job=home>. Applications and notifications for leases for managed access systems would continue to be placed on a weekly information public notice once granted or accepted, as required under the Commission's rules. 47 C.F.R. §§ 1.9020(e)(1)(iii), (2)(iii); 1.9030(e)(1)(ii); 1.9030(e)(2)(iii); 1.9035(e)(3).

¹²⁹ 47 C.F.R. §§ 1.9020(f), 1.9030(f) (establishing that the lease is effective in the Commission's records, and for application of the leasing rules, upon the date of the lease term as specified in the notification or application).

¹³⁰ Under the Commission's current spectrum leasing rules, applications or notifications that are subject to immediate processing or approval must be "sufficiently complete." *Id.* §§ 1.9020(e)(2)(i), 1.9030(e)(2)(i), 1.9035(e).

¹³¹ *Id.* § 1.913(a)(5) ("FCC Form 608 is used by licensees and spectrum lessees . . . to notify the Commission regarding spectrum manager leasing arrangements and to apply for Commission consent for *de facto* transfer leasing arrangements . . ."). See also FCC Form 608, FCC Application or Notification for Spectrum Leasing Arrangement, www.fcc.gov/forms.

¹³² FCC Form 608 at 9-11. Additionally, *de facto* applications must be accompanied by the requisite filing fee. 47 C.F.R. §§ 1.9030(e), (e)(2), 1.9035(e).

¹³³ See 47 C.F.R. §§ 1.9020(e)(1), 1.9030(e)(1).

¹³⁴ See 47 C.F.R. §§ 1.9020(e)(2)(i)(A), 1.9030(e)(2)(i)(A).

¹³⁵ *Second Secondary Market Report and Order*, 19 FCC Rcd at 17516-17, ¶ 25.

¹³⁶ In the *Second Secondary Market Report and Order*, the Commission explained that competition policies focused "on services that could potentially affect the product market for mobile telephony, which includes interconnected mobile voice and/or data services." *Id.* at 17518, ¶ 26.

41. *Designated Entity/Entrepreneur Eligibility.* We also propose to immediately process lease applications or notifications for managed access systems in correctional facilities regardless of whether they implicate designated entity rules, affiliation restrictions, unjust enrichment prohibitions, or transfer restrictions.¹³⁷ We believe managed access leases do not raise public interest concerns regarding compliance with these rules that would necessitate a more in depth review of the applications or notifications. The Commission's unjust enrichment rules and transfer restrictions are designed to prevent a designated entity or entrepreneur from gaining from the special benefits conferred with the designation by selling or transferring the license,¹³⁸ and to ensure that "small business participation in spectrum-based services is not thwarted by transfers of licenses to non-designated entities."¹³⁹ Further, the Commission's affiliation and controlling interests rules for designated entities are meant to prevent a non-eligible affiliate of a designated entity from gaining through the special benefits conferred with the designation.¹⁴⁰ These rules were crafted under authority to ensure that certain entities have the opportunity to participate in the provision of wireless service, and to impose transfer disclosures and anti-trafficking restrictions to avoid unjust enrichment.¹⁴¹ Eliminating this certification for managed access leases covering correctional facilities does not impact the opportunity of another entity to participate in the provision of wireless service outside of the correctional facility, and likely will not result in unjust enrichment or transfer violations. It will similarly not impact the ability of a small business to participate in the provision of wireless services. We believe managed access lease arrangements implemented to combat contraband wireless devices in correctional facilities are in the public interest and override any potential marginal benefit a lessor might gain from leasing spectrum within the limited geographic area of a correctional facility. We seek comment on this proposal and analysis, and on any costs or benefits of this proposal.

42. *Procedural Requirements.* We propose to modify FCC Form 608 to allow managed access providers and CMRS licensees to identify that a proposed lease is a managed access lease exclusively for a system in a correctional facility. We also propose to require managed access providers to attach a written certification to the application or notification explaining the nature of the managed access system, including the location of the correctional facility, the managed access provider's relationship to the correctional facility, and the exact proposed coordinates of the leased spectrum boundaries. The information and certification on Form 608 will establish that the lease is to be used solely for a managed access system, and the coordinates will establish the geographic boundaries of the leased area.

43. As outlined in the *Second Secondary Market Report and Order* and incorporated into the Commission's rules, once a lease application grant or notification acceptance is announced by public notice, interested parties may petition for reconsideration of the grant or acceptance within 30 days of the public notice, and the Commission may reconsider the grant or acceptance on its own motion within 40

¹³⁷ Short-term *de facto* leases similarly are not reviewed for implication of designated entity rules, affiliation restrictions, unjust enrichment prohibitions, or transfer restrictions. 47 C.F.R. § 1.9035(e). See also *First Secondary Market Report and Order*, 18 FCC Rcd at 20676, ¶ 176; *Second Secondary Market Report and Order*, 19 FCC Rcd at 17525, ¶ 44.

¹³⁸ See 47 C.F.R. § 1.2111.

¹³⁹ Amendment of Part 1 of the Commission's Rules – Competitive Bidding Procedures; Allocation of Spectrum Below 5 GHz Transferred from Federal Government Use; 4660-4685 MHz, WT Docket No. 97-82, ET Docket No. 94-32, *Third Report and Order and Second Further Notice of Proposed Rulemaking*, 13 FCC Rcd 374, 406, ¶ 52 (1997).

¹⁴⁰ See 47 C.F.R. § 1.2110(c)(2); *Second Secondary Market Report and Order*, 19 FCC Rcd at 17538, ¶ 71. A controlling interest is an entity or individual with *de jure* or *de facto* control over the designated entity. 47 C.F.R. § 1.2110(c)(2).

¹⁴¹ See *Second Secondary Market Report and Order*, 19 FCC Rcd at 17538, ¶ 71; 47 U.S.C. § 309(j)(4)(D)-(E).

days of the public notice.¹⁴² Regarding enforcement mechanisms, the Commission “retains the right to investigate and terminate any spectrum manager leasing arrangement if it determines, post-notification, that the arrangement . . . is otherwise in violation of the rules of this chapter, or . . . raises public interest concerns.”¹⁴³ The Commission further requires that agreements between licensees and spectrum lessees concerning spectrum leasing arrangements must contain a provision that the “spectrum lessee must comply at all times with applicable rules set forth in this chapter and other applicable law and that spectrum leasing arrangement may be revoked, cancelled, or terminated by the licensee or Commission if the spectrum lessee fails to comply with the applicable requirements.”¹⁴⁴ The Commission has also provided that *de facto* spectrum lessees are issued authorizations that bring them within the scope of the direct forfeiture procedures under Section 503(b) of the Act.¹⁴⁵ Finally, as stated in the *Second Secondary Market Report and Order*, to the extent the Commission determines that any certification made by the licensee or lessee “is not true, complete, correct, and made in good faith, the Commission will be vigilant in taking appropriate enforcement action, potentially including forfeitures or termination of the spectrum leasing arrangement.”¹⁴⁶ We seek comment on our proposal to continue to apply these rules to managed access leases, and whether these protections are sufficient to ensure rule compliance in the context of Commission authorization of managed access systems deployed to combat contraband phone use, and whether any additional conditions or alternative mechanisms are required to further the public interest. We also seek comment on any associated costs or benefits of our proposed approach.

44. Finally, we seek comment on whether managed access operators should be encouraged or required to provide notification to households and businesses in the vicinity of the correctional facility in which a managed access system is installed. If so, we seek comment on the form of such notification, for example, an informational notice on the company’s website, a placard or informational flyer on the doors of households and businesses within a certain proximity to the correctional facility, or a newspaper advertisement or other public notice. Additionally, if notification were required, we seek comment on the methods that managed access vendors should offer to wireless users to contact the managed access provider to address any impact on nearby consumer wireless services. We also seek comment on how the appropriate boundary of the notice area would be established, the timeframe for providing notice within that boundary, and related concerns. Lastly, we seek comment on the costs that would be associated with notification.

ii. PMRS Presumption

45. We propose to amend Section 20.9 of our rules to establish that managed access services in correctional facilities provided on spectrum leased from CMRS providers shall be presumptively treated as PMRS. We propose to require the lessee to certify on the application or notification that the leased spectrum will be used solely for the operation of a managed access system at a correctional facility. Where managed access operations are confined to a correctional facility and are not intended for provision of commercial service to the public, we believe that PMRS classification is appropriate under our rules because the provider is not offering service to the public or a substantial portion of the public.¹⁴⁷ Under

¹⁴² See *Second Secondary Market Report and Order*, 19 FCC Rcd at 17520, 17527-28, ¶¶ 31, 49; 47 C.F.R. §§ 1.106(f), 1.117.

¹⁴³ 47 C.F.R. § 1.9020(g).

¹⁴⁴ *Id.* § 1.9040(a)(1).

¹⁴⁵ *Id.* § 1.9030(c)(2).

¹⁴⁶ *Second Secondary Market Report and Order*, 19 FCC Rcd at 17521, ¶ 33.

¹⁴⁷ 47 C.F.R. §§ 20.3, 20.9. As discussed herein, PMRS licensees are not subject to common carrier obligations applicable to CMRS licensees under the Act.

this proposal, managed access providers will not need to file a separate application to request PMRS treatment following approval or acceptance of the lease. The PMRS presumption will apply to all leases of spectrum used exclusively in managed access systems in correctional facilities, and will be reflected upon the approval or acceptance of the lease. This proposal is not intended to restrict a lessee's flexibility to operate within a chosen regulatory status for which the system qualifies. Therefore, a managed access lessee would retain the option of applying for CMRS status by including an exhibit to Form 608 demonstrating that the service meets the CMRS definition or is the functional equivalent of CMRS.¹⁴⁸ We seek comment on these proposals, and on any costs or benefits they may impose.

46. We also seek comment on whether we should apply the Commission's 911 and enhanced 911 (E911) rules to managed access services that provide access to 911 and E911.¹⁴⁹ As a technical matter, managed access systems can be configured to pass 911 and E911 calls to the appropriate public safety answering point, regardless of whether the call is made from an unauthorized device.¹⁵⁰ Although managed access services ordinarily qualify as PMRS, and therefore are not subject to the Commission's 911 and E911 rules,¹⁵¹ we seek comment on whether there are potential benefits to applying some or all of the Commission's 911 or E911 rules to a managed access provider operating as a PMRS that transmits 911 or E911 calls on its system.¹⁵² We also seek comment on any associated costs or burdens that would be created by such a requirement.

iii. Compliance with Sections 308, 309, and 310(d) of the Act

47. In the *Second Secondary Market Report and Order* the Commission exercised forbearance in order to immediately process, without public notice or prior Commission review or consent, *de facto* leases that met eligibility and use restrictions but not did require a waiver or declaratory ruling and did not raise issues regarding competition, designated entity or entrepreneurship restrictions, or other public interest concerns.¹⁵³ We propose to extend that forbearance in order to immediately process *de facto* leases for managed access systems in correctional facilities that do not raise concerns with use and

¹⁴⁸ The lessee can continue to utilize the existing mechanism in the Commission's rules for rebutting the presumption that a mobile service does not meet the CMRS definition through a petition for declaratory ruling. 47 C.F.R. § 20.9(a)(ii).

¹⁴⁹ See 47 C.F.R. § 20.18.

¹⁵⁰ See NTIA Report at 21-22; MDOC Petition at 7; AT&T NTIA NOI Comments at 11; Sprint Nextel NTIA NOI Comments at 1; Tecore NTIA NOI Comments at 11; T-Mobile NTIA NOI Comments at 8; Verizon Wireless NTIA NOI Comments at 10. *But see* Enterprise Electronics NTIA NOI Comments at 5 (arguing that despite the ability of managed access systems to provide 911 and E911 access to contraband devices, inmates will abuse the service and should not be granted access).

¹⁵¹ Section 20.18 of the Commission's rules applies to CMRS providers that "[o]ffer real-time, two way switched voice service that is interconnected with the public switched network; and [u]tilize an in-network switching facility that enables the provider to reuse frequencies to accomplish seamless hand-offs of subscriber calls." 47 C.F.R. § 20.18(a). The Commission's spectrum leasing rules impose varying E911 obligations for the licensee and lessee depending on the type of lease. In long-term *de facto* lease arrangements, the lessee is required to meet the Commission's E911 requirements to the same extent that the licensee is, "insofar as the spectrum lessee's operations are encompassed within the E911 obligations." *Id.* § 1.9030(d)(8). In spectrum manager leases, the licensee retains any E911 obligations that apply to the leased spectrum. *Id.* § 1.9020(d)(8). In short-term *de facto* leases, the licensee retains any E911 obligations with respect to the leased spectrum, and the lessee is not required to comply with any E911 obligations. *Id.* § 1.9035(d)(4).

¹⁵² See *id.* § 20.18.

¹⁵³ *Second Secondary Market Report and Order*, 19 FCC Rcd at 17512-13, 17521-23, ¶¶ 15, 34-37.

eligibility restrictions, that do not require a waiver or declaratory ruling with respect to a Commission rule, but that do involve leases of spectrum in the same geographic area or involve designated entity rules, affiliation restrictions, unjust enrichment prohibitions, and transfer restrictions. Specifically, we propose to forbear from the applicable prior public notice requirements and individualized review requirements of Sections 308, 309, and 310(d) of the Act.¹⁵⁴

48. Section 10 of the Act authorizes the Commission to forbear from applying any regulation or provision of the Act to a telecommunications carrier or telecommunications service, or any class of telecommunications carriers or telecommunications services, if:

- (1) enforcement of such regulation or provision is not necessary to ensure that the charges, practices, classifications, or regulations by, for, or in connection with that telecommunications carrier or telecommunications service are just and reasonable and are not unjustly or unreasonably discriminatory; (2) enforcement of such regulation or provision is not necessary for the protection of consumers; and (3) forbearance from applying such provision or regulation is consistent with the public interest.¹⁵⁵

In the *Second Secondary Market Report and Order* the Commission found that the forbearance prongs were met for *de facto* leases that did not raise concerns with eligibility and use restrictions, foreign ownership restrictions, designated entity or entrepreneur restrictions, competition concerns, or other public interest concerns.¹⁵⁶ The Commission based its decision on its finding that even lease applications that were not immediately processed were not reviewed for the impact on the practices or charges of the providers, and therefore forbearance would have no impact on practices or charges.¹⁵⁷ Further, it found that a more thorough application review for leases qualifying for immediate approval was not necessary to protect consumers because the Commission had concluded that it would only immediately approve applications that did not raise public interest concerns.¹⁵⁸ Finally, the Commission concluded that forbearance from public notice and individualized Commission review were in the public interest because leases that did not raise public interest concerns would be approved quickly, reducing transaction costs, speeding time to market of services, improving spectrum access and efficiency, and increasing consumers' access to advanced wireless services.¹⁵⁹

49. We seek comment on whether the statutory forbearance requirements are met for our proposal to forbear from applying the individualized review and public notice provisions of Section 308, 309, and 310(d) of the Act for *de facto* managed access leases that do not raise concerns with eligibility and use restrictions or foreign ownership restrictions, and that do not require a waiver or declaratory ruling with respect to a Commission rule. For the reasons discussed in the *Second Secondary Market Report and Order*, we believe that managed access leases also generally qualify for the forbearance granted to all *de facto* leases.¹⁶⁰ Further, we believe that the statutory forbearance requirements are met for *de facto* managed access leases that comply with the necessary immediate approval procedures in our rules, but also involve leases of spectrum in the same geographic area or involve designated entity unjust enrichment

¹⁵⁴ 47 U.S.C. §§ 308, 309, 310(d).

¹⁵⁵ 47 U.S.C. § 160(a).

¹⁵⁶ *Second Secondary Market Report and Order*, 19 FCC Rcd at 17512-13, ¶ 15.

¹⁵⁷ *Id.* at 17522, ¶ 35.

¹⁵⁸ *Id.* at 17522-23, ¶ 36.

¹⁵⁹ *Id.* at 17523, ¶ 37.

¹⁶⁰ *Id.* at 17522-23, ¶¶ 35-37.

provisions and transfer restrictions. As described *supra*, these systems necessarily require overlapping spectrum in the same geographic area and likely do not run counter to the intent and purpose behind our rules governing unjust enrichment or transfer restrictions.¹⁶¹ We believe there is an overriding public interest in preventing prisoners from using wireless devices to further a criminal enterprise from within correctional facilities, which necessitates a streamlined application review process for spectrum leases for managed access systems in correctional facilities. We seek comment on this analysis.

iv. Streamlined Special Temporary Authority Request Processing

50. Finally, we propose to streamline the process for a managed access provider to obtain STA to operate a managed access system in a correctional facility prior to obtaining a more permanent authorization. We propose to exempt managed access providers seeking STAs for a managed access system in correctional facilities from the requirement that they file the STA application ten days prior to operation.¹⁶² We also propose to process STA requests for managed access systems in correctional facilities without prior public notice. Further, we propose to make changes to ULS to electronically process STA applications for market based licenses, such as PCS. Under this process, applicants would still be required to meet all of the existing requirements to be granted STA.¹⁶³ Additionally, applicants would be required to attach an exhibit to the application explaining the nature of the managed access system, including the location of the correctional facility, the applicant's relationship to the correctional facility, and the exact coordinates of the spectrum boundaries.¹⁶⁴ We also propose to modify FCC Form 601, which is used to apply for STAs, to allow an applicant to identify that the application is being filed for a managed access system in a correctional facility. This will allow the application to be removed from ordinary processing and entered into expedited processing.

51. We seek comment on the extent to which the expedited STA process proposed above will facilitate the deployment of managed access systems. In light of our proposals to expedite processing and approval for qualifying managed access leases, we do not anticipate that managed access providers will ordinarily require STAs prior to the grant of a lease application or acceptance of a lease notification. However, to the extent a managed access operator needs to test the system or operate on an emergency basis prior to obtaining approval or acceptance of a lease, this proposed streamlined process may serve to expedite the entire deployment timeframe. We seek comment on this analysis and proposal, and any costs it may impose or benefits it may generate.

3. Other Proposals

52. GTL and MDOC separately filed petitions for rulemaking seeking various rule changes to expedite the deployment of managed access systems,¹⁶⁵ and Tecore filed comments in another proceeding

¹⁶¹ See *supra* Part III.A.2.i.

¹⁶² See *id.* § 1.931(a).

¹⁶³ See *id.* (establishing that applications “must contain complete details about the proposed operation and the circumstances that fully justify and necessitate the grant of STA”).

¹⁶⁴ We propose to require that applicants for immediate lease application approval or notification processing include the same exhibit in the lease application or notification. See *supra* Part III.A.2.i.

¹⁶⁵ See generally GTL Petition; MDOC Petition. GTL proposes rule changes that would expedite the lease negotiation process, impose network upgrade notification obligations on licensees, set limits on the amount of “over-coverage” by managed access systems, and protect E911 in areas where managed access systems operate. GTL Petition at 9. MDOC seeks rule changes to allow state and local government entities to obtain site-based licenses for managed access systems on a coordinated secondary basis to licensee use of the licensed spectrum. MDOC Petition at 11.

outlining several rule and procedural changes it also believes are necessary to expedite managed access lease processing and system deployment.¹⁶⁶ We seek comment generally on these proposals and the extent to which they may be incorporated into the lease processing and approval proposals outlined above.¹⁶⁷

B. Detection

1. Overview and Regulatory Environment for Detection Systems

53. In addition to our proposals regarding streamlining the lease application process for managed access systems, we also seek comment on proposals to facilitate the deployment of detection systems. Detection systems are another method used by correctional facility administrators or operators to meet the joint objectives of discovering and disabling contraband wireless devices without interfering with legitimate wireless users.¹⁶⁸ Detection systems generally identify the location of a contraband wireless device through triangulation,¹⁶⁹ and can be accurate to within a few meters.¹⁷⁰ The systems are highly scalable – they can expand coverage with new sensors, and can detect signals across many frequency bands.¹⁷¹ Detection system operators do not require a FCC license or FCC authorization.¹⁷² As detection systems are passive and can only approximate the location of a contraband device, correctional facility employees must search for and physically confiscate the identified contraband device to terminate operations.¹⁷³ This potentially increases the cost and reduces the effectiveness of these systems and unnecessarily threatens the safety of correctional facility workers.¹⁷⁴

54. In September 2011, CellAntenna filed a petition for rulemaking requesting rule changes that would require wireless carriers to terminate service to unauthorized wireless devices operating in correctional facilities discovered by a detection system.¹⁷⁵ CellAntenna argues that detection systems are superior to managed access and jamming systems because detection systems do not threaten to cause

¹⁶⁶ See generally Tecore Wireless Service Interruption Comments. Tecore urges the Commission to make rule changes to create a scheme that would authorize the installation of a managed access system either by a relevant licensee or through a spectrum lease with a relevant state or local agency or designated third party. *Id.* at 46-50.

¹⁶⁷ We note that we will incorporate these petitions into the record established pursuant to this *Notice* through GN Docket No. 13-111.

¹⁶⁸ See CTIA NTIA NOI Comments at 17; ITT NTIA NOI Comments at 3; Sprint NTIA NOI Comments at 2; T-Mobile NTIA NOI Comments at 9-10.

¹⁶⁹ See NTIA Report at 27; BINJ NTIA NOI Comments at 7; Enterprise Electronics NTIA NOI Comments at 8.

¹⁷⁰ See ITT NTIA NOI Comments at 18; NTIA Report at 29.

¹⁷¹ See ITT NTIA NOI Comments at 8; BINJ NTIA NOI Comments at 4; Berkley Varitronics NTIA NOI Comments at 5.

¹⁷² See NTIA Report at 30. The equipment itself, however, may need Commission certification before it can be marketed and sold. See 47 C.F.R. § 15.101(a) (listing unintentional radiators as equipment that shall be authorized under the Commission's rules, including several types of receivers).

¹⁷³ See CellAntenna 2011 Petition at 7 (“[T]he ensuing physical searches are time (and resource) consuming and can be dangerous for correctional personnel.”); ITT NTIA NOI Comments at 5 (“The drawback to detection is that someone has to take an action to retrieve the phone.”).

¹⁷⁴ CellAntenna 2011 Petition at 7; GTL NTIA NOI Comments at 3-4; ITT NTIA NOI Comments at 5. Even if identified contraband devices are not confiscated, however, detection systems are capable of gathering a large amount of data about contraband wireless devices, including the number of transmissions, the times of day they are used, and the length of use. See BINJ NTIA NOI Comments at 7; CTIA NTIA NOI Comments at 14.

¹⁷⁵ See CellAntenna 2011 Petition at 7-8.

interference with carrier networks.¹⁷⁶ CellAntenna also believes its proposal will remedy the need to physically confiscate contraband wireless devices, a clear drawback of current detection systems.¹⁷⁷ CellAntenna proposes a three step plan. First, the correctional facility identifies unauthorized wireless devices within the facility; second, the warden transmits the identifying information of the contraband device to the appropriate CMRS provider via email or fax; and third, the CMRS provider sends a SMS message to the unauthorized device notifying the user that the device is unauthorized and suspends service to the device within one hour of receiving notice from the warden.¹⁷⁸

55. CellAntenna also proposes a new rule to hold harmless CMRS providers from violation of a law or regulation when the provider terminates service to a device if the provider acted in good faith to terminate service in reliance on a warden's notice and took immediate action to reinstate suspended service if "presented with compelling evidence contradicting the Warden's notice."¹⁷⁹ As discussed below, we seek comment on CellAntenna's proposal, including any costs or benefits of the proposal.

2. Disabling Contraband Wireless Devices through Improved Coordination

56. Consistent with CellAntenna's proposal, we propose to require CMRS licensees to terminate¹⁸⁰ service to contraband devices within correctional facilities pursuant to a qualifying request from an authorized party. We seek comment on the costs and benefits of this proposal.

57. We note the nexus between this proposal and the wireless industry's recent voluntary commitment to take steps to help deter smartphone thefts and protect consumer data.¹⁸¹ Under the commitment, participating wireless providers will work to implement and deploy database solutions using unique smartphone identification numbers to prevent stolen smartphones from being activated or from receiving service.¹⁸² The commitment represents a significant recognition of the public interest benefits of deterring unauthorized use of wireless devices and the feasibility of a technological solution that can uniquely identify a stolen device and terminate service to the device.¹⁸³

58. Similar technological solutions could be used to combat the serious problem of contraband wireless device use in correctional facilities, for example by enhancing the effectiveness of detection technologies through CMRS provider termination of service to identified contraband devices. Detection systems arguably have the least impact on legitimate wireless users relative to other technical approaches to

¹⁷⁶ *Id.* at 6-7.

¹⁷⁷ *Id.* at 6-9.

¹⁷⁸ *Id.* at 8.

¹⁷⁹ *Id.* at 10.

¹⁸⁰ CellAntenna refers to the "suspension" of service under its proposal. *Id.* at 8.

¹⁸¹ See CTIA Consumer Info, U.S. Wireless Industry Steps to Help Deter Smartphone Thefts and Protect Consumer Data (Wireless Industry Commitment), available at http://www.ctia.org/consumer_info/safety/index.cfm/AID/12084.

¹⁸² *Id.* As announced, the commitment only applies to GSM and LTE smartphones. See *id.*

¹⁸³ See *id.* Chairman Genachowski, in remarks delivered at a press conference announcing the initiative, noted that similar database solutions were operating in the United Kingdom and other countries. See Julius Genachowski, Chairman, FCC, Prepared Remarks on Stolen Cell Phones Initiative (Apr. 10, 2012), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-313512A1.pdf.

combating contraband wireless device use in correctional facilities,¹⁸⁴ but their overall effectiveness is limited by the inability of the system operator to terminate service to detected devices. Detection-based interdiction technology is more effective when combined with carrier termination of service to identified contraband devices by all CMRS providers covering a given correctional facility. If a single CMRS provider whose coverage area includes a correctional facility does not terminate service to contraband devices identified in the facility, the demand for contraband devices that can receive service from that provider will likely dramatically increase. When all CMRS providers terminate service to unauthorized devices pursuant to authenticated requests, detection systems can transform from a solution that can only identify wireless devices to a powerful solution that can lead to the termination of service without physical intervention, and without a significant impact on legitimate wireless users. We seek comment on this analysis. We also seek comment on the possible effectiveness of voluntary carrier participation in an industry wide effort to terminate service to contraband wireless devices.

59. In addition to the proposals to facilitate managed access or detection systems discussed above, we also propose to adopt several elements of the CellAntenna proposal to require CMRS providers to terminate service to identified contraband wireless devices. We seek comment below on the specific information that the correctional facility must transmit to the provider to effectuate termination, timing for carrier termination, methods of authenticating a termination request, and other issues. We also seek comment on the costs and benefits on each of the proposals discussed below.¹⁸⁵ In particular, we seek comment on the specific cost burdens that a carrier would face in establishing the reporting mechanisms, technical upgrades, if any, operational enhancements, and personnel training necessary to handle requests for termination. In addition, to the extent that carriers incur such costs to support requests for termination, we seek comment on mechanisms by which carriers could recoup the initial and ongoing expense of complying with a requirement to terminate service to contraband devices, including cost sharing mechanisms with correctional facilities.

60. We believe the Commission has authority under Section 303 to require CMRS providers to terminate service to contraband wireless devices.¹⁸⁶ Under Section 303(b), the Commission is required to “[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class.”¹⁸⁷ Additionally, Section 303(d) requires the Commission to “[d]etermine the location of classes of stations or individual stations,”¹⁸⁸ and Section 303(h) grants the Commission the “authority to establish areas or zones to be served by any station.”¹⁸⁹ When tied together with Section 303(r), which requires the Commission to “[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this chapter,”¹⁹⁰ and Section 4(i), which authorizes the Commission to “perform any and all acts, make such rules and

¹⁸⁴ Wireless detection systems do not transmit radio frequencies and therefore do not pose a risk of interference to other wireless users. NTIA Report at 28; CellAntenna 2011 Petition at 6-7.

¹⁸⁵ As established in the previous Part, when we seek comment on a proposal, we ask commenters to take into account the costs and benefits that flow directly from the particular rules or proposals, including potential alternative requirements. We further ask commenters to be specific, to the extent possible, by including estimated dollar figures or any other supporting documentation or evidentiary support. *See supra* ¶ 25.

¹⁸⁶ *See* 47 U.S.C. § 303.

¹⁸⁷ 47 U.S.C. § 303(b). *See also Cellco Partnership v. FCC*, 700 F.3d 534, 542-43 (D. C. Cir. 2012) (upholding Commission’s roaming rules for mobile data providers, broadly reading phrase “prescribe the nature of the service to be rendered” to mean “lay[] down a rule about ‘the nature of the service to be rendered’”).

¹⁸⁸ 47 U.S.C. § 303(d).

¹⁸⁹ *Id.* § 303(h).

¹⁹⁰ *Id.* § 303(r).

regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions,¹⁹¹ we believe that these provisions empower the Commission to implement this proposal. We seek comment on this analysis.

i. Identifying Contraband Devices

61. We seek to ensure that service is terminated only to contraband devices operated within a correctional facility and not lawful subscriber devices possibly operating in close proximity to a correctional facility. Existing detection technologies are reportedly capable of accurately identifying the location of unauthorized wireless devices in a correctional facility within several meters,¹⁹² with reportedly little or no risk of identifying legitimate wireless devices outside of the facility.¹⁹³ Each sensor in a detection system can be physically positioned to detect wireless transmissions within a certain path, and can determine the approximate distance between the sensor and the detected device.¹⁹⁴ The unknown location of the contraband device is determined by “measuring the distances from the point of [the] unknown location . . . to three or more points of known location.”¹⁹⁵ Detection providers can increase accuracy by positioning multiple sensors with overlapping zones of detection.¹⁹⁶ Software analyzes the data from the sensors to generate coordinates used to identify the approximate location of the device, which can then be displayed using a geographic information system depicting the location of the device on a floor plan or some other map of the facility.¹⁹⁷

62. Detection systems can reportedly identify wireless devices in various states of use, including when a wireless device places or receives a call, sends or receives a text message, or sends or retrieves data.¹⁹⁸ When a device attempts to connect to the network, CellAntenna asserts that detection systems can identify specific information about the device, including the service provider, electronic serial number (ESN), mobile identification number (MIN), international mobile equipment identifier (IMEI), or the international mobile subscriber identity (IMSI).¹⁹⁹ According to CellAntenna, when this unique identifying information is transmitted to the device’s CMRS provider, the CMRS provider could identify the device in its systems by its ESN, MIN, IMEI, or IMSI and terminate service to the device.²⁰⁰ We seek comment on this technical analysis and on any safeguards that may be necessary to protect against the unlikely event that an authorized device outside of the correctional facility is detected. We also seek comment on the costs and benefits of any proposed safeguards.

63. While the Commission does not directly license the operation of detection systems, we seek comment on the appropriate criteria that must be met by an entity requesting that a carrier terminate service to a contraband device in a correctional facility identified by a detection system. In its petition,

¹⁹¹ *Id.* § 154(i).

¹⁹² See ITT NTIA NOI Comments at 18; NTIA Report at 29.

¹⁹³ BINJ NTIA NOI Comments at 2 (“Cell phone detection systems do not pose a threat to legitimate cell phone use by the general public outside the prison.”).

¹⁹⁴ See Enterprise Electronics NTIA NOI Comments at 10.

¹⁹⁵ TruePosition NTIA NOI Comments at 2.

¹⁹⁶ See NTIA Report at 29.

¹⁹⁷ See Enterprise Electronics NTIA NOI Comments at 8; BINJ NTIA NOI Comments at 2.

¹⁹⁸ See BINJ NTIA NOI Comments at 8; Enterprise Electronics NTIA NOI Comments at 7-8.

¹⁹⁹ CellAntenna 2011 Petition at 7.

²⁰⁰ See *id.*