CONTRABAND CELL PHONES IN PRISONS

Possible Wireless Technology Solutions

U.S. Department of Commerce
Gary Locke
Secretary of Commerce

Lawrence E. Strickling
Assistant Secretary for
Communications and
Information

December 2010

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Telecommunications and Information Administration (NTIA) submits this report in response to a direction from Congress in December 2009 that NTIA, in coordination with the Federal Communications Commission (FCC), the Federal Bureau of Prisons (BOP), and the National Institute of Justice (NIJ), develop a plan to investigate and evaluate wireless jamming, detection, and other technologies that might be used to prevent contraband cell phone use by prison inmates. NTIA has identified and evaluated several technology solutions for this report that can be used in a prison environment, including jamming, managed access, and detection techniques. In the preparation of this report, NTIA sought input from the FCC, NIJ, and BOP regarding their efforts to combat contraband cell phone use.

The Administration believes that contraband cell phone use by prison inmates to carry out criminal enterprises is intolerable and demands an effective solution. Prison 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.

To obtain public input on these issues to assist in developing this report, NTIA issued a Notice of Inquiry (NOI) in May 2010 soliciting comment on a series of detailed questions to help identify, clarify, and characterize these solutions. NTIA received comments from forty-six sources. In addition to providing input regarding the three technologies identified in the NOI, commenters identified additional technologies for consideration.

Working in coordination with its Institute for Telecommunication Sciences, NTIA performed both laboratory and field measurements on a selected jammer. NTIA subsequently analyzed the results of those measurements to determine, as far as possible, the potential impact of that jammer on other authorized radio operations.

This report discusses the characteristics and capabilities of the various technologies and considers the potential interference effects that they may have on authorized radio services, including commercial wireless, public safety communications, and 9-1-1 calls. Three possible wireless technology solutions were identified in the NOI that commenters further expounded upon: jamming, managed access, and detection. NTIA's observations on each of these technologies are as follows.

A **jamming** device transmits on the same radio frequencies as the cell phone, disrupts the communication link between the phone and the cell phone base station, and essentially renders the hand-held device unusable until such time as the jamming stops. A cell phone jammer has the potential to cause interference outside of the prison or to adjacent bands unless properly designed. Jamming interferes with 9-1-1 and authorized calls and violates the Communications Act of 1934 when performed by non-Federal officials. Implementation costs vary with the complexity of the prison site.

Managed access systems intercept calls in order to prevent inmates from accessing carrier networks. The cell signal is not blocked by a jamming signal, but rather, is captured (or re-routed) and prevented from reaching other network base stations, thereby preventing the completion of the call. Managed access systems have the potential to cause interference outside of the prison or to adjacent bands unless properly designed. However, such systems do permit 9-1-1 and known authorized calls. They require FCC approval and carrier consent for deployment. Costs can vary based on the complexity of the prison site.

Detection is the process of locating, tracking, and identifying various sources of radio transmissions – in this case, cell phone signals from prisons. Detection systems are passive in that they do not transmit, and therefore do not cause interference. Such systems protect 9-1-1 and authorized calls and, unless they are used for data gathering for law enforcement intelligence, raise no regulatory or legal issues.

Commenters on the NOI identified the following additional possible wireless technology solutions: standardized protocols, hybrid systems, and Non-Linear Junction Detectors (NLJDs). Standardized protocols rely on "sets of instructions" communicating with the hand-held device by essentially locking the device and making it unusable. This suggested solution is predicated on the adoption and implementation of standardized protocols (by the wireless industry) embedded in the firmware of mobile devices. Hybrid systems use a combination of both managed access and detection techniques to locate and control contraband cell phone use. Hybrid systems do not cause interference if using detection-only; however, for managed access, the potential exists to cause interference outside prison or to adjacent bands unless properly designed. Hybrid systems permit 9-1-1 and authorized calls but require FCC approval and carrier consent. Costs could vary based upon the complexity of the prison site. NLJDs are hand-held devices that require staff to physically search a prisoner's cell for the contraband phone. They present no regulatory or legal issues and do not interfere with other authorized users.

Each of the technologies identified has trade-offs and its own set of advantages and disadvantages. Some of the approaches come with legal hurdles or limitations. Furthermore, each prison's own unique characteristics (e.g., size and configuration of the prison), environment (rural versus urban setting), resources (e.g., financial and staff), and requirements (e.g., need for law enforcement intelligence) will help determine which approach is the most practical, feasible, and economical to implement.

SECTION 1
INTRODUCTION

OVERVIEW

The mobile phone industry has experienced significant growth since the inception of the analog wireless cell phone network in the early 1980s.[1] The 1990s saw the development of digital networks, and thereafter, high-speed data networks became available to consumers. The growth of the mobile phone industry has been fueled, in part, by consumer demand for instant access to communication services anywhere and anytime. Features such as data, image, and video communications have also contributed to the overwhelming demand for mobile services and applications. Mobile devices have become a critical component of our information society, contributing to public knowledge, commerce, and public safety.

Just as consumer demands for mobile devices have risen rapidly, the use of cell phones by prison inmates has grown as the U.S. prison population continues to expand.[2] This use is considered contraband by prison officials. The number of cell phones confiscated by prison officials has dramatically increased in only a few years. For example, during 2006, California correctional officers seized approximately 261 cell phones in the State's prisons and camps; by 2008, that number increased ten-fold to 2,811.[3] Similarly, in 2009, Maryland prison officials confiscated nearly 1,700 phones, up from approximately 1,200 phones the year before.[4] NTIA did not investigate the causes of increased confiscation of contraband cell phones. This increase in unauthorized cell phone use by inmates is a mounting concern among correctional administrators across the country.[5]

---

[1] For the purpose of this report, the use of the word "cell phone" refers to any wireless, portable device that is available to the public on a subscription or prepaid basis for delivering voice and/or data services such as text messages. It includes, for example, phones operating within the Cellular Radio Service in the 800 MHz bands; broadband Personal Communications Services (PCS) in the 1.9 GHz bands; the Advanced Wireless Services (AWS) in the 1.7 GHz band; Specialized Mobile Radio (SMR) services in the 800 and 900 MHz bands; and any future mobile wireless devices that plan to operate in bands such as the 700 MHz band.

[2] At the end of 2008, Federal and State correctional authorities had jurisdiction over roughly 1.6 million prisoners, of which over 200,000 (about 13 percent) were housed in Federal facilities. The Federal and State prison population rose by approximately 1 percent from year-end 2007 to 2008. *See* Sabol, William J., Heather C. West, and Matthew Cooper, "Prisoners in 2008," *Bureau of Justice Statistics Bulletin*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Dec. 2009, page 16, available at http://bjs.ojp.usdoj.gov/content/pub/pdf/p08.pdf.

[3] Special Report, *Inmate Cell Phone Use Endangers Prison and Public Safety*, Office of the Inspector General, State of California, May 2009, available at http://www.oig.ca.gov/media/reports/BCI/Special%20Report%20of%20Inmate%20Cell%20Phone%20Use.pdf.

[4] State of Maryland Fact Sheet, *Keeping Communities Safe*, Maryland Department of Public Safety and Correctional Services, Feb. 2010.

[5] *See* Department of Justice, Office of Justice Programs, National Institute of Justice, *Cell Phones Behind Bars*, Dec. 2009, available at http://www.ncjrs.gov/pdffiles1/nij/227539.pdf; Washington Examiner, *Drug Dealer Who Planned Murder Gets Life Sentence*, Scott McCabe, May 4, 2009, available at http://www.washingtonexaminer.com/local/crime/Drug-dealer-who-planned-murder-gets-life-sentence-44327767.html; *Wired Magazine*, "Prisoners Run Gangs, Plan Escapes, and Even Order Hits With Smuggled Cellphones", Vince Beiser, May 22, 2009, available at http://www.wired.com/politics/law/magazine/17-

In December 2009, Congress directed the National Telecommunications and Information Administration (NTIA), in coordination with the Federal Communications Commission (FCC), Federal Bureau of Prisons (BOP), and the National Institute of Justice (NIJ), to develop a plan to investigate and evaluate how wireless jamming, detection, and other technologies might be utilized for law enforcement and corrections applications in Federal and State prison facilities.[6] In response to Congress, this report presents the results from NTIA's plan—coordinated with other agencies—for the investigation and evaluation of those technologies.

ABOUT THIS REPORT

This report is the outcome of an overall plan to investigate and evaluate wireless technologies to prevent contraband cell phone use in prisons. NTIA has taken a number of actions and steps on issues that deal with contraband cell phone use.

NTIA's Institute for Telecommunication Sciences (ITS) performed laboratory measurements on a jamming system at its laboratory in Boulder, Colorado in 2009. Further, ITS performed field measurements on the same jamming system at a Federal Corrections Facility in Cumberland, Maryland in 2010. Subsequently, NTIA performed a technical analysis based on these measurements. The results and findings from these efforts are discussed in Section 2 and in separate NTIA reports.[7]

Also in 2010, NTIA formed an interagency working group with the FCC, BOP, and NIJ to coordinate the activities of this effort as required by Congress, and to become cognizant of other Federal agency efforts concerning contraband cell phones.

Further, NTIA, in coordination with the FCC, BOP, and NIJ, issued a comprehensive Notice of Inquiry (NOI – see Appendix A) on May 12, 2010 to seek public input in order to assist NTIA with its investigation and evaluation of technologies to prevent the use of contraband cell phones in Federal and State facilities. NTIA received forty-six comments (see Appendix B) from a variety of interested and concerned parties categorized as follows:

06/ff_prisonphones. Contraband cell phone use has been noted to be a problem in Federal prison facilities as well. *See* Testimony of Harley J. Lappin, Director, U.S. Bureau of Prisons before the U.S. Congress, Hearing on the Fiscal Year 2009 Budget Request for the Bureau of Prisons, the U.S. Marshal Service, and the Office of the Federal Detention Trustee, available at http://www.november.org/stayinfo/breaking08/LappinTestimony.html.

[6] H.R. Conf. Rep. No. 111-366 (2009), Division B, Title 1, Page 619, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_reports&docid=f:hr366.111.pdf.

[7] Sanders, Frank, H., Johnk, Robert, T., McFarland, Mark, A., Hoffman, Randall, J., *Emission Measurements for a Cellular and PCS Signal-Jamming Transmitter*, NTIA Institute for Telecommunication Sciences, NTIA Report TR-10-465, February 2010, available at http://www.its.bldrdoc.gov/pub/ntia-rpt/10-465/10-465.pdf (hereinafter TR-10-465); NTIA Report TR-10-466, Emission Measurements of a Cellular and PCS Jammer at a Prison Facility, May 2010, available at http://www.ntia.doc.gov/osmhome/contrabandcellphones/NTIAPrisoncelljammerreport_TR_10_466.pdf (hereinafter TR-10-466); NTIA Technical Memorandum 10-468, Initial Assessment of the Potential Impact From a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers, May 2010, available at http://www.ntia.doc.gov/osmhome/contrabandcellphones/NTIATechnicalMemorandum_10_468.pdf (hereinafter TM-10-468).

- manufacturers, vendors and consultants (representing 41% of comments filed);
- public safety, government, and correctional officials (representing 33% of comments filed);
- wireless service providers and associations (11%); and
- others (15%).

These comments, including information from various manufacturers of these technologies (see Appendix C) and NTIA's efforts on contraband cell phone use, are available at http://www.ntia.doc.gov/osmhome/contrabandcellphones/index.html.

This report first details Federal agency activities to investigate and evaluate methods to prevent contraband cell phone use, and then describes the various wireless intervention technologies.

SECTION 2
FEDERAL EFFORTS

The Administration supports the goal of combating contraband cell phone use while protecting critical Federal Government and public safety operations.[8] Given that a number of Federal agencies have a vested interest in preventing contraband cell phone use in prisons, Congress directed NTIA to coordinate the development of this evaluation with the FCC, BOP, and NIJ. Along with NTIA, these agencies have been dealing with issues relative to contraband cell phone use, some for a number of years. Each of the agencies provided their respective input for inclusion into the report, based on their efforts, experiences, insights, and evaluations.

NTIA

Laboratory Measurements

In December 2009, in response to the growing concern over contraband cell phone use and the interest at that time in jamming as a solution, NTIA's ITS measured, at its laboratory in Boulder, Colorado, the radiated emission levels for a jammer designed to deny service for communications devices operating in the 869-894 MHz Cellular Radiotelephone Service ("Cellular") and 1930-1990 MHz Personal Communications Service (PCS) frequency bands.[9] Laboratory measurements were performed for the purpose of obtaining a set of peak-detected and root mean square (RMS, or average) emission spectrum data, in the form of effective isotropic radiated power (EIRP), of a jammer transmitter that can be used to characterize the jammer's radiated emissions. The jammer used in the measurements operated at a power level of up to 100 watts in each band, repetitively sweeping a carrier-wave signal across the range of frequencies in which service was to be denied. ITS performed frequency domain emission measurements from 100 MHz to 6 GHz with 100 dB of dynamic range. With the installation of a diplexer on the jamming transmitter output – acting as a radio frequency (RF) filter – some measurable out-of-band (OOB) emissions occurred in spectrum adjacent to the fundamental frequency bands. Across the rest of the 100 MHz to 6 GHz spectrum range, unwanted emission levels were suppressed by 100 dB or more with the diplexer installed. OOB emissions in adjacent bands may be reduced by sweeping across less than the full width of the targeted bands at a cost of jamming effectiveness, or by installing custom-designed RF output filtering.[10]

[8] Letter from Cameron Kerry, U.S. Department of Commerce General Counsel, to John D. Rockefeller, IV, Chairman, Senate Committee on Commerce, Science and Transportation (Oct. 2, 2009), available at http://www.ogc.doc.gov/ogc/legreg/letters/111/S251Oct209.pdf. *See also* Letter from Gary Locke, Secretary of the U.S. Department of Commerce, to Martin O'Malley, Governor of Maryland (Oct. 21, 2009).
[9] TR-10-465.
[10] *Id*. at xiii.

Field Measurements

As a follow-on effort to the above laboratory measurements, ITS performed in February 2010 field measurements of limited deployment of a device similar to that tested at the ITS Lab in Boulder, Colorado at a Federal Correctional Institution in Cumberland, Maryland.[11] The purpose of these field measurements was to perform emission spectrum measurements on jammer signals inside and outside a jamming zone at the BOP facility with multiple measurement bandwidths and detectors, both in-band and in selected Federal land mobile radio (LMR) and Global Positioning System (GPS) spectrum bands. Measurements at each location were performed with the jammer "on" versus "off" so as to show the relative power levels of the jamming signal and the ambient Cellular and PCS signals at each location. ITS measured in-band jammer emissions outside the targeted zone at distances of up to 127 meters from the edge of the targeted zone. The device, deployed strictly for test purposes, produced measureable signal levels in the 869-894 MHz Cellular and 1930-1990 MHz PCS radio bands. It also produced measureable levels in the bands used for GPS and bands used for Federal public safety and law enforcement operations such as may be used in and around a Federal prison. However, use of the diplexer suppressed the levels outside the cellular and PCS bands by 100 dB or more, making the installed device unlikely to interfere with Federal operations. The report also noted a significant number of variables with each jammer implementation. Some of these variables pertained to the jamming technology and some pertained to the prison facility.

Technical Analysis

In May 2010, NTIA published a technical memorandum to examine issues related to the potential interference impact of a specific cellular and PCS jammer transmitter on selected out-of-band and in-band receivers.[12] The report is based on the measurements taken by ITS at the Cumberland, Maryland facility. When operating at full power and jamming in the cellular and PCS bands, the tested jammer transmitter could cause some impact to LMR receivers at the prison and to GPS receiver use in and around the facility. However, the use of a diplexer decreased the potential interference and reduced the required distance separations to such low values as to be negligible. Therefore, the specific jammer tested could be implemented with the diplexer or another appropriate filter without risk to Federal operations. However, because of the limited deployment of the jammer transmitter at the Federal facility, NTIA could not draw any conclusions from the field measurements about the potential of aggregate interference to out-of-band receivers if multiple jammer transmitters of this same type were operated throughout the facility. Further, the results of this study are unique to the location where the jammer was tested. Each prison differs in size, shape and structure and the limited conclusions cannot be applied across the board.

Interference protection criteria (IPC) values for cellular and PCS handsets are required to assess potential interference to in-band receivers (e.g., establish distance from a facility where communication is not disrupted). The field measurements only examined one type of jammer transmitter, thus the results of the measurements and analysis cannot be broadly applied to all jammer transmitters. For example, the measurements did not examine the in-band emission

[11] TR-10-466.
[12] TM-10-468.

levels outside targeted jamming areas that would result from jamming inside different building structures or jamming inside larger building interiors. Due to the limited deployment of the jammer transmitter at the Federal facility, NTIA could not draw conclusions from the field measurements assessing the potential of aggregate interference to in-band receivers if multiple jammer transmitters were operated throughout the facility. That is, NTIA could not determine the effects of the jammer on cellular and PCS devices outside the prison facility.

FEDERAL COMMUNICATIONS COMMISSION (FCC)

The FCC has assisted with regulatory approvals (e.g., special temporary authorizations, applications to lease spectrum from carriers to managed access providers, etc.) related to testing and deployments of non-jamming cell phone detection and signal-control technologies. These initiatives have included tests conducted by the Maryland Department of Public Safety and Correctional Services in 2009 at a decommissioned facility in Jessup, Maryland, and a subsequent study of non-jamming technologies in three commissioned correctional facilities. Two vendors, AirPatrol of Columbia, Maryland, and Digital Receiving Technology of Germantown, Maryland, deployed passive technology that they indicate detects cell phone use, collects data from active cell phones and does not interfere with Cellular and PCS frequencies. A third vendor, Tecore of Columbia, Maryland, deployed its managed access system, which required and received prior FCC approval for its operation.[13] FCC staff has also assisted the State of Mississippi's decision to deploy Tecore's managed access system throughout its State prisons, beginning with the Mississippi State Penitentiary, a maximum security prison in Parchman, Mississippi. In July 2010, the FCC's Wireless Telecommunications Bureau issued a letter to Tecore clarifying various legal issues/concerns raised by carriers regarding the proposed Parchman deployment.[14] FCC staff has also assisted Tecore and the affected wireless carriers in Mississippi with required regulatory filings and initially issued temporary authorizations permitting the deployment of Tecore's managed access systems at the Parchman facility, and have now granted Tecore/carrier applications for permanent authority. FCC staff is also working to develop a streamlined regulatory process for similar future applications involving managed access technology.

In addition to these regulatory actions, the FCC assists prison authorities in identifying and evaluating available technologies to defeat contraband cell phone use in prisons. To this end, FCC staff has regularly interacted with State corrections officials from across the country, organizations including the American Correctional Association (ACA) and the Association of State Correctional Administrators (ASCA); vendors; wireless providers; and Federal agency partners including the NIJ, NTIA, and BOP.

[13] The FCC conditioned Tecore's temporary authorizations such that the operation could not commence without the consent of the local carriers. The FCC granted Tecore two temporary experimental authorizations to demonstrate and test its equipment in the Maryland Correctional Institution in Jessup, Maryland.

[14] Specifically, the letter addressed issues related to the application of Sections 201, 202, and 333 of the Communications Act of 1934, as amended, to Tecore's proposed system.

On September 30, 2010, the FCC held a public workshop/webinar to discuss contraband cell phones in prisons.[15] The workshop/webinar was conducted in partnership with NIJ and the ASCA. This workshop/webinar discussed technologies currently available to combat contraband cell phone use in prisons, as well as the need to address statutory barriers and policy concerns relating to cell jamming and other interfering technologies. In addition, discussion focused on ensuring that available technologies are operated in accordance with the law without jeopardizing public safety or the lawful use of cell phones by the public, including calls to 9-1-1. The session also addressed possible solutions, including previous tests and pilots, and a recently-deployed managed access system in Mississippi.

FEDERAL BUREAU OF PRISONS (BOP)

Over the past 15 years, the BOP has evaluated a large number of cell phone interdiction technologies. The BOP has set four basic requirements in the context of these evaluations:

1. The equipment must work without impacting or collecting information from the general public located outside the secure perimeter;
2. The solution should have no legal restrictions;
3. The equipment must work with all cellular phone protocols; and
4. The overall cost of equipment and installation must be reasonable.

BOP, in its quest for a solution, continues to investigate a wide variety of technical solutions.[16] These options include jamming, spoofing, denial of service, managed access, direction-finding, scanners, hand-held frequency detectors, voice recognition, non-linear junction detectors, picocells and femtocells.

Based on BOP's observations of product demonstrations and vendor outreach, review of technical specifications, and/or actual testing in BOP facilities, BOP has found that each of the solutions has one or more shortcomings, such as: (1) equipment is not covert; inmates see staff coming with portable sensors and shut off the phones; (2) many systems do not detect all cell phone frequencies and protocols or those which are designed for the European market with a single protocol; (3) very short detection distance; (4) direction-finding systems are ineffective and confused due to the large amount of metal (doors, rebar, etc.) in the hardened construction of prisons reflecting multiple-path RF signals; (5) systems are too sophisticated and/or expensive for daily operations by non-technical staff; (6) some systems detect or interfere with cell phones outside the secure perimeter of a prison, such as on a public street or visitor parking lot; (7) many systems designed for the military and law enforcement have a wide variety of expensive features that go beyond most of the requirements of the correctional community and/or require legal authority to operate (these include voice monitoring and collecting cell phone identifying information); and (8) many systems are impractical to implement with prison compounds that have large acreage and dozens of buildings.

---

[15] *Public Safety and Homeland Security Bureau to Hold Workshop/Webinar on Contraband Cell Phone Use in Prisons*, Public Notice (Sept. 13, 2010), available at http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0913/DOC-301424A1.pdf

[16] The BOP continues to work with other Federal, State and local agencies on the problem of inmates with cell phones, including via a close working relationship with NIJ. Along with NIJ and a variety of State departments of corrections, BOP will continue to exchange information and participate on numerous technical committees working toward solutions.

To date, only cell phone detection systems have been able to meet BOP's requirements. At one high-security facility, BOP is evaluating sophisticated fixed sensors that detect RF signals emitted from unauthorized cell phones. The evaluation has shown this technology to be effective, but costly (more than $200,000 per site), in order to achieve a high level of detection accuracy. In an effort to reduce the cost, BOP plans to evaluate an RF detection system with fewer sensors, thereby sacrificing system accuracy for cost.

NATIONAL INSTITUTE OF JUSTICE (NIJ)

The NIJ has been actively engaged in the issue of contraband cell phone use in prisons for a number of years. It has examined a number of potential approaches to dealing with this issue. Most recently, it funded the development of an electronic surveillance system to detect the presence of cell phones within a known structure, for example a prison, and pin-point the location of the cell phone to within a one to two prison-cell area. The design and execution of the initial testing of this device was conducted on April 4, 2010 within the Virginia Department of Corrections. Concurrently, NIJ is funding significant research in developing improved means to collect digital forensic evidence from cell phones and other mobile devices.

In July 2010, NIJ convened a Conference Plenary Panel: Cell Phones in Prisons as part of its annual conference. As a result of that panel and the public interest surrounding this issue, NIJ established a Federal agency working group including all relevant Federal agencies (BOP, FCC, and NTIA). The group is expected to expand internal NIJ conversations; enhance cross-agency collaboration; and further discussion of next steps.

In addition, NIJ has been working with the FCC, ASCA, and practitioner networks to further explore and understand this issue. Most recently, NIJ co-sponsored a contraband cell phone webinar with the FCC, which drew nearly 700 participants and included Federal, State and practitioner panelists. Initial investigation by NIJ in this area suggests that technology is only one of a number of options to be considered when attempting to limit illegal cell phone use in prisons and jails. Just as important is a review and possible revisions of existing institutional policies, procedures, training, and enforcement efforts.

SECTION 3
JAMMING

OVERVIEW

Radio jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of disrupting use of electronic devices, equipment, or systems – in this case, mobile devices such as cell phones. A cell phone works by communicating with its service network through a cell tower or base station. These cell towers divide an area of coverage into cells, which range in size from a few city blocks to hundreds of square miles. The base station links callers into the local public switched telephone network, another wireless network, or even the Internet.

A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication link between the phone and the cell phone base station, essentially rendering the hand-held device unusable until such time as the jamming stops. The jamming device may vary its signal over an entire band used for cell phone operations, disrupting, on any particular channel, the connection between the base station and handset for a short period of time. The jammer cycles through its range of channels rapidly and frequently enough to prevent functioning connections over all the range of its capability. Jamming devices do not discriminate among cell phones within range of the jamming signal – both contraband and legitimate cell phones are disabled. Currently, the operation by non-Federal entities of transmitters designed to jam or block wireless communications violates the Communications Act of 1934, as amended.[17]

SUMMARY OF COMMENTS

Many NOI commenters oppose the use of jammers to block cell phone signals. In particular, the wireless industry suggests the use of technologies other than jammers.[18] Verizon Wireless provides three primary points on jamming: (1) small scale jamming can create a significant threat of interference; (2) jamming becomes more complex when multiple frequency bands are involved: and (3) managed access is the best way to stop contraband cell phone use.[19] Similarly, the public safety community, such as the National Emergency Number Association (NENA) and the Association of Public Safety Communications Officials (APCO) cite concerns over the effects that jammers could have on critical public safety communications and 9-1-1 calls.[20] Zocalo Data Systems believes that jamming would be too problematic a solution to deploy.[21]

---

[17] 47 U.S.C. § 301, 302a, 333. The FCC had reiterated this fact. See *Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States*, Public Notice, DA-05-1776, June 27, 2005, available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-1776A1.pdf.

[18] *See, e.g.*, CTIA comments at 9-17; T-Mobile USA comments at 7-9; Verizon Wireless comments at 9-11; AT&T comments at 10-13.

[19] Verizon Wireless comments at 4.

[20] *See generally* NENA comments; APCO comments; Rappahannock Regional Jail comments.

[21] Zocalo Data Systems comments at 1.

However, one respondent, without further explanation or elaboration, suggests buying "a cell phone jammer to block the transmission."[22] Kentucky Correctional Industries suggests an interference device could be installed that would render cell phones useless.[23] Additionally, a number of correctional departments, citing NTIA's testing of jammers, express support for the use of cell phone jammers in prisons.[24]

Devices and Frequency Bands

In the NOI, NTIA asked a number of questions regarding whether the various technologies could transverse multiple frequency bands. CellAntenna states that jamming is the only technology that can prevent the use of any and all frequencies/protocols and that blocking the cellular communications would solve 90-95% of illegal use in prisons.[25] ITT notes that jamming would be able to cover newer bands such as the 700 MHz band, but will require new transmitters, new hardware and software to be scalable.[26] Similarly, ShawnTech states that jamming can stop all calls on cellular devices with all technologies available.[27]

The wireless providers also respond on this issue. Sprint Nextel submits that "today's jamming systems lack the capability to block all of the frequency bands that prisoners could use…"[28] As Verizon Wireless notes, jammers will not work to block all of the wireless signals in the vicinity of the prisons, citing the fact that some smart phones switch to Wi-Fi when commercial signals are not available.[29] Additionally, T-Mobile USA asserts that jammers installed at prisons will not sufficiently block all forms of communications.[30]

Interference to Other Radio Services

Many of the commenters, particularly the wireless industry, express concern over the potential for interference from jammers to other radio services near prisons.[31] Furthermore, many of the respondents specifically mention interference to the critical public safety radio service operating

---

[22] Paul Velasquez comments at 1.
[23] Kentucky Correctional Industries comments at 1.
[24] South Carolina Department of Corrections comments at 2; State of Maryland/Department of Public Safety and Corrections comments at 2; California Department of Corrections and Rehabilitation comments at 2. Several groups have filed with the FCC petitions for waivers to permit the use of cell phone jammers in prisons. Stating that it did not have the authority to permit such jamming, the FCC has denied the petitions. *See, e.g.*, Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Devon Brown, Director, District of Columbia Department of Corrections, DA 09-354, Feb. 18, 2009, available at http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-09-354A1.pdf; Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Howard Melamed, CEO, CellAntenna Corporation, DA 09-622, March 17, 2009, available at http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-09-622A1.pdf.
[25] CellAntenna comments at 3-4.
[26] ITT comments at 8.
[27] ShawnTech comments (slides) at 23.
[28] Sprint Nextel comments at 2.
[29] Verizon Wireless comments at 6-7.
[30] T-Mobile USA comments at 6.
[31] *See, e.g.*, AT&T comments at 7-9; Verizon Wireless comments at 5-8; T-Mobile USA comments at 2-5; Sprint Nextel comments at 2; CTIA comments at 18-25.

within or adjacent to jammers.[32] Motorola notes that the deployment of jammers could cause intermodulation effect in public safety receivers with "devastating effects."[33]

However, South Carolina argues that surgical jamming does not cause interference to public safety radios, and calls/frequencies, including calls to 9-1-1, are not blocked outside of the prison perimeter.[34] Maryland, citing the results from the NTIA test demonstration at the Federal Correctional Facility, submits that jamming can work without interference or compromising public safety.[35] Similarly, California cites the results of the NTIA tests as a reason why jammers should be tested and approved in other jurisdiction such as in California.[36]

Protecting 9-1-1 and Authorized Calls

Many respondents express concern over the effects that jammers could have on critical communications such as 9-1-1, public safety and everyday cellular communications.[37] NENA has concerns about the possibility of wireless jammers blocking 9-1-1 calls.[38] APCO concurs that jammers could block calls to 9-1-1 to report an emergency.[39] Jamming of signals could potentially interfere with other authorized cell phone frequencies used by laptop computers for broadband access, security and alarm systems.[40] But CellAntenna states that if the system is properly engineered and the signal levels of the jamming units are much lower than any outside the prison, 911 calls by the public are not affected.[41]

The wireless carriers express concern about the interference that jammers could cause to in-band cell phones, based upon the NTIA tests at the Cumberland, Maryland facility. In its comments, Sprint Nextel contends that after analyzing data gathered at one of its cell sites, interference may have occurred to cell phones attempting to communicate with that cell site.[42] Sprint Nextel notes that this cell site provides coverage to the area immediately north of the jamming zone.[43] Additionally, Sprint Nextel states that during the test period, there was a "definite trend upward in the rate of dropped calls and a trend downward in successful call attempts."[44] Verizon Wireless concludes that "signal measurements from the NTIA jamming tests taken at the furthest distance outside the prison from the jammer location are strong enough to cause harmful

[32] *See, e.g.*, NENA comments; APCO comments; Motorola comments.
[33] Motorola comments at 3.
[34] South Carolina Department of Corrections comments at 2.
[35] State of Maryland/Department of Public Safety and Corrections comments at 2. However, the technical analysis on the field measurements taken by NTIA at the Cumberland facility do not support drawing any conclusions about either the potential of aggregate interference to out-of-band or in-band receivers if multiple jamming transmitters of this same type were operated throughout the facility. *See Supra* note 12.
[36] California Department of Corrections and Rehabilitation comments at 2.
[37] For example, Rappahannock Regional Jail states that by jamming the "800 MHz and 1900 MHz frequency ranges you will affect most if not all cell phones (especially Nextel phones) and some PCS EMS Public Safety portable radio systems used inside of the jails and prisons today." Rappahannock Regional Jail comments at 1.
[38] NENA comments at 3.
[39] APCO comments at 2.
[40] Paul Kruger comments at 1.
[41] CellAntenna comments at 5.
[42] Sprint Nextel comments at 3-6.
[43] *Id.*
[44] *Id.*

interference to commercial mobile subscriber devices."[45] Other carriers note their concerns over the results of the NTIA testing and the potential for interference.[46]

Cost Considerations

The affordability of technologies to prevent contraband cell phone use in prisons is a concern among the commenters.[47] CellAntenna states that jammers provide the best and most economical way to prevent cell phone use in prisons, require very little staff time, and that the cost of the system depends on a number of factors such as the size and shape of prison, the area to be covered, and incoming tower signal levels.[48] However, Enterprise Electronics states that because jammers need certification, type acceptance/approval, this process will increase the costs of the product, thereby making it potentially cost-prohibitive to deploy.[49] ITT notes that the biggest costs associated with jamming systems are infrastructure costs (number of antenna, cable type) and these costs can vary according to building codes and local laws and compliance.[50] Further, ITT states that for a particular scenario, a jamming system could cost two to three times more than a detection system.[51]

Locating Contraband Cell Phones

As the NOI points out, RF jamming equipment cannot locate the source of the contraband call. CellAntenna affirms that this is the case, noting that there is really no need to locate the phone and spend time doing so.[52] Other commenters note that jamming does not have the capability to locate the phone.[53]

Regulatory/Legal Issues

The Communications Act of 1934 prohibits non-Federal entities from intentionally interfering with radio signals.[54] Many of the respondents reaffirm this as well. For example, the wireless industry expresses their concerns over deploying a device that violates the Communications Act of 1934.[55] Manufacturers, vendors and industry also note the problems of using cell phone jammers.[56] One respondent suggests adopting strict rules to address the issue of contraband cell phones with jamming where it can be done safely.[57]

---

[45] Verizon Wireless comments at 5.
[46] T-Mobile USA comments at 5; AT&T comments at 9.
[47] *See, e.g.*, ICSolutions comments at 4; Big Spring Correctional Center comments at 1.
[48] CellAntenna comments at 5.
[49] Enterprise Electronics comments at 2.
[50] ITT comments at 14-15.
[51] *Id.*
[52] CellAntenna comments at 6.
[53] *See, e.g.*, Enterprise Electronics comments at 2; Berkeley Varitronics Systems comments at 2.
[54] 47 U.S.C. § 333.
[55] *See, e.g.*, CTIA comments at 6-9; Sprint Nextel comments at 2; T-Mobile USA comments at 10-12; AT&T comments at 4-7.
[56] *See, e.g.*, Enterprise Electronics comments at 2; Tecore comments at 15-17; ShawnTech comment (slides) at 24.
[57] Marcus Spectrum Solutions comments at 4.

In October 2009, the United States Senate passed a bill, the Safe Prisons Act of 2009, that would amend the Communications Act of 1934 to authorize the FCC to permit the supervisory authority of a correctional facility to operate a jamming system within the facility to prevent, jam, or otherwise interfere with unauthorized wireless communications by individuals held in the facility.[58] The House of Representatives has not taken up similar legislation. A number of respondents indicate support for the proposed legislation.[59]

Still other respondents question the applicability of the Communications Act of 1934 as it relates to the use of jammers by prisons. CellAntenna explains:

> The 1934 Communications act deals only with legal communications. The act specifically states that local and state governments cannot interfere with Licensed and Authorized communications. The fact is that the cell phone is illegal to use in prisons. It is therefore not licensed or authorized and can be stopped.[60]

Further, Global Tel*Link (GTL) questions whether Section 333 of the Communication Act of 1934 is applicable in a prison setting.[61] Additionally, Marcus Spectrum Solutions, while recognizing that jamming of cellular communications by non-Federal entities is illegal, states that this is the case only because the FCC has "never adopted rules authorizing such jamming."[62]

Technical Issues

In the NOI, NTIA asked if there are any technical issues to be considered for the various technologies. CellAntenna states that there are a number of technical factors that can be used to ensure that the signal levels of the jammer are substantially less than those transmitted by the carrier cell towers that cover the prison, including: (1) deployment in each prison must be designed separately because antennas, power levels, and jamming protocols can be a determining factor; (2) quality of amplifiers; (3) refining jamming to be more dynamic by adjusting power levels based upon incoming signals; (4) vigilant monitoring to reduce communication disruption outside of the prison; and (5) coordination with cellular carriers on signal levels to adjust jamming signals.[63]

Bahia 21 states that, although pure jamming alone disrupts cellular communications without differentiating the source of the call, it has developed "location selective jamming." It notes that this system is reactive, radiating only when an attempt to communicate is detected in an unauthorized location, thus limiting the impact on the network.[64] It indicates that the advantages

---

[58] S. 251, Safe Prisons Communications Act of 2009, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s251es.txt.pdf.

[59] *See, e.g.*, State of Maryland/Department of Public Safety and Corrections comments at 2; Oklahoma Department of Corrections comments at 1; California Department of Corrections and Rehabilitation comments at 2.

[60] CellAntenna comments at 6.

[61] GTL comments at 4.

[62] Marcus Spectrum Solutions comments at 1.

[63] CellAntenna comments at 4.

[64] Bahia 21 comments at 1.

of this approach include: no interference to cell phones outside of the prison perimeter, access to 9-1-1 is unaffected, very low radiated power is required to jam small or large prisons, and selective jamming can be tailored to the denial service area.[65]

In comments to the NOI, ITT states that jamming systems are effective against: voice, text and data; short-burst transmissions (because jamming is constant); and new modulation formats such as in the 700 MHz band.[66]

OBSERVATIONS

The following key observations highlight the use of jamming as a possible solution to mitigate contraband cell phone use by inmates:

- Any transmitter has the potential to cause interference to other radio services.[67] Jammers are transmitters that are specifically designed to disrupt cellular and other mobile radios. To prevent over-jamming, proper RF site engineering and extensive testing at each prison is essential to reduce interference to other radio services. This is likely to increase the cost of deployment, perhaps substantially.
- As required by FCC Rules, all mobile phones operating on commercial mobile radio spectrum must be able to call 9-1-1 for assistance during emergencies.[68] Cell phone jammers cannot differentiate between contraband cell phone calls and authorized calls, including 9-1-1 calls.
- The use of jammers by State or local prison officials is a violation of the Communications Act of 1934, and hence illegal. The FCC has denied previous requests to operate cell phone jammers at State correctional facilities. A bill passed by the U.S. Senate would allow State and local prison officials to petition the FCC to allow jamming at prisons on a case-by-case basis. This bill, however, is not law.
- NTIA sought comment through the NOI on an appropriate Interference Protection Criteria (IPC) value for mobile phones. No commenters recommended any values.[69] If the law is changed, the mobile phone industry may need to come to agreement on an acceptable value to enable in-band interference effects to mobile devices to be evaluated.
- Incomplete areas of coverage in which prisoners have access to cell phones could lead to the prisoners identifying and exploiting dead-zones.
- Jamming that is limited to specific bands and technologies could lead to inmates selecting certain technologies and service providers as the "technology-of-choice."

---

[65] *Id.* at 2.
[66] ITT comments at 19.
[67] As examples, in India and Brazil, jamming prisons affected authorized cell phone users up to 5 km away. In Ireland, a jamming system interfered with cell phone users in a hospital, which was across the street from the prison. *See* "Technical Issues in Checking Contraband Cell Phone Use in Jails and Prisons," Terry Bittner, April 5, 2010, available at http://www.corrections.com/articles/24025-technical-issues-in-checking-contraband-cell-phone-use-in-jails-and-prisons. *See also* CTIA comments at 20-21.
[68] Under FCC Rules, the 9-1-1 requirements are only applicable to Commercial Mobile Radio Service providers. *See* 47 C.F.R. § 20.18.
[69] ITT suggests that an acceptable IPC would require analysis and characterization and be established by lab measurements. ITT comments at 10.

SECTION 4
MANAGED ACCESS

OVERVIEW

Managed access systems intercept calls in order to prevent inmates from accessing carrier networks. The cell signal is not blocked by a jamming signal, but rather, is captured (or re-routed) and prevented from reaching other base stations, thereby disallowing completion of the call. This technology permits calls by known users (i.e., prison-authorized cell phone numbers) by handing them off to the network, but prevents others by denying access to the network.[70]

Managed access systems include one or more base stations configured to cover the borders of the target area, as well as the technologies and frequency bands of the wireless provider networks. The footprint is optimized through the use of power control, directional antennas, and repeaters to limit the coverage of the base stations to the desired target areas. When a cell phone within the target area attempts to connect to the wireless provider network, it will be captured by the managed access network because its base stations serve the target area with relatively stronger signals than the nearest base stations of the wireless provider network. Therefore, the devices will connect first to the managed access network. Based on policies selectable by the system administrator, devices can be either locked to the managed access network and prevented from initiating or receiving communications, or cleared and redirected to the applicable commercial networks. The systems can also be used in a passive manner to simply detect cell phone use and collect data from active cell phones. While an unapproved device is locked to the managed access network, the display and appearance of the device will be the same as if it were connected to the commercial network. Once a device is captured by the managed access network, if the caller attempts to place a call, send a text message, connect to the Internet or otherwise access a wireless network, the attempt will fail. Once the device is located outside of the managed access system's target coverage area, it will re-register with the appropriate commercial network.

SUMMARY OF COMMENTS

A number of commenters, including the wireless carriers, mention the viability of using managed access technologies as a method of controlling contraband cell phone use.[71] GTL contends that managed access is the frontrunner for technology of choice from the wireless industry's point of

[70] In 2009, the Maryland Department of Public Safety and Correctional Services hosted a demonstration of various non-jamming technologies, including managed access systems. In January 2010, it issued a follow-on report. The demonstration showed, among other things, that: (1) several intelligence gathering abilities could be implemented depending upon specific laws governing each State; and (2) the types of technology tested could allow certain phones to operate and allow 9-1-1 calls to be processed. *See* Maryland Department of Public Safety and Correctional Services, *Overview of Cell Phone Demonstration*, available at http://www.dpscs.state.md.us/publicinfo/media/pdf/FinalReport_2008-09-10.pdf. One managed access technology (Tecore) was demonstrated and operated pursuant to an experimental license granted by the FCC for this occasion. *See also* Maryland Department of Public Safety and Correctional Services, *Non-Jamming Cell Phone Pilot Summary*, Jan. 20, 2010, available at http://www.dpscs.state.md.us/media/Cell-Phone-Pilot-Summary_Final.pdf.

[71] *See, e.g.*, Tecore comments at 2-5; AT&T comments 10-14; T-Mobile USA comments at 7-8.

view.[72] While not specifically mentioning managed access, several commenters suggest that methods of dropping calls or dead zones would be a solution.[73]

Device and Frequency Bands

Any solution to the contraband cell phone problem in prisons needs to address the growing number of telecommunications methods. This includes, for example, the Cellular, PCS, AWS, SMR, WiMAX, 700 MHz and General Mobile Radio bands. Additional methods of telecommunication include satellite, Wi-Fi, and Bluetooth mobile devices. Managed access solutions focus on the more common, licensed commercially available bands, but can be upgraded to cover Long Term Evolution (LTE) and the 700 MHz band.[74] Prohibiting access to the commercial cellular networks "would solve 90-95% of all illegal communications within a prison."[75] Verizon Wireless mentions that a managed access system can "prevent phones from switching to other bands and would not need to intercept as many spectrum bands within prisons."[76] Yet a managed access solution is "unlikely to operate with unlicensed solutions," leaving potential avenues for prison inmates to exploit.[77] Sprint Nextel recommends that "for a time period, it may be appropriate that managed access systems be supplemented with cell phone detection systems that cover a wide range of frequency bands." [78]

In its comments, AT&T expresses certainty that a managed access system can "evolve to support new frequencies and technologies."[79] It is possible with new technologies and available communication frequencies that a managed access system will need hardware and software upgrades. Any operator of a managed access system will also require prior notification from the local service providers when they update their own systems.[80] This is to be expected – and the process can be streamlined – as the managed access solution requires a high level of communication between the service provider(s) and system operators. The wireless industry commenters express their resolve to do so.[81]

Interference to Other Radio Services

An effective solution must not interfere with legitimate use of the radio spectrum. This includes use within and beyond the boundaries of a correctional facility, and particularly 9-1-1 calls and public safety communications. According to comments submitted by Berkeley Varitronics Systems (BVS), "[t]he only strategy which may be subject to this concern is jamming."[82] AT&T

---

[72] GTL comments at 5.
[73] *See, e.g.*, Rich Veach comments at 1; B.B. Sixty Rayburn Correctional Center comments at 1; Madison Juvenile Correctional Facility comments at 1; Dayton Correctional Institution comments at 1; Mike Kouri comments at 1.
[74] Tecore comments at 6.
[75] CellAntenna comments at 4.
[76] Verizon Wireless comments at 14.
[77] ITT comments at 7.
[78] Sprint Nextel comments at 2.
[79] AT&T comments at 11.
[80] Marcus Spectrum Solution comments (citing letter to FCC Chairman Genachowski from the South Carolina Department of Corrections, Oct. 21, 2009, at 3), available at http://www.ntia.doc.gov/comments/100504212-0212-01/attachments/09-30_10-21-2009_South_Carolina_Department_of_Corrections_7020142659-2.pdf .
[81] *See, e.g.*, CTIA comments at 9; AT&T comments at 19.
[82] BVS comments at 5.

points to Tecore's iNAC managed access solution as having a "great potential for addressing the problem . . . without jeopardizing public safety and commercial communications."[83] Of particular concern are Nextel/SMR devices, which operate in close proximity to public safety frequencies and use proprietary protocols. Verizon Wireless states that a managed access system "can intercept Nextel/SMR calls within prisons without interfering with public safety radios."[84] Sprint Nextel believes "that a properly configured managed access system that has been coordinated with the relevant commercial mobile operators would have little likelihood of causing interference to cell phone users outside the prison facility."[85]

Comments from T-Mobile USA reinforce the effectiveness of a managed access solution (compared to a jamming solution) in protecting public safety spectrum. T-Mobile USA states that a managed access system will "provide more precise control over the bands selected for disruption, thus preventing interference with public safety wireless communication …. unexpected interference to other services is reduced."[86]

Coordination with commercial service providers ensures that the managed access solution conforms to the boundaries of a correctional facility by matching power output levels. This prevents the system from adversely affecting legitimate radio frequencies outside of the prison, while commanding the spectrum within the prison. CTIA adds that, "[m]anaged access solutions can use location determination-technologies to ensure that the controls apply only in the geographic area of the prison."[87]

Wireless communication systems deployed by prison officials must not encounter interference. The managed access solution has a list of authorized and unauthorized phones enabling it to exclude authorized communication from its coverage by adding those devices to the list of authorized users.[88]

Protecting 9-1-1 and Authorized Calls

In a managed access system, 9-1-1 and authorized calls can connect to the cellular network.[89] NENA and APCO support non-jamming solutions to the problem because jammers cannot discern between legitimate, illegitimate, 9-1-1 and public safety communications.[90] The wireless providers – AT&T, Verizon Wireless, Sprint Nextel, and T-Mobile USA – all respond in favor of a managed access solution. This is due in large part to the system's ability to allow public safety, 9-1-1, and authorized calls to reach the cellular networks. Verizon Wireless states:

---

[83] AT&T comments at 2.
[84] Verizon Wireless comments (slides) at 14.
[85] Sprint Nextel comments at 1-2.
[86] T-Mobile USA comments at 8.
[87] CTIA comments at 10.
[88] ShawnTech comments (slides) at 25-28.
[89] Tecore comments at 11. *See also* CellAntenna comments at 5; ITT comments at 13. Enterprise Electronics raises the concern that inmates are not a reliable reporting source for 9-1-1 and, given the chance, will abuse the privilege and create harmful traffic for the 9-1-1 operators. Enterprise Electronics comments at 5.
[90] *See generally* NENA comments; APCO comments. Tecore notes in its comments that "certain jamming systems can detect the initiation of a 9-1-1 call, and can switch off the jamming transmission to allow such a call to connect to the commercial network. However, [d]uring that period, other devices including contraband cell phones may also have access to the commercial network." Tecore comments at Appendix B, n.10.

> Managed access can allow the system operator to maintain a list of approved callers – a list that can be amended constantly as subscribers that live, work, or frequently visit areas near the prison and are captured by the system are identified – whose calls will be allowed to [be] completed rather than blocked.[91]

Further, Verizon Wireless states that:

> Managed access systems allow prison officials, working with the system operator and nearby licensees, to set the parameters of how captured calls are handled. For example, prison officials can decide to allow the first call from a device not on the approved list to be completed, but block subsequent calls (in order to prevent blocking calls from random subscribers near the prison), can decide to limit the duration of calls from non-approved callers, or can deliver a message to non-approved callers letting them know their call is being blocked by the prison system and advising them to move away from the prison to try again.[92]

Cost Considerations

ShawnTech contends that a managed access system is costly (> $200K per site).[93] Marcus Spectrum Solutions believes that the "proponents [of managed access] have never addressed the full … cost implications."[94] According to Tecore Networks, a managed access provider, there are three primary cost factors: (1) the number of different commercial networks and utilized frequencies in the target area; (2) the geography/topology of the area; and (3) the range of functions the system will perform.[95] RF surveys of each facility are necessary to determine the proper hardware configuration. Post-installation RF surveys will confirm site coverage. Each facility will need to train staff to operate the system.

Commenters note that there are methods to reduce the costs associated with a managed access solution. If the managed access vendors are responsible for operating the system(s), it would reduce the cost of staff training.[96] Tecore asserts that "[t]he iNAC operating expenses can further be minimized if it is deployed centrally at a managed access facility."[97] ManTech's response supports Tecore's assertion, stating that, "centralizing control and data management, even when operations are site-specific, can minimize cost by networking, systematic planning, and systems operations."[98] The first managed access system deployed in the United States (by

[91] Verizon Wireless comments at 10.
[92] *Id*., n. 21.
[93] ShawnTech comments (slides) at 26.
[94] Marcus Spectrum Solutions comments at 3.
[95] Tecore comments at 11. A system is less expensive, for instance, without the additional location or data-mining technology.
[96] ITT comments at 15.
[97] Tecore comments at 12.
[98] ManTech comments at 16.

Tecore in Mississippi) was deployed at no cost to the prison authority, because Tecore entered into a separate arrangement with the pay phone service provider through its contract obligations with the agency for inmate telephone service.[99]

Locating Contraband Cell Phones

A basic managed access system does not locate contraband phones.[100] A managed access system equipped with data-mining technology could locate phones with a built-in GPS. However, a prisoner can turn off the GPS function on the phone, disabling that capability. There is also the potential for a managed access system to locate cell phones using RF triangulation.[101] As stated previously, a managed access system can work in conjunction with detection technologies.[102] Some respondents recommend this approach, at least in the short-term, until the managed access systems can capture all forms of wireless communication.[103] Others recommend utilizing detection technologies for aiding managed access operators in determining whether a call is legitimate (e.g., if the call originates from a cell block, the operator can add the number to the list of unauthorized callers).[104]

According to BVS, the forensic value within phones is in the subscriber identity module (SIM) card. Because managed access systems do not locate cell phones, BVS states that managed access systems do not provide information.[105] But a managed access solution can provide important data according to Tecore Networks:

> [t]he iNAC [managed access system] can provide the type and detail of information available from a commercial network operator. Information about device identity, activity record including numbers dialed and text messages sent, along with the capability for CALEA compliant interfacing to Law Enforcement Agencies.[106]

T-Mobile USA expounds upon additional information that a managed access solution can provide for prison and law enforcement intelligence purposes, stating that "[c]onsistent with local wiretap and surveillance laws, managed access systems may allow prison officials to observe who is using illicit phones in prisons, identify whom they are contacting or being contacted by, and perhaps even monitor the content of the communications."[107]

---

[99] Mississippi Department of Corrections, Office of Communications, Press Release, Operation Cellblock-Commissioner Epps Shuts Down Illegal Inmate Cell Phone Usage, Sept. 8, 2010, available at http://www.mdoc.state.ms.us/PressReleases/2010NewsReleases/Illegal%20Cell%20Phone%20Press%20Conference%20Release.pdf.

[100] *See, e.g.,* BVS comments at 2; Boeing comments at 3; ITT comments at 16.

[101] ITT comments 16.

[102] Boeing's comments to the NOI propose a piece of "hybrid" technology that is a combination of managed access and detection systems. Boeing comments at 3. This technology is described in Section Six: Other Technologies.

[103] Sprint Nextel comments at 2.

[104] *Id*.

[105] BVS comments at 3.

[106] Tecore comments at 12.

[107] T-Mobile USA comments at 9.

CellAntenna makes comment that a managed access solution nulls the necessity to confiscate contraband phones.[108] Tecore discusses the topic further, stating:

> Tecore does not believe it is effective to require contraband cellular devices to be physically located and removed. This approach entails additional resources and time from the prison administration. Managed access is designed to assure the prevention of unauthorized communications without requiring the retrieval of devices, which is manpower-intensive.[109]

Regulatory/Legal Issues

Managed access technology, in hand with proper authorizations from the FCC, may be an effective tool to combat the contraband cell phone problem in correctional facilities.[110] In order to operate a managed access system, the managed access provider "would require both a license to transmit and authorization by the carriers servicing the area."[111] Tecore Networks was able to provide a demonstration of its iNAC managed access solution after it acquired an FCC issued Special Temporary Authority (STA) "as well as a coordinated sublease of spectrum from the carriers."[112] If utilized, long-term spectrum leases, which serve as transmitting authorizations upon FCC approval, will be necessary. The wireless carriers, in contract, must "retain the right to terminate the lease or take other action in the event of harmful interference outside the prison."[113] For the managed access deployment in Parchman, the FCC has approved all required filings from Tecore and the wireless carriers, including long-term spectrum lease agreements.

ITT raises a privacy concern, specifically questioning whether, "[e]ven though it might be forbidden for an inmate to possess and use a cell phone … are calls from the inmate to his lawyer or doctor protected, and if so, how would the system distinguish these calls from other calls?"[114]

Technical Issues

Prior to installing a managed access system, an RF survey should be conducted to identify the correct system configuration. Once installed and activated, the managed access system will perform its duties, including the passage of 9-1-1 calls to the commercial carrier networks without interference. A managed access system intercepts calls and text messages utilizing both GSM and CDMA modulation schemes, and as stated previously, can be upgraded to cover LTE and the 700 MHz band.[115]

In their comments to the NOI, Verizon Wireless notes that they are working on a spectrum lease agreement to enable Tecore to operate a managed access system in Mississippi on frequencies

[108] CellAntenna comments at 6.
[109] Tecore comments at 12.
[110] ShawnTech comments (slides) at 26.
[111] ITT comments at 17.
[112] Tecore comments at 26.
[113] AT&T comments at 12.
[114] ITT comments at 17.
[115] Tecore comments at 6.

licensed to Verizon Wireless.[116] Since then, with the actual deployment of that managed access system in Mississippi, the technology was shown to be able to discriminate between authorized calls (including to 9-1-1) and calls from contraband, unknown, and unregistered phones.[117] As described by the Mississippi Department of Corrections, the deployed managed access system has the following effect: "[n]ow, instead of a hearing a familiar voice on the other end of the line, Parchman inmates communicating with illegal cell phones are going to hear a voice recording that states, '*the cellular device you are using at the Mississippi State Penitentiary has been identified as contraband and is illegal to possess under the criminal statute, 47-5-193. The device will no longer function.*' "[118]

OBSERVATIONS

The following key observations highlight the use of managed access technologies as a possible solution to mitigate contraband cell phone use by inmates:

- A managed access system can and must be designed to operate at specific boundaries. Managed access systems intercept calls within those boundaries in order to allow corrections officials to prevent inmates from accessing carrier networks. The cell signal is not blocked by a jamming signal, but rather, is captured (or re-routed) and prevented from reaching the intended base station, thereby disallowing the completion of the call.
- A managed access system can provide the desirable result – preventing prisoners from communicating by cell phone with people outside of the prison. However, the system permits authorized users to pass through to the network and all 9-1-1 calls are forwarded as well.
- Managed access techniques do not violate the Communications Act if the FCC issues the proper authorizations and the users comply with the terms of those authorizations. It is unclear, however, whether the use complies with other statutes.[119]
- Managed access requires structured coordination and cooperation between a managed access system vendor and the wireless service providers in the affected area. The partnership with the wireless carriers is critical to ensuring the long-term efficacy of the solution as new products and different frequencies are utilized in the wireless landscape. Coordination of spectrum issues between the FCC, the wireless carriers, and the managed access provider is critical for successful implementation.

---

[116] Verizon Wireless comments at 11.
[117] *Supra* note 99.
[118] *Id.* Since its deployment, Mississippi Corrections blocked over 216,000 communication attempts in one month. *See* http://www.mdoc.state.ms.us/PressReleases/2010NewsReleases/2010-09-01 Combined Final.ppt, page 29. The report does not address whether there were unauthorized calls that were not captured by the managed access system.
[119] For example, interception of signals may risk violating certain wiretap statutes. In particular, managed access operations may be subject to the "pen/trap" statute. Generally, managed access operations fit the definition of a "trap and trace device," 18 U.S.C. § 3127(4), because they capture "dialing, routing, addressing, and signaling information reasonably likely to identify the source of the wire or electronic communication." Trap and trace devices are allowed only pursuant to a court order or under one of the exceptions to the pen/trap statute found in 18 U.S.C. § 3121(b). One of the exceptions applies when the consent of the user of the wire or electronic communications has been obtained. To the extent that a managed access operation is strictly limited to the prison grounds, it should be possible to establish a regime of consent for the usage of a trap and trace device, which in turn would eliminate the risk of violation of the pen/trap statute.

- Costs to implement a managed access system can have a number of variables (such as the number of frequency bands to cover). Centralizing control and management of the systems is an important method to lower the cost of installation as well as long-term operational and maintenance costs. Deploying a managed access system that covers multiple frequency bands will increase costs.
- Managed access systems can be operated remotely and the controlling base station antenna can be mounted on towers, mobile platforms, or other locations outside of the prison confines, which are not accessible to inmates or prison staff.
- As experienced in the Mississippi deployment, managed access systems also can be potentially deployed at no cost to the prison authority, based on a separate arrangement between the managed access and pay phone service vendors.

SECTION 5
DETECTION

OVERVIEW

Detection is the process of locating, tracking, and identifying various sources of radio transmissions – in this case, cell phone signals from prisons. Detection, or direction-finding, is used in a wide variety of applications including, for example, cell phone assignments, the location of 9-1-1 emergency calls and marine distress calls. For accurate position location in an environment such as within a prison facility, detection technology triangulates a cell phone signal and requires correctional 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 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. These systems can only detect a cell phone when it is in use – either placing or receiving a call. The devices are "passive" receive-only devices, and do not necessarily require any authorization or license for the equipment or the user to implement and operate.

SUMMARY OF COMMENTS

A number of commenters to the NOI support the use of detection technologies to eliminate contraband cell phone use. For example, ICSolutions notes that location and detection of cell phone calls provides investigators with real time information, call timing, and call patterns that assist with law enforcement intelligence gathering capabilities.[120] Motorola believes that detection methods (in combination with managed access) are the preferred approaches as they are far less likely to cause interference.[121] CTIA contends that detection methods have advantages over jamming and would better enable correctional officials to confiscate contraband cells phones and investigate contraband use habits.[122] Similarly, Sprint Nextel supports detection technologies as a preferred solution over jamming.[123] Canada correctional facilities have deployed a number of capabilities to fight this problem such as interception and detection.[124]

Devices and Frequency Bands

A number of commenters affirm that detection systems are receive-only solutions that have a frequency band or bands programmed into the system. For example, Enterprise Electronics submits that certain types of detectors have multiple frequency bands and formats in them to do the necessary analysis to detect and locate the phones of interest.[125] ITT states that detection

[120] ICSolutions comments at 3.
[121] Motorola comments at 3-4.
[122] CTIA comments at 4.
[123] Sprint Nextel comments at 1.
[124] Correctional Services of Canada comments at 1.
[125] Enterprise Electronics comments at 9.

systems are compatible with any device since they do not require protocol participation, and hence offer the widest range of coverage and are easily scalable to any frequency band.[126] The BVS hand-held bloodhound cell detector is a multi-band receiver that can detect in a number of frequency bands.[127] ShawnTech notes that all detection systems (hand-held, portable and fixed sensor) detect all technologies available.[128] BINJ confirms that detection systems have the ability to adapt to new frequency bands.[129] The AirPatrol Wireless Locator System can detect Wi-Fi and cellular service.[130]

Interference to Other Radio Services

Because detection systems do not emit RF energy, a number of commenters tout the value in detection systems as not interfering with other radio services. For example, ICSolutions states that "detection-location is a non-invasive solution that will not interfere with administrative radio or other facility administrative equipment."[131] AirPatrol states that its solution does not cause interference to cellular services or public safety communications.[132] ITT also notes that RF detection systems do not interfere with any communication system.[133] BVS implies that jamming is the only solution that would cause concern of interference to other radio services.[134]

Protecting 9-1-1 and Authorized Calls

The NOI asked several questions with regard to the technologies capable of protecting both 9-1-1 and authorized calls, as Congress specifically directed that NTIA evaluate this in its tasking. Several commenters elaborate on the fact that detection systems do not block 9-1-1 or authorized calls from being completed since they do not transmit any RF energy to block a signal. For instance, BINJ notes that cell detection systems do not block or deny cell phone use.[135] ITT notes that detection systems do not disrupt cellular traffic.[136] T-Mobile USA contends that this is the case and asserts that detection is preferable over jamming since detection systems do not interfere with critical public safety and legitimate communications.[137] Similarly, ManTech states that "passive detection systems do not impact the neighboring commercial networks."[138]

Cost Considerations

The cost for implementing detection systems varies according to the complexity of the detection system deployed, and the time and labor required to retrofit the facility. Hand-held units are at

[126] ITT comments at 6-7.
[127] BVS comments at 5.
[128] ShawnTech comments (slides) at 19-21.
[129] BINJ comments at 3.
[130] AirPatrol comments at 2.
[131] ICSolutions comments at 4.
[132] AirPatrol comments at 2.
[133] ITT comments at 3.
[134] BVS comments at 5.
[135] BINJ comments at 8.
[136] ITT comments at 3.
[137] T-Mobile USA comments at 9.
[138] ManTech comments at 6.

the low-end of the cost scale since they require no infrastructure. BVS contends that these units are attractive in terms of costs.[139]

More sophisticated systems increase costs. ITT suggests that the largest unknown cost for a detection system is in the infrastructure, while detection systems have much lower on-going and recurring costs than jamming and managed access solutions.[140] ITT provides cost estimates for their detection system: $20,000 to $600,000 depending on area of coverage, number of buildings/sensors, and number of inmates.[141] One-day training for staff costs $1,500.[142]

BINJ offers that software and technical support are on-going costs and that the size of the facility and the accuracy (that is, number of sensors) most likely affect costs.[143] Further, BINJ states that the hardware and software for a 500-cell facility with accuracy down to an inmate's cell costs $350,000.[144]

Locating Contraband Cell Phones

The NOI asked several questions with regard to the capabilities of the technologies on location and location accuracy.[145] The size of the devices makes them easily hidden so that finding them is a concern.[146] By design, detection systems identify, with a certain degree of accuracy, the location of the caller.[147] The location accuracy depends on the number of sensors installed, prison composition, and other factors. ITT notes that its system can obtain an accuracy of 3-5 meters.[148] AirPatrol states that the Wireless Location System has an accuracy of 3 meters.[149] Additionally, BINJ asserts that the age of the facility and composition affect the accuracy, but with newer facilities, the resolution is to the prisoner's cell.[150] Bahia 21 claims a geo-location accuracy of 10-15 meters is sufficient to initiate a physical search of the contraband cell phone.[151] Using triangulation, the location of the cell phone can be determined to within a few yards.[152]

---

[139] BVS comments at 3.
[140] ITT comments at 13-14.
[141] *Id.* ITT contends that for the same area of coverage, a distributed jamming system would cost two to three times more. *Id.*
[142] *Id.*
[143] BINJ comments at 5.
[144] *Id.* at 6.
[145] The Maryland Department of Public Safety and Correctional Services demonstrated a number of detection technologies, and the report concluded that there were varying degrees of accuracy in terms of cell phone detection based upon each vendor's technological abilities. *See Supra* note 70.
[146] Art Beller comments at 1.
[147] BVS states in its comments that during a 2-hour sweep of cell blocks in the Maryland demonstration, the Bloodhound hand-held device successfully located 5 smuggled contraband phones. BVS comments at 4.
[148] ITT comments at 16.
[149] AirPatrol comments at 1.
[150] BINJ comments at 7. The BINJ system (CellScan) was tested with the Washington, DC Department of Corrections with an accuracy of detection of 100%. *See* CTIA comments at 15.
[151] Bahia 21 comments at 3.
[152] Peter McDonald comments at 1.

Regulatory/Legal Issues

As is the case with all potential technologies, one the chief concerns of regulatory agencies is the effects that these technologies have on the rules and regulations promulgated within the structure of the U.S. telecommunications environment. Noting this concern, the NOI asks a series of questions on this topic. The consensus of the commenters is that there are no regulatory and/or legal issues associated with detection technologies. ITT states that no regulatory agreements are needed for their system.[153] BVS notes that, because of the passive nature of its product as detecting signal strength in cell phone uplink signals, it has no regulatory/legal issues.[154] ShawnTech concurs that the use of detections systems is legal.[155] According to AirPatrol, no FCC licenses, waivers, or permits are required to deploy the Wireless Locator System.[156]

As is the case for all potential solutions, however, if detection goes beyond direction-finding to include recording of information, such as numbers called or even the number of the contraband cell phone, legal issues may be invoked. These capabilities may reside within a detection technology as additional features, but are not necessary for locating a transmitting cell phone.

Technical Issues

A number of technical issues are discussed in the comments to the NOI. TruePosition argues that location accuracy depends upon the type of location solution that is employed and that network-based location Uplink Time Difference of Arrival provides "more than reliable location information for corrections officials to detect and find the contraband cell phones."[157] Contrary, location detection by Advanced GPS will not work in a prison because of the prison structure (and hence signal loss) and the ability of the end user to turn off this capability.[158] ITT similarly notes that GPS is easily defeated by turning off the GPS receiver.[159]

On other technical issues, ITT notes that the detection system it uses is independent of modulation, requires very little on-site RF engineering, and can perform detection during text messaging.[160] BINJ concurs and notes that no site engineering is needed, modulation schemes or channel access methods do not impact the BINJ detection system, shorter air time from text messages do not present problems, and the system is effective against high-speed, high-data rate formats such as LTE that are expected to operate in the 700 MHz band.[161] AirPatrol's Wireless Locator System can locate the phone during voice conversations, internet browsing, sending and receiving emails, or text messaging.[162]

[153] ITT comments at 17.
[154] BVS comments at 5.
[155] ShawnTech comments (slides) at 18.
[156] AirPatrol comments at 2.
[157] TruePosition comments at 3.
[158] *Id.*
[159] ITT comments at 16.
[160] *Id.* at 18-19.
[161] BINJ comments at 7-8.
[162] AirPatrol comments at 2.

OBSERVATIONS

The following key observations highlight the use of detection systems as a possible solution to mitigate contraband cell phone use by inmates:

- Detection systems can range from simple hand-held and portable units to more complex fixed units with sensors attached by wireless or by wire-line to the sensing hardware and software.
- Hand-held detection units offer the least expensive equipment costs to find the contraband cell phones, yet require staff resources and time to physically locate them. However, inmates may react to movement of prison staff and avoid using cell phones during times when prison staff are known to be on patrol. Fixed detection sensors require more equipment and installation, and increase the costs for these technologies.
- Sensors used to identify the location of the contraband cell phones should be placed in a location where inmates cannot tamper with or destroy them, or be tamper-proof. Location accuracy of these systems depends upon a number of factors including the number of sensors used and prison construction.
- Detection systems are passive by nature and, unless they are used for data mining, have no regulatory or legal issues; do not transmit and therefore do not interfere with authorized and 9-1-1 calls. They do not cause interference to other radio services and have the capability to cover a wide array of frequency bands and access methods used by mobile devices.
- Locating and then confiscating contraband cell phones provides law enforcement officials with opportunities for intelligence-gathering. Correctional and law enforcement officials may seek to obtain the illegal cell phones and conduct forensic analysis on the devices for further investigation.

SECTION 6
OTHER TECHNOLOGIES

The NOI asked if there are technologies available other than the three categories previously described. A number of respondents indicated that standardized protocols, hybrid systems, and Non-Linear Junction Detectors (NLJDs) are other technologies to consider for preventing contraband cell phone use in prisons.[163]

STANDARDIZED PROTOCOLS

In their comments to the NOI, Try Safety First notes that it has developed a simple, cost-effective, comprehensive solution for contraband prison cell phones as it believes that, in addition to enormous costs and possible violation of law, jamming equipment cannot jam Skype and satellite phones.[164] Further, Try Safety First contends that managed access and detection systems are not the best solution due to the need for constant monitoring and the inability to detect, confiscate, and prevent many of the illegal activities prior to the directives being carried out.[165]

The Try Safety First solution is based upon using a series of low-cost Bluetooth sensors located throughout the prison (programmed for coverage between 1 to 60 meters) coupled with universal and standardized protocols that would have to be incorporated into the firmware of the handsets. These "sets of instructions" communicate with the hand-held device by essentially locking the device and making it unusable. Try Safety First contends that this solution is inexpensive, cannot be turned off nor tampered with by inmates, and protocols can be incorporated into the handset as new units are introduced into the market.[166] For funding, Try Safety First proposes a $1 per phone fee that would offset the expenses to retrofit the prisons with the Bluetooth sensors.[167]

---

[163] A number of commenters suggest that decreasing prison landline phone rates reduces contraband cell phone use. *See, e.g.*, Letter to the Honorable Larry Strickling, Assistant Secretary for Communications and Information, from the Honorable Rick Boucher, Member of Congress, and the Honorable Bobby Rush, Member of Congress (May 27, 2010) (*citing* Paul Hammel, "Prison Phone Smuggling Reduced," Omaha World-Herald (May 17, 2010)); Paul Kruger comments. Some commenters suggest more vigilant screening of staff and visitors (Ann Worth comments), using shielding on prison walls such as copper mesh (Roy Stratton comments), or metal detectors, body scanners and x-rays (Enterprise Electronics comments). Although these all may have merit, they are beyond the scope of this report. However, Section 3 of the Cell Phone Contraband Act of 2010 requires the Government Accountability Office to conduct a study of landline rates in prisons and efforts to prevent the smuggling of cell phones. Pub. L. No. 111-225, 124 Stat. 2387 (Aug. 10, 2010). Also, the FCC is considering prison land-line rates in an open docket, CC Docket No. 96-128, *Alternative Rulemaking Proposal Related to Inmate Calling Services.*

[164] *See generally* Try Safety First comments.

[165] *Id.*

[166] *Id.*

[167] *Id.*

HYBRID SYSTEMS

Boeing suggests that NTIA consider another category for a potential solution – a combination of technologies known as hybrid systems.[168] Boeing states that its Digital Receiver Technology (DRT) uses a combination of both managed access and detection techniques to locate and control contraband cell phone use. In arguing against other technologies, Boeing states that jamming does not discriminate between users, is imprecise and excessive, and does not locate the actual device; and detection technologies are the least effective in preventing contraband cell phone use.[169] Boeing asserts that managed access technologies are the most effective solution for preventing use in prisons.[170]

Boeing explains that the DRT device mimics a cellular base station to:

> cause dormant cell phones to perform a registration with the DRT device. Cell phones not of interest are released. Cell phones of interest are forced to transmit location information to the DRT device operator who can then assist prison personnel to locate the contraband phone and user. Depending on the DRT device mode used, cell phones of interest can then be returned to their network or locked into the DRT device, preventing contraband use.[171]

NON-LINEAR JUNCTION DETECTORS (NLJDs)

A number of commenters offer another category for inclusion into the technologies used to prevent contraband cell phone use – NLJDs.[172] NLJDs hunt for semiconductor junctions in the electronics (transistors, diodes, etc.). The Orion NLJD has an antenna that is passed over an electronic device (in this case, a cell phone) and alerts when it is in the presence of such devices by sending a signal similar to a metal detector.[173] Research Electronics International (REI) submits that this device detects cell phones regardless of the device being on or off, does not depend on frequency band, is FCC compliant and has no regulatory or legal issues, and will not interfere with other radio services, other cell phone calls or 9-1-1 calls.[174] Bahia 21 notes that its device is currently used by many customers for the detection of contraband cell phones in prisons.[175] A number of commenters note the success at correctional facilities in finding and locating contraband cell phones using NLJDs.[176]

A few commenters note the drawbacks of using such devices. For example, Enterprise Electronics notes that NLJDs send a radio signal invasive to people, are large in size, and cannot

[168] Boeing comments at 3.
[169] Boeing comments at 2.
[170] Boeing comments at 3.
[171] Boeing comments at 6.
[172] *See, e.g.*, REI comments at 1-3; Enterprise Electronics comments at 7; BVS comments at 1; Bahia 21 comments at 2.
[173] REI comments at 1-2. A unit costs $15,800 and training is required.
[174] *Id.*
[175] Bahia 21 comments at 2.
[176] *See, e.g.*, CTIA comments at 16; REI comments at 2.

be deployed in open areas to detect cell phones.[177] BVS suggests that NLJDs are not stealthy; they must be in very close proximity to the device to detect it and require excessive amounts of time by correctional officials to scan for contraband cell phones.[178]

OBSERVATIONS

The following key observations highlight the use of the above technologies as possible solutions to mitigate contraband cell phone use by inmates:

- The Try Safety First solution is predicated upon standardized protocols being developed, adopted, and implemented by the wireless industry. To date, no such standards exist and this potential solution will not come to fruition until the wireless industry adopts standardized protocols for wireless mobile devices.
- Hybrid systems utilize a combination of techniques, such as managed access and detection, to control and locate contraband cell phones. The Boeing DRT system uses technology that detects cell phone usage, collects data from active cell phones and then releases or locks the phone.[179] Like some other solutions, costs may be a consideration for correctional officials. Additionally, holding cell phone signals and collecting data present potential legal issues as "trap and trace" devices.
- NLJDs are hand-held, overt devices that require staff to physically search a prisoner's cell for the phone. They present no regulatory or legal issues and do not interfere with other authorized users.

[177] Enterprise Electronics comments at 7.
[178] BVS comments at 1.
[179] The DRT was part of the Maryland Department of Corrections December 2009 testing and the DRT sensors identified 11 phones that may have been contraband. The managed access portion of the DRT was not used.

SECTION 7
SUMMARY

As commenters note, prisoners are using contraband cell phones to conduct criminal activity. Although some facilities are making progress, correctional officials must be vigilant and use all available means to stop the phones from making their way to inmates in the first place.[180] Nevertheless, the record indicates that prison authorities are devoting increasing financial resources and personnel time to ferreting out, confiscating, and eradicating contraband cell phones in their prisons. Further, the record identifies a number of technologies that can reduce or eliminate contraband cell phone use in prisons. Signal jamming, cell phone detection, managed access, and other technologies are ways to mitigate cell phone use by inmates.

All the solutions involve a wide array of issues, including: complex technical, legal and regulatory issues; installation and operational costs; and interference potential. Each approach has trade-offs and each offers advantages and disadvantages. The use of jammers by State or local prison officials is a violation of the Communications Act of 1934, and hence illegal. Jamming cell signals may be effective where legal in Federal applications, and in some settings with careful design, but its effectiveness and utility may be greatly diminished by interference with other communications, including critical police, firefighter and emergency medical communications and 9-1-1 calls. Managed access technologies hold promise as a solution. The technology requires close coordination with the FCC and wireless carriers; and the FCC has already developed the necessary regulatory requirements. Further, while the first managed access deployment in Mississippi was accomplished at no cost to the prison authority, it is uncertain whether this business model can be applied successfully in other States. Thus, implementing such systems elsewhere, especially for large-prison environments, may be costly, although comparable to other methods including cell jamming. Detection technologies and NLJDs have no regulatory or legal issues, but involve additional costs and time for searches if locating the contraband phones is a requirement for correction officials.

What may be a reasonable approach for one institution may not work for another. Each prison is unique in size, shape, structure, security level, and location. As such, one technology does not fit all and a particular solution may be preferable over the other choices based upon each institution's requirements and setting. For instance, a prison located in a rural setting may opt for a different solution than a prison located in an urban area where there is a greater density of wireless communications devices operating nearby. Also, a combination of approaches, for example, managed access with detection technologies, may be a "best-fit" for correctional officials at their respective prisons. Further, costs and time are drivers for correctional officials to consider when implementing these technologies, and these costs will vary based upon

[180] The Maryland Department of Corrections has seen a drop in the number of cell phones found in their prisons by nearly one-third from 2009. They attribute this to increased intelligence, search and seizure, and investments in technology. *See* http://www.dpscs.state.md.us/publicinfo/news_stories/press_releases/20100727a.shtml. Also, a new law has been enacted that prohibits Federal prisoners from possessing or using cell phones and similar wireless devices. *See* Cell Phone Contraband Act of 2010, Pub. L. No. 111-225.

coverage area at each prison, among other things. Some correctional facilities may have a requirement to physically locate and confiscate the phones. If this is the case, detection technologies may be preferable over other solutions.

When considering the solutions, it is essential to maintain and protect authorized radio communications (for example, authorized cell phone calls by consumers, 9-1-1 calls and public safety communication networks), both inside and outside of the prison walls. Proper RF site engineering and testing specific to a particular location are critical when implementing some of these technologies in order to reduce interference by creating an RF footprint that matches as closely as possible to the prison confines.

The proliferation of mobile devices will lead to more services and features such as high-speed data and video. With that comes new frequency bands in which they operate, such as the 700 MHz band. Technologies used against contraband cell phones will need to keep pace with the speed at which mobile devices are introduced into the marketplace. It is reasonable to assume that interdiction efforts will not prevent access to a plethora of devices by inmates and that it will not take long for them to find out which devices work and which ones are blocked, dropped, or detected. Deploying technologies that transverse all available parts of the radio spectrum in which these mobile devices operate comes with a price and prison officials must consider the cost-benefit analysis. Equipment upgrades to these "contraband-fighting" technologies will be required, and close coordination with the wireless industry will be necessary. Correctional officials will need to decide what devices and hence frequency bands will be targeted (i.e., cellular and/or PCS and/or SMR/iDEN and/or 700 MHz, etc.).

The risk that prisoners will tamper with equipment is an issue that needs to be considered. Managed access systems can be operated remotely and the controlling base station antenna(s) can be mounted on towers or other locations within their permissible range of operation that are not accessible to inmates or prison staff. Jamming or detection systems in particular have to be installed in closer proximity to prisoners' living areas, and unless mounted in secure or inaccessible locations, may be subject to damage or removal.

Table 7-1 shows a general summary of the various technologies as possible solutions to prevent contraband cell phone use in prisons. There are various iterations within each category. For instance, there are fixed detection sensing systems or hand-held portable detection units; managed access techniques may be performed differently among the vendors; detection techniques will vary from one vendor to another and may offer additional capabilities and features. Therefore, correctional officials should consult with the manufacturers and vendors of these technologies for specific details regarding their prison and unique requirements.

Table 7-2 summarizes the advantages and disadvantages for each of the technologies discussed in this report. Some of the approaches come with legal hurdles or limitations. Furthermore, each prison's own unique characteristics (e.g., size and configuration of the prison), environment (rural versus urban setting), resources (e.g., financial and staff), and requirements (e.g., need for law enforcement intelligence) will help determine which approach is the most practical, feasible, and economical to implement.

Table 7-1
Technological Approaches to Combat Contraband Cell Phone Use in Prisons

	Jamming	Managed access	Detection	NLJDs	Hybrid/DRT	Standard protocols
Covers all frequency bands	New hard/software needed to upgrade as bands change	Could match any band used in area where service providers agree	Yes	Detects devices	With equipment changes and carrier consent	If protocols are established in the various devices
Potential to interfere with other radio services	Yes-emits RF energy	Yes-emits RF energy; requires proper installation and operation	No-does not transmit	No	No for detection-only; yes for managed access	No
Protects 9-1-1 and authorized calls	No-pure jamming does not discriminate	9-1-1 yes; authorized calls if in database of known users	Yes-only detects	Yes	Yes	No-all phones are locked within the boundaries
Identifies location	No	No	Yes	Through physical search	Yes, with portable device	No
Cost considerations	Extensive testing prior to implementation; can vary based on complexity of site; infrastructure costs	Depends on coverage, frequency bands, etc; can be at no-cost to prison authority or vary based on complexity of site; infrastructure costs	Hand-held units less expensive; number of sensors, installation	Less expensive; requires staff time	Implementation costs can be expensive	Inexpensive Bluetooth communications
Regulatory/legal issues	Illegal for non-Federal entities; pending legislation for case-by-case jamming	Requires FCC regulatory authorizations and agreements between system vendor and carriers; any data mining may have legal implications; trap and trace issues with State and locals	No authorization required for direction-finding, but any data mining may have legal implications	None	Trap and trace issues with State and locals for data mining capabilities; requires regulatory authorizations between vendor and carriers	Impose a $1 per-phone fee to offset installation costs
Technical issues/other issues	Depends on size, shape, structure; RF engineering needed	RF engineering needed; all forms of communication	Location accuracy; sense any technology	Must be very close to phone; overt	RF engineering needed	Adoption of protocols by industry; conceptual only

Table 7-2

Advantages and Disadvantages of Various Technologies to Mitigate Contraband Cell Phone Use

Jamming • Potential to cause interference outside prison or to adjacent bands unless properly designed • Does not permit 9-1-1 and authorized calls • Violates the Communications Act of 1934 when performed by non-Federal officials • Costs vary with complexity of the site • Significant site analysis and testing needed	**Detection** • Does not cause interference • Protects 9-1-1 and authorized calls • Provides general location of devices • May require legal authorization unless limited to direction-finding • Low-cost hand-held solutions available
Managed access • Potential to cause interference outside prison or to adjacent bands unless properly designed • Permits 9-1-1 and known authorized calls • Legal under the Communications Act but requires FCC approval and carrier consent • Multiple formats and technologies • Costs can vary with complexity of site, yet in first deployment was zero for the prison authority	**Non-linear junction detectors** • Does not cause interference • Protects 9-1-1 and authorized calls • No regulatory or legal issues • Requires staff time to locate phones
Hybrid systems/digital receiver technology • Does not cause interference if using detection-only; for managed access, potential to cause interference outside prison or to adjacent bands unless properly designed • Permits 9-1-1 and authorized calls • Regulatory or legal issues; requires FCC approval and carrier consent • Costs could be high based upon complexity of the site	**Standardized protocols** • Would not cause interference • Conceptual • Need for adoption and implementation of standardized protocols in mobile devices • Proposed $1 per-phone fee to offset installation

Appendix A
NTIA NOI on Contraband Cell Phones

subject merchandise; and (3) no compelling reasons for denial exist, we are granting this request and are postponing the final determination until no later than 135 days after the publication of this notice in the **Federal Register**. Suspension of liquidation will be extended accordingly.

ITC Notification

In accordance with section 733(f) of the Act, we have notified the ITC of the Department's preliminary affirmative determination. If the Department's final determination is affirmative, the ITC will determine before the later of 120 days after the date of this preliminary determination or 45 days after our final determination whether imports of copper pipe and tube from Mexico are materially injuring, or threatening material injury to, the U.S. industry. *See* section 735(b)(2) of the Act. Because we are postponing the deadline for our final determination to 135 days from the date of the publication of this preliminary determination, the ITC will make its final determination no later than 45 days after our final determination.

Public Comment

Interested parties are invited to comment on the preliminary determination. Interested parties may submit case briefs to the Department no later than seven days after the date of the issuance of the last verification report in this proceeding. *See* 19 CFR 351.309(c)(1)(i). Rebuttal briefs, the content of which is limited to the issues raised in the case briefs, must be filed within five days from the deadline date for the submission of case briefs. *See* 19 CFR 351.309(d)(1) and 19 CFR 351.309(d)(2). A list of authorities used, a table of contents, and an executive summary of issues should accompany any briefs submitted to the Department. Executive summaries should be limited to five pages total, including footnotes. Further, we request that parties submitting briefs and rebuttal briefs provide the Department with a copy of the public version of such briefs on diskette. In accordance with section 774(1) of the Act, the Department will hold a public hearing, if timely requested, to afford interested parties an opportunity to comment on arguments raised in case or rebuttal briefs, provided that such a hearing is requested by an interested party. *See* also 19 CFR 351.310. If a timely request for a hearing is made in this investigation, we intend to hold the hearing two days after the rebuttal brief deadline date at the U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230, at a time and in a room to be determined. Parties should confirm by telephone, the date, time, and location of the hearing 48 hours before the scheduled date.

Interested parties who wish to request a hearing, or to participate in a hearing if one is requested, must submit a written request to the Assistant Secretary for Import Administration, U.S. Department of Commerce, Room 1870, within 30 days of the publication of this notice.

Requests should contain: (1) the party's name, address, and telephone number; (2) the number of participants; and (3) a list of the issues to be discussed. At the hearing, oral presentations will be limited to issues raised in the briefs.

This determination is issued and published pursuant to sections 733(f) and 777(i)(1) of the Act.

Dated: May 5, 2010.

Ronald K. Lorentzen,

Deputy Assistant Secretary for Import Administration.

[FR Doc. 2010–11342 Filed 5–11–10; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 100504212–0212–01]

Preventing Contraband Cell Phone Use in Prisons

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of inquiry.

SUMMARY: The U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) seeks comment on technical approaches to preventing contraband cell phone use in prisons. Congress tasked NTIA with developing, in coordination with the Federal Communications Commission (FCC), the Federal Bureau of Prisons (BOP), and the National Institute of Justice (NIJ), a plan to investigate and evaluate how wireless jamming, detection and other technologies might be utilized for law enforcement and corrections applications in Federal and State prison facilities. To assist in its evaluation of these technologies, NTIA requests information from the public on technologies that would significantly reduce or eliminate contraband cell phone use without negatively affecting commercial wireless and public safety services (including 911 calls and other government radio services) in areas surrounding prisons.

DATES: Comments are requested on or before June 11, 2010.

ADDRESSES: Parties may mail written comments to Richard J. Orsulak, Emergency Planning and Public Safety Division, Office of Spectrum Management, National Telecommunications and Information Administration, U.S. Department of Commerce, 1212 New York Avenue, NW., Suite 600B, Washington, DC 20005, with copies to Edward Drocella, Spectrum Engineering and Analysis Division, Office of Spectrum Management, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW., Room 6725, Washington, DC 20230. Alternatively, comments may be electronically submitted in Microsoft Word format to *contrabandcellphones@ntia.doc.gov*. Comments will be posted on NTIA's Web site for viewing at *http://www.ntia.doc.gov/osmhome/contrabandcellphones/*.

FOR FURTHER INFORMATION CONTACT: Richard J. Orsulak, Emergency Planning and Public Safety Division, Office of Spectrum Management, National Telecommunications and Information Administration, U.S. Department of Commerce, 1212 New York Avenue, NW., Suite 600B, Washington, DC 20005; telephone (202) 482–9139 or e-mail *rorsulak@ntia.doc.gov*.

SUPPLEMENTARY INFORMATION:

Overview

The mobile phone industry has enjoyed significant growth since the inception of the analog wireless cell phone network in the early 1980s.[1] The 1990s saw the development of digital networks, and thereafter, high-speed data networks became available to consumers. The growth of the mobile phone industry has been fueled, in part, by consumer demand for instant access anywhere and anytime. Features such as data, image, and video communications have also contributed to the overwhelming demand for mobile

[1] For the purpose of this Notice of Inquiry (NOI), the use of the word "cell phone" will refer to any wireless, portable device that is available to the public on a subscription or prepaid basis for delivering voice and/or data services such as text messages. It includes, for example, phones operating within the Cellular Radio Service in the 800 MHz bands; broadband Personal Communications Services (PCS) in the 1.9 GHz bands; the Advanced Wireless Services (AWS) in the 1.7 GHz band; Specialized Mobile Radio (SMR) services in the 800 and 900 MHz bands; and any future mobile wireless devices that plan to operate in bands such as the 700 MHz band.

services and applications. As of December 2009, there were approximately 286 million wireless subscriber connections in the United States compared to nearly 208 million in December of 2005, which represents an increase of 38 percent.[2] During this same time period, the number of minutes used (on an annual basis) increased by 150 percent, while the wireless penetration (as a percentage of total U.S. population) increased from 69 percent to 91 percent.[3] These trends indicate that more people are relying on wireless mobile devices to communicate for their daily business and personal needs.

The use of contraband cell phones by inmates has risen as the U.S. prison population continues to expand.[4] The number of cell phones confiscated by prison officials has dramatically increased in only a few years. For example, during 2006 California correctional officers seized approximately 261 cell phones in the State's prisons and camps; by 2008, that number increased ten fold to 2,811.[5] Maryland and other States have also seen a rise in the number of confiscated cell phones in their State prisons. In 2009, Maryland prison officials confiscated nearly 1,700 phones, up from approximately 1,200 phones the year before.[6] This increase in cell phone use by inmates is a mounting concern among correctional administrators across the country.[7]

Recognizing the need to take action to curb contraband cell phone use, the United States Senate passed a bill in 2009 that would amend the Communications Act of 1934 to authorize the FCC to permit the supervisory authority of a correctional facility to operate a system within the facility to prevent, jam, or otherwise interfere with unauthorized wireless communications by individuals held in the facility.[8] Also, legislation has been introduced and passed in the U.S. Senate that would prohibit Federal prisoners from possessing or using cell phones and similar wireless devices.[9]

In December 2009, Congress inserted language in the Conference Report to the Department of Commerce FY 2010 Appropriations tasking NTIA, in coordination with the FCC, BOP, and NIJ, to develop a plan to investigate and evaluate how wireless jamming, detection, and other technologies might be utilized for law enforcement and corrections applications in Federal and State prison facilities.[10] Congress also asked that the plan consider the adverse effects that these technologies impose on commercial wireless and public safety services in areas surrounding the prisons.[11] This NOI seeks public input to assist NTIA with its evaluation of technologies to prevent the use of contraband cell phones in Federal and State facilities.[12]

NTIA understands that a number of technological approaches exist that could help prison officials block or reduce unauthorized use of cell phones by inmates provided that these approaches could be legally implemented. NTIA, in coordination with the FCC, BOP, and NIJ, have preliminarily identified three categories of contraband cell phone intervention: jamming, managed network access, and detection.

Jamming

Radio jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of disrupting use of electronic devices, equipment, or systems—in this case, mobile devices such as cell phones. A cell phone works by communicating with its service network through a cell tower or base station. These cell towers divide an area of coverage into cells, which range in size from a few city blocks to hundreds of square miles. The base station links callers into the local public switched telephone network, another wireless network, or even the Internet.

A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication link between the phone and the cell phone base station, essentially rendering the hand-held device unusable until such time as the jamming stops. Jamming devices do not discriminate among cell phones within range of the jamming signal—both contraband and legitimate cell phones are disabled. Currently, the operation by non-Federal entities of transmitters designed to jam or block wireless communications violates the Communications Act of 1934, as amended.[13] Nonetheless, several groups have filed with the FCC petitions for waivers to permit the use of cell phone jammers in prisons.[14] Groups such as

[2] CTIA Wireless Quick Facts, available at *http://www.ctia.org/advocacy/research/index.cfm/AID/10323.*

[3] *Id.*

[4] At the end of 2008, Federal and State correctional authorities had jurisdiction over roughly 1.6 million prisoners, of which over 200,000 (about 13 percent) were housed in Federal facilities. The Federal and State prison population rose by approximately 1 percent from year-end 2007 to 2008. *See* Sabol, William J., Heather C. West, and Matthew Cooper, "Prisoners in 2008," *Bureau of Justice Statistics Bulletin*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Dec. 2009, page 16, available at *http://bjs.ojp.usdoj.gov/content/pub/pdf/p08.pdf.*

[5] Special Report, *Inmate Cell Phone Use Endangers Prison and Public Safety*, Office of the Inspector General, State of California, May 2009, available at *http://www.oig.ca.gov/media/reports/BCI/Special%20Report%20of%20Inmate%20Cell%20Phone%20Use.pdf.*

[6] State of Maryland Fact Sheet, Keeping Communities Safe, Maryland Department of Public Safety and Correctional Services, Feb. 2010.

[7] *See, e.g.*, Department of Justice, Office of Justice Programs, National Institute of Justice, *Cell Phones Behind Bars*, Dec. 2009, available at *http://www.ncjrs.gov/pdffiles1/nij/227539.pdf;* Washington Examiner, *Drug Dealer Who Planned Murder Gets Life Sentence*, Scott McCabe, May 4, 2009, available at *http://www.washingtonexaminer.com/local/crime/Drug-dealer-who-planned-murder-gets-life-sentence-44327767.html;* Wired Magazine, *Prisoners Run Gangs, Plan Escapes, and Even Order Hits With Smuggled Cellphones*, Vince Beiser, May 22, 2009, available at *http://www.wired.com/politics/law/magazine/17-06/ff_prisonphones.* Contraband cell phone use is a problem in Federal prison facilities as well. *See* Testimony of Harley J. Lappin, Director, U.S. Bureau of Prisons before the U.S. Congress, Hearing on the Fiscal Year 2009 Budget Request for the Bureau of Prisons, the U.S. Marshal Service, and the Office of the Federal Detention Trustee, available at *http://www.november.org/stayinfo/breaking08/LappinTestimony.html.*

[8] S. 251, Safe Prisons Communications Act of 2009, available at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s251es.txt.pdf.* The Bill is under consideration in the House.

[9] S. 1749, The Cell Phone Contraband Act of 2010, available at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s1749is.txt.pdf.*

[10] H.R. Conf. Rep. No. 111–336 (2009), Division B, Title 1, Page 619, available at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_reports&docid=f:hr366.111.pdf.* The language specifically refers to methods of preventing contraband cell phone use within prison facilities. Jamming and detecting cell phone uses for other applications (such as within movie theaters) are not germane to either this NOI or NTIA's evaluation.

[11] *Id.*

[12] Although other contraband interdiction technologies may help to prevent the use of, or access to, contraband cell phones in prisons (such as x-rays, dogs, body scanning imagery, and other methods which detect contraband phones hidden on prison employees, visitors, and inmates), this NOI and NTIA's subsequent report will be limited to radio frequency (RF)-based, wireless technology solutions.

[13] 47 U.S.C. Sections 301, 302a, 333. The FCC had reiterated this fact in a Public Notice, *Sale or Use of Transmitters Designed to Prevent, Jam or Interfere with Cell Phone Communications is Prohibited in the United States*, DA–05–1776, June 27, 2005, available at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-1776A1.pdf.*

[14] *See, e.g.*, Letter from Devon Brown, Director, District of Columbia Department of Corrections, to Michael Copps, Acting Chairman, Federal Communications Commission, Feb. 2, 2009; Letter from Howard Melamed, CEO, CellAntenna Corporation, to Marlene H. Dortch, Secretary, Federal Communications Commission, March 3, 2009. The cellular radio service and other commercial wireless services fall under the auspices of the FCC rules and regulations, which are promulgated in Title 47 of the Code of Federal Regulations (C.F.R.). See *http://wireless.fcc.gov/index.htm?job=rules_and_regulations.*

the Association of Public Safety Communications Officials International, Inc. and CTIA have opposed the use of jamming for fear of interference to critical public safety operations and legitimate cell phone use in and around prisons.[15] Others, however, have supported its use in prisons.[16] Stating that it did not have the authority to permit such jamming, the FCC has denied the petitions.[17]

Managed Access

Managed access systems intercept calls in order to allow corrections officials to prevent inmates from accessing carrier networks. The cell signal is not blocked by a jamming signal, but rather, is captured (or re-routed) and prevented from reaching the intended base station, thereby disallowing the completion of the call. This technology permits calls by known users (*i.e.*, prison-authorized cell phone numbers) by handing them off to the network, and prevents others by denying access to the network. It is unclear whether or how well these systems can discriminate among prison-authorized cell phone numbers and "unknown" phones to avoid capturing/cancelling calls that do not involve inmates.

As a tool to deal with contraband cell phone use, some of these systems employ passive technology that detects cell phone use and collects data from active cell phones. Some systems deny access to calls from numbers they do not recognize. Other techniques redirect cell phone transmissions to portable antennas set up specifically around the prison, and only allow communication from prison-authorized cell phones to be forwarded to carrier cell towers. Denial of service approaches use electronic hardware located in the vicinity of the cell phone user to "spoof" the cell phone into thinking it is communicating with the carrier tower. The cell phone user receives a message that indicates that there is no service available. This type of denial of service system operates independently of the carrier and spoofs all cell calls.

In an effort to eliminate the unauthorized use of cell phones in Maryland State prisons, in 2009 the Maryland Department of Public Safety and Correctional Services hosted a demonstration of various non-jamming technologies, including managed access systems.[18] In January 2010, they issued a follow-on report.[19] The demonstration showed, among other things, that: (1) Several intelligence gathering abilities could be implemented depending upon specific laws governing each State; and (2) the types of technology tested could allow certain phones to operate and allow 911 calls to be processed.[20]

Detection

Detection is the process of locating, tracking, and identifying various sources of radio transmissions—in this case, cell phone signals. Detection, or direction finding, is used in a wide variety of applications including, for example, cell phone assignments, the location of 911 emergency calls and marine distress calls. For accurate position location in an environment such as within a prison facility, detection technology triangulates a cell phone signal and requires the use of correctional 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 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. These systems can only detect a cell phone when it is in use—either placing or receiving a call. The devices are generally "passive" receive-only devices, and do not necessarily require any authorization or license for the equipment or the user to operate.

Additionally, the Maryland Department of Public Safety and Correctional Services demonstration included a number of detection technologies, and the report concluded that there were varying degrees of accuracy in terms of cell phone detection based upon each vendor's technological abilities.[21]

Request for Comments

NTIA requests comment on the questions below in order to assist in evaluating technology solutions to prevent contraband cell phone use in prisons. These questions are not a limitation on comments that may be submitted. When making reference to studies, research, and other empirical data that are not widely published, commenters should provide copies of the referenced material with the submitted comments. Comments will be posted on the NTIA Web site for viewing at *http://www.ntia.doc.gov.*

1. Technologies or Approaches

We have initially identified three broad categories of approaches that provide solutions for preventing contraband cell phone use: jamming, managed access, and detection. Are these characterizations accurate and complete? Are there technologies other than these categories, and if so, how do they work? What approaches can be taken to jam within irregular structures such as prisons, within indoor and outdoor areas and within rural versus urban settings? What specific types of managed access and detection techniques are available? What risk does each system pose to legitimate cell phone use by the general public outside the prison? What risk does each system pose to public safety and government use of spectrum? How can any of the foregoing risks be mitigated or eliminated? What are the benefits and drawbacks of implementing these techniques? Are certain systems more suitable for certain prison environments or locations? To what extent does the installation of each system require a

[15] Letter from Chris Fischer, President, Association of Public Safety Communications Officials International, Inc. to Michael Copps, Acting Chairman, Federal Communications Commission, March 13, 2009, available at *http://files.ctia.org/pdf/CTIA_Position_Papers_Letter_APCO_Re_cell_phone_jamming_3_13_09.pdf;* CTIA Policy Topics, Contraband Cell Phones in Prisons, available at *http://www.ctia.org/advocacy/policy_topics/topic.cfm/TID/58.*

[16] *See, e.g.*, Wired, *Prison Mobile Phone Debate Jammed up in the System*, Ryan Singel, March 15, 2010, available at *http://www.wired.com/epicenter/2010/03/prison-mobile-phone-debate-jammed-up-in-the-system/.* Also, a recent survey at the International CTIA Wireless Conference showed that nearly three-quarters of respondents favor jamming of cell phones in prisons. *See http://www.enrthtimes.org/articles/show/survey-at-international-ctia-wireless,1231600.shtml#ixzz0ju7Exz3B.*

[17] *See, e.g.*, Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Devon Brown, Director, District of Columbia Department of Corrections, DA 09–354, Feb. 18, 2009, available at *http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-09-354A1.pdf;* Letter from James D. Schlichting, Acting Chief Wireless Telecommunications Bureau, Federal Communications Commission to Howard Melamed, CEO, CellAntenna Corporation, DA 09–622, March 17, 2009, available at *http://fjallfoss.fcc.gov/edocs_public/attachmatch/DA-09-622A1.pdf.*

[18] Maryland Department of Public Safety and Correctional Services, *Overview of Cell Phone Demonstration*, available at *http://www.dpscs.state.md.us/publicinfo/media/pdf/FinalReport_2008-09-10.pdf.* One managed access technology was demonstrated and operated pursuant to an experimental license granted by the FCC for this occasion.

[19] Maryland Department of Public Safety and Correctional Services, Non-Jamming Cell Phone Pilot Summary, Jan. 20, 2010, available at *http://www.dpscs.state.md.us/media/Cell-Phone-Pilot-Summary_Final.pdf.*

[20] *Supra* note 18 at page 5. The conclusions reached from the demonstrations were that each State will have to identify its own specific needs since the technology is such that one solution may not work for every facility within a given State. *Supra* note 18 at page 6.

[21] *Id.*

customized approach for each prison? How disruptive is the installation process? What approaches can be used in the implementation of systems employing detection techniques? How does each system provide for completion of critical calls or radio communications such as those from public safety officers (including use of handheld two-way radios) or 911? What ability does each of these technologies possess for upgrades to include new frequency bands, technologies, modulation techniques, etc. as they are introduced into the marketplace? How quickly can they be upgraded?

2. Devices and Frequency Bands

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

Do, or will, the technologies identified above effectively cover all of the bands likely to be used for commercial wireless services and how do, or will, they do so? Specifically, which frequency bands does each approach currently best address, and which could they best address in the future? How can the technologies prevent an inmate from communicating with a device employing proprietary technology (*e.g.*, SMR radios)? Will the technologies deal with phones that plan to operate in other bands where new services will be offered in the future, such as in the 700 MHz band? What will be necessary to extend the capabilities of the technologies to new bands (new hardware or software, new antennas, agreements, etc.)?

3. Interference to Other Radio Services

Avoiding interference to authorized cell phone reception E83A; as well as other radio services outside the cell phone bands E83A; is a critical element in evaluating the various technologies. The longstanding radio spectrum regulation principle, embodied in the Communications Act of 1934, is to preclude harmful interference and not to block access to or receipt of information transmitted wirelessly.[22] In addition to producing emissions in specific bands and within specific areas to deny service, jamming systems also produce unwanted signals outside of their intended operating bands and are not naturally confined to a prescribed area. These signals have the potential to produce interference to other radio services operating in numerous frequency bands (including Federal Government operations) and outside of the prison facility.

If jamming configurations are set up properly (that is, based upon site-specific radio frequency (RF) engineering), can these unwanted emissions be reduced or eliminated at a distance that is based on jammer and site parameters at each individual prison? Is the location of the prison (rural versus urban) also a factor, and if so, why and how would that affect the feasibility or implementation of a jamming system?

What jammer system parameters (*e.g.*, power levels, modulation, antennas) can be used to control out-of-band (OOB) and unwanted emissions? Which of these parameters have the greatest impact on the effectiveness of the jammer transmitter? Swept frequency techniques are often employed in jamming systems.[23] What other jamming techniques can be employed to disrupt wireless communication systems? Are filters commercially available that could be used to reduce the OOB and unwanted emission levels from jammer transmitters? Commenters should provide details on the specifications for the filter (*e.g.*, manufacturer, model number). Will jamming multiple frequency bands simultaneously affect the emission characteristics of the jammer transmitter (*e.g.*, generation of intermodulation products)?

NTIA also seeks comment on other techniques that cell phone jammers can implement to reduce interference to other radio services. Can spectrum sensing be used in conjunction with jamming techniques to reduce the transmit duty cycle of the jammer transmitter?[24] Are there variable strength cell phone jammers that are capable of dynamically adjusting their strength? What are the factors that can vary the signal strength of the jammer if it is putting out too much power?

The emissions from jammer transmitters can potentially cause interference to receivers beyond the intended jamming area. A critical parameter necessary to assess the potential impact to a receiver is the interference protection criteria (IPC).[25] There are currently no industry-adopted or Federally-mandated standards for in-band interference from other systems to wireless mobile handset receivers. How should the IPC for these handsets be established? What IPC values should be used for assessing potential interference to these handset receivers?

An approach to regulating jammer transmitters could be to establish a distance at which the jammer signal must be below a specified level necessary to protect in-band and out-of-band receivers. An alternative approach could be to specify maximum allowable equivalent isotropically radiated power (EIRP) limits necessary to protect in-band and out-of-band receivers as a function of frequency. Since the variations in the jammer configurations, effects of multiple jamming transmitters, structural characteristics of buildings, and propagation factors will be different depending on the installation and the facility, can analytical analysis techniques be used to develop the distances or EIRP limits necessary to protect in-band and out-of-band receivers? If analytical analysis techniques can be employed, explain the methodology to be used and all appropriate conditions considered in the analysis, including, but not limited to, propagation loss modeling and

[22] *Supra* note 13.

[23] A swept frequency jammer transmitter operates by repetitively frequency-sweeping (referred to as chirping) a carrier wave signal across the bands to be jammed.

[24] The duty cycle is the fraction of time that a transmitter is in an "active" state.

[25] The IPC is a relative or absolute interfering signal level at the receiver input, under specified conditions, such that the allowable performance degradation is not exceeded.

building attenuation modeling. How should the effect of multiple jammer transmitters and antennas be taken into consideration? Are there other approaches that can be used to regulate jammer systems?

The impact of jamming signals would also depend on the prison environment. Outside of the facility, will the variations in the measured levels of the jammer transmitter signal make it difficult to distinguish such a signal from the cellular and PCS signals in the environment, for example? If so, is this problem exacerbated in areas where there is a high density of cellular and PCS signals, such as in and around an urban prison location. The variations in the measured jammer transmitter signal levels could likely be due to propagation effects and building attenuation losses that will be different at each facility and for each jammer installation. Furthermore, depending on the relative signal levels, it can be difficult to differentiate between the measured jammer transmitter signal and the cellular and PCS signals. Given variations in signal levels and the potential to distinguish the jammer signal from the background signals, is it possible to measure accurately the jammer transmitter signal outside of a facility?

Within a facility, is it possible to distribute the jammer transmitter power spatially across an array of antennas (or, in some cases, lossy cables) in order to better control and provide lower power density around individual antennas than could be produced if a single antenna were used to radiate a high-power signal? What techniques can be employed in the design of the jamming system to reduce the potential for interference to in-band and out-of-band receivers? Can restrictions be placed on the jammer transmitter antenna height to minimize the potential for interference outside of the area that is being jammed? Is it possible to employ directional or sector antennas to focus the jammer transmitter signal in the intended areas within a facility while minimizing the signal levels outside of the facility? Can down tilting the antennas be used to minimize the jammer transmitter signal level at the horizon? What restrictions can be placed on the antennas without impacting the effectiveness of the jamming system?

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

Do other technologies or approaches have the potential to interfere with other authorized radio services within the same bands or adjacent bands? If so, under what conditions and how can an operator mitigate interference? In some of the bands identified above, public safety frequencies are interleaved or operate in close proximity with frequencies used by mobile devices, for instance in the 800 MHz SMR and 700 MHz bands. How will internal and external land mobile systems, including systems used by the prisons themselves, as well as other public safety operations, be protected? Are there other radio communications systems within prisons that could also experience interference, such as internal private land mobile systems used by prison officials or medical telemetry devices in prison infirmaries? [26]

4. Protecting 911 Calls and Authorized Users

The preservation and protection of calls to 911 from cell phones is a paramount concern as more consumers rely on mobile devices.[27] The number of cell phones calling 911 has been steadily increasing as more consumers are using them. The National Emergency Number Association estimates that wireless telephone users account for nearly half of the calls to 911.[28] Jamming radio signals in and around prisons cannot differentiate between normal cell phone traffic and 911 calls.[29] Managed access systems, however, can be selective and designed to ignore 911 calls (*i.e.*, letting them connect to the network), and detection systems typically use passive devices that do not affect transmission or reception. How are 911 calls preserved in areas around the prisons where the public is making a call to 911 if they come in proximity to the prison? Are there any other technologies identified that can protect 911 calls and how do they do so?

Wireless consumers expect their wireless calls to be completed without being dropped or busy. In and around prisons, consumers and public safety officials, as authorized users of the system, will expect their wireless devices to communicate. How are authorized users allowed to make calls with the technologies described? If the caller passes through a "dummy" cell site set-up within the prison vicinity, will the call go through if a call is initiated within that cell (*e.g.*, will it result in a busy signal or a dropped call)? Are calls handed off to the carrier cell site and network? How does managed access work if the caller is an authorized user, but the phone number is not known (*i.e.*, in the database of authorized users) to the managed access system?

5. Cost Considerations

The cost of preventing cell phone use in prisons is a factor that must be considered and varies according to the type of technology, area to be covered, and additional features. What factors impact the cost of implementing each of the technologies as described above? Are there on-going or recurring costs associated with each? To what extent will installation costs vary in light of the particular characteristics of each prison (e.g., geographic setting)? What

[26] State governmental entities are eligible to hold authorizations for frequencies in the Public Safety Pool to operate radio stations for transmission of communications essential to its official activities. *See* 47 CFR 90.20. BOP uses medical telemetry at Federal Medical Centers and at some non-medical prisons. Additionally, some inmates have devices that are monitored remotely by local hospitals.

[27] More than one in five households have discontinued wireline service (or chosen not to use it) and rely solely on wireless communications as their primary telephone service. See Centers for Disease Control and Prevention, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July-Dec. 2008*, May 6, 2009, available at *http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless200905.pdf.*

[28] National Emergency Number Association, Cell Phones and 911, *http://www.nena.org/cellular-wireless-911. See also* FCC Consumer Facts, Wireless 911 Services, available at *http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html.* As a case-in-point, there has been a sharp increase by residents of Jefferson County, Arkansas dialing 911 from cell phones, where there are three State prisons. Nearly 70 percent of calls to 911 in 2008 were made from a cell phone. *See* Arkansas Daily-Gazette, *Cell Phone Calls Place Burden on Ark. 911 Dispatch Center*, Mike Linn, Oct. 5, 2009, available at *http://www.firerescue1.com/fire-products/communications/articles/595629-Cell-phone-calls-place-burden-on-Ark-911-dispatch-center/.*

[29] However, at some distance away from the prison which is unique to each prison's features and jammer set-up, jamming contraband cell phone signals should not affect authorized or 911 calls.

characteristics are most likely to affect costs? What are the ancillary costs for each type of approach (e.g., maintaining network connectivity for managed access systems, resources required to physically locate the phone for detection/location systems such as canines, staff time, etc.)? Are there typical costs or a range for each, and if so, what are they? Is training required for prison staff to properly operate the equipment? What staff costs are associated with each technology?

6. Locating Contraband Phones

In order to completely eradicate contraband cell phone use, the cell phone must be physically located and removed, which can be labor-intensive. Inmates may use them for a short period of time and turn them off and then move them, making the devices more difficult to locate. Jamming cannot identify the specific location of a contraband cell phone. How do managed access and detection technologies locate a cell phone caller? What software and hardware is needed? How accurate are detection technologies? With the insertion of GPS chip-sets into mobile devices, are cell phone locations easily identifiable through managed access or are other means necessary (*e.g.*, hardware or software)? Do managed access and detection technologies have the capability of providing intelligence-gathering information for prison officials, and if so, what type of information? What other means are necessary to physically locate the phones once a position is known?

7. Regulatory/Legal Issues

The Communications Act of 1934 established the FCC and set specific rules on wireless radio services.[30] Both the operation of mobile wireless devices, and effective means and solutions to deny the use of them have regulatory and legal implications. The FCC has primary responsibility for regulating spectrum issues for the types of systems typically used within the State and local prisons and jails (for example, private internal radio communications and commercial systems used by prison staff). NTIA, on behalf of the President, authorizes the use of the radio frequencies for equipment operated by Federal entities, including the BOP.[31]

While the Communications Act prevents the FCC from authorizing jamming or other acts of intentional interference to the radio communications of authorized stations, those same provisions do not apply to the Federal government itself. Therefore, NTIA is not limited in its authority to permit jamming at Federal prison facilities. We seek comment on State/local or Federal laws, rules, or policies that need clarification or that may hinder deployment of any of these technologies or others that may be raised by commenters. These might include not only radio regulatory issues, such as the approval necessary to operate or conduct experimentation and demonstration, but also ancillary issues such as the privacy and legal implications of trap-and-trace technologies? What agreements, agency relationships, or licensing requirements between the prison, service provider, and access provider would be required for temporary or experimental demonstration or for permanent operation?

8. Technical Issues

The identification of technical issues is another factor in investigating and evaluating contraband cell phone use in prisons. Are there any technical issues to be considered for the technologies identified above? For example, the actual range of a jammer depends on its power, antenna orientation, and the local environment (size and shape), which may include hills or walls of a building (that could be made of a variety of materials) that block the jamming signal. How accurate are the location technologies? Does each site need specific RF engineering for each of the approaches? How do the technologies allow authorized users, including 911 calls, to be protected? How are different modulation schemes or channel access methods (for example, Global System for Mobile Communications—GSM, or Code Division Multiple Access—CDMA) handled for each category and does the solutions depend on the type of access method that the wireless carrier is using?

Text-messaging continues to increase as a form of communication from hand-held wireless devices.[32] Wireless hand-held devices in the possession of prison inmates afford them this option as an alternative to talking. Is there a need to differentiate between voice and data, such as text messages, and are the technologies discussed above effective against data use by prison inmates? Does shorter air-time use from text messaging present problems with detection and/or capturing the call and ultimately locating the phone? Will the technologies identified above be effective against high-speed, high-capacity data formats, such as Long Term Evolution (LTE) for devices that are expected to operate in the 700 MHz band?

Please note that all comments received will be posted on NTIA's Web site. Commenters that submit any business confidential or proprietary information in response to this notice should clearly mark such information appropriately. Commenters should also submit a version of their comments that can be publicly posted on NTIA's Web site.

Dated: May 7, 2010.

Kathy D. Smith,

Chief Counsel.

[FR Doc. 2010–11350 Filed 5–11–10; 8:45 am]

BILLING CODE 3510–60–P

[30] For example, cellular service rules are set forth in 47 CFR parts 1 and 22; AWS in 47 CFR part 27; and SMR in 47 CFR part 90.

[31] *See generally*, NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management, Sept. 2009, Section 1, available at *http://www.ntia.doc.gov/osmhome/redbook/1.pdf*.

[32] CTIA estimates that the number of monthly text messages sent increased from 9.8 billion in December 2005 to 152.7 billion in December of 2009. *Supra* note 2. *See also* CNet News, *U.S. Text Usage Hits Record Despite Price Increases*, Marguerite Reardon, Sept. 10, 2008, available at *http://news.cnet.com/8301-1035_3-10038634-94.html*.

COMMODITY FUTURES TRADING COMMISSION

Sunshine Act Meeting Notice

AGENCY HOLDING THE MEETING: Commodity Futures Trading Commission.

DATE AND TIME: May 19, 2010 at 9:30 a.m.

PLACE: Three Lafayette Centre, 1155 21st St., NW., Washington, DC, Lobby Level Hearing Room (Room 1000).

STATUS: Open.

MATTERS TO BE CONSIDERED: Agenda: (1) Consideration of the trading of futures and binary options based on motion picture box office receipts and to gather the views of interested parties; and (2) Reestablishment of the CFTC Technology Advisory Committee.

CONTACT PERSON: Sauntia Warfield, Assistant Secretary, 202–518–5084.

SUPPLEMENTARY INFORMATION: The Commission is undertaking a review of issues related to the trading of futures or options related to motion picture box office receipts. The Commission will have oral presentations by panels of invited witnesses representing Media Derivatives Exchange (MDEX), Cantor Exchange (Cantor), segments of the motion picture industry, and other interested parties.

Appendix B
List of Commenters by Group[181]

Public Safety (Correctional, Governments, Associations, etc.)	Industry (Vendors, Consultants Manufacturers, etc.)	Wireless Providers (Carriers, Associations)	Others (Citizens, non-affiliated)
Association of Public Safety Communications Officials (APCO)	AirPatrol	AT&T	Art Beeler
B.B. Sixty Rayburn Correctional Center	Bahia 21	CTIA	Mike Kouri
Big Spring Correctional Center	Berkeley Varitronics Systems (BVS)	Sprint Nextel	Paul C. Kruger
California Department of Corrections and Rehabilitation	BINJ Laboratories (BINJ)	T-Mobile USA	Peter McDonald
Correctional Services of Canada	Boeing Company	Verizon Wireless	Roy Stratton
Dayton Correctional Institution	CellAntenna		Paul Velasquez
Kentucky Correctional Industries	Enterprise Electronics		Ann Worth
Madison Juvenile Correctional Facility	Global Tel*Link Corp (GTL)		
National Emergency Number Association (NENA)	ICSolutions		
Oklahoma Department of Corrections	ITT		
Rappahannock Regional Jail	ManTech International		
Rick Veach, Warden	Marcus Spectrum Solutions		
South Carolina Department of Corrections	Motorola		
State of Maryland/Department of Public Safety and Corrections	Research Electronics International (REI)		
Letter from Members of Congress, Honorable Rick Boucher and Honorable Bobby Rush	ShawnTech Communications		
	Tecore Networks		
	TruePosition		
	Try Safety First		
	Zocalo Data Systems		

[181] The comments are available at http://www.ntia.doc.gov/comments/100504212-0212-01/.

Appendix C
Vendors and Solutions for Contraband
Cell Phone Interdiction

Vendor	Technology(ies)	Web Address
AirPatrol	Detection	http://www.airpatrolcorp.com/
Bahia 21	Jamming, NLJDs, detection, managed access	http://www.bahia21.com/
Berkeley Varitronics Systems	Detection	http://www.bvsystems.com/Products/Security/Bloodhound/bloodhound.htm
BINJ Labs	Detection	http://www.binjlabs.com/index.html
Boeing	Hybrid	http://www.drti.com/
CellAntenna	Jamming, managed access	http://www.cellantenna.com/
Enterprise Electronics	Detection	http://www.eeontheweb.com/cell_phone_detectors.htm
ITT	Detection	http://iiw.itt.com/products/cellHound/prodCell.shtml
Research Electronics International	NLJDs	http://www.research-electronics.com/cgi-bin/main.cgi
Tecore Networks	Managed access	http://www.tecore.com/
Try Safety First	Standardized Protocols	http://trysafetyfirst.com/

Appendix D
Commonly Used Acronyms

APCO	Association of Public Safety Communications Officials
AWS	Advanced Wireless Services
BOP	Bureau of Prisons
BVS	Berkeley Varitronics Systems
DRT	Digital Receiver Technology
FCC	Federal Communications Commission
GPS	Global Positioning System
IPC	Interference Protection Criteria
ITS	Institute for Telecommunication Sciences
LMR	Land Mobile Radio
LTE	Long Term Evolution
NENA	National Emergency Number Association
NIJ	National Institute of Justice
NLJD	Non-Linear Junction Detector
NOI	Notice of Inquiry
NTIA	National Telecommunications and Information Administration
PCS	Personal Communications Services
REI	Research Electronics International
RF	Radio Frequency
SMR	Specialized Mobile Radio