Billing Code 3510-60-P

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 [INSERT DATE OF 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

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 website for viewing at 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 email 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 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]

---

[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.

[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

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

---

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.

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 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

---

[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.

[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.earthtimes.org/articles/show/survey-at-international-ctia-wireless,1231800.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.

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.

---

[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.

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 website 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 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)

[21] *Id.*

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 — as well as other radio services outside the cell phone bands — 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).

---

[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.

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 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?

---

[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.

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 anoperator 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

[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 C.F.R. Part 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.

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 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

---

[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.

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?

---

[30] For example, cellular service rules are set forth in 47 C.F.R. Parts 1 and 22; AWS in 47 C.F.R. Part 27; and SMR in 47 C.F.R. 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.

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 website. 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 website.

Dated: __May 7, 2010_____.

_____

Kathy D. Smith,
Chief Counsel.

[FR Doc. 2010-11350 Filed 05/11/2010 at 8:45 am; Publication Date: 05/12/2010]

[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.