Before the
NATIONAL TELECOMMUNICATIONS
AND INFORMATION ADMINISTRATION
Washington DC, 20230

In the Matter of	)	
	)	
Preventing Contraband Cell Phone Use in Prisons	)	Docket No. 100504212-0212-01
	)	
	)	

COMMENTS OF SPRINT NEXTEL CORPORATION

Sprint Nextel (Sprint) welcomes the opportunity provided by NTIA's Notice of Inquiry (NOI) to provide comments on technical approaches to preventing contraband cell phone use in prisons. Sprint appreciates the problems that have been raised regarding the contraband use of cell phones in prisons and supports efforts to eliminate them.

Sprint has been working within CTIA and with several industry partners to investigate and develop technology solutions that can be used to prevent contraband cell phone use in prisons. In particular, Sprint assisted with demonstrations of managed access technology to the Maryland Department of Public Safety and Correctional Services in September 2009 and December 2009. Sprint is also holding numerous discussions with several managed access technology vendors regarding additional demonstration projects.

The three broad categories of approaches being considered for preventing contraband cell phone use in prisons, aside from interdicting and confiscating unauthorized cell phones as they are brought into prisons, include: managed access, cell phone detection, and jamming. Sprint believes that managed access and cell phone detection systems offer the best potential solution to the problem, aside from interdiction and confiscation. Sprint has serious concerns with the ability of jamming technologies to avoid causing interference to legitimate communications users and to function effectively at reasonable cost. Sprint offers its views on each of these categories, while noting that future technology developments may offer additional approaches to denying service to contraband cell phones in prison environments.

Managed Access Systems. It appears that several managed access vendors have taken somewhat different approaches for managed access deployments. In general, however, they would all provide systems that intercept cell phone calls made within the confines of the prison. Calls that are determined to originate from previously-approved phones (for example, phones used by prison guards) could be permitted to access the base stations of nearby commercial mobile operators, while phones not previously approved would be denied access. In addition, calls to 911 emergency services, regardless of the cell phone user, could be permitted.

Sprint respectfully submits 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. Coordination would ensure

that signal levels and operating practices are adjusted so as to avoid callers outside the prison from being pulled into the managed access cell, while at the same time ensuring the cell phones users within the prison are captured and vetted by the managed access system. Because managed access systems likely would be built using base station equipment that commercial mobile operators use to serve cell phones today, it is likely that managed access systems can be deployed in virtually all traditional commercial mobile service frequency bands for reasonable cost. However, commercial terrestrial mobile communications are being introduced in additional spectrum bands creating the possibility of prisoners obtaining handsets using these new bands for conducting illicit communications.[1] Therefore, at least for a period of time, it may be appropriate that managed access systems be supplemented with cell phone detection systems that cover a wide range of frequency bands.

Detection Systems. Cell phone detection systems could be used to detect the presence of cell phone communications within the prison. The detection system could locate the source of the signal, and then additional actions could be taken. Such actions could include the activation of camera systems to record the activity in the area of the transmission or the immediate dispatch of correctional staff to locate the source of the communications. It could also include the identification of the cell phone electronic serial number (ESN) and a request to the appropriate mobile provider to deny service to that phone. Detection systems could also be used in conjunction with managed access systems to ensure that only cell phone calls made in near proximity to the detection system are subject to managed access restrictions.

Jamming Systems. As the NOI points out, the Communications Act currently prohibits the use of jamming systems by non-Federal entities. In addition, the Communications Act prohibits any person from causing willful or malicious interference to a licensed radio communication. Yet that is precisely the intent of using a cell phone jamming device. Although some parties have called for changes to the Communications Act to permit use of jammers in prisons, Sprint believes that those parties should instead focus on currently legal alternatives that do not pose an interference risk to public safety and commercial mobile users.

Numerous public safety and commercial mobile service providers have expressed concern about the interference that can be caused by jamming devices. In addition, today's jamming systems lack the capability to block all of the frequency bands that prisoners could use to conduct illicit communications, making their use ineffective. For example, jammers do not operate in the 800/900 MHz bands that Sprint uses for its iDEN network. Those bands contain both public safety and commercial operations in very close proximity to each other from a frequency standpoint, and any jamming device would likely disrupt both public safety and commercial communications at the same time. In addition, jamming systems disrupt all cell signals in a band and would not meet the needs of prison officials that want their employees to be able to use cell phones.

---

[1] Cell phones are available today for the Cellular (824-849/869-894 MHz), PCS (1850-1990 MHz), AWS-1 (1710-1755/2110-2155 MHz), SMR (806-824/851-869 MHz and 896-901/935-940 MHz), and BRS (2496-2690 MHz) bands. In 2011, cell phones are likely to be offered in the 700 MHz band (698-806 MHz). Some MSS operators have also indicated that they will deploy ancillary terrestrial component networks in the L-band (1525-1559/1626.5-1660.5 MHz), 2 GHz MSS (2000-2020/2180-2200 MHz), and Big LEO bands (1610-1626.5/2483.5-2495 MHz) over the next few years. Furthermore, similar voice and data devices can operate in the Family Radio (462.5625-467.7125 MHz), General Mobile Radio (462-467 MHz), Personal Radio (various frequencies), Amateur Radio (various frequencies), and unlicensed bands (various frequencies).

The recent NTIA measurements made of a cellular and PCS jamming system installed at the Federal Bureau of Prisons facility, in Cumberland, MD shows the potential for interference. NTIA's Report indicates that the jamming signal was routinely able to be detected and measured outside of the targeted jamming zone. In fact, even at the measurement point farthest from the jamming zone (location O-5, 131 meters from the center of the targeted zone and 127 meters from the edge of the targeted zone), which appears to be located at the boundary of the prison property, the jamming signal was as strong or stronger than the Sprint PCS signal on 1938.5 MHz intended to serve that area.[2] Under such conditions, it is likely that cell phone users would receive harmful interference. Indeed, to avoid interference, cell phones generally require that the cell phone signal be several dB stronger than any interference or radio noise level. Thus, interference likely could extend well beyond the 131 meter distance that was measured and the boundaries of the prison facility.[3]

Testing of cell phone jamming was conducted on Tuesday, February 16, 2010 and Wednesday, February 17, 2010, at the Cumberland facility. No advance notice was provided to the wireless industry, and thus no cell phone operator had the opportunity to conduct simultaneous testing to determine whether the jamming testing was causing interference to its network, even though the wireless industry had repeatedly raised concerns about the potential for such interference.

After learning about the testing, Sprint analyzed data gathered from its cell sites in the Cumberland area to see if there was any sign of interference. Our analysis indicates that such interference may have occurred to cell phones attempting to communicate with a cell site located approximately 5 km (3 miles) away and 390 meters (1290 feet) higher in elevation to the northeast of the jamming zone. This cell site provides coverage in the area immediately north of the jamming zone, including the Cumberland Airport. Other cell sites in the area, located farther from the jamming zone, did not appear to receive similar interference.

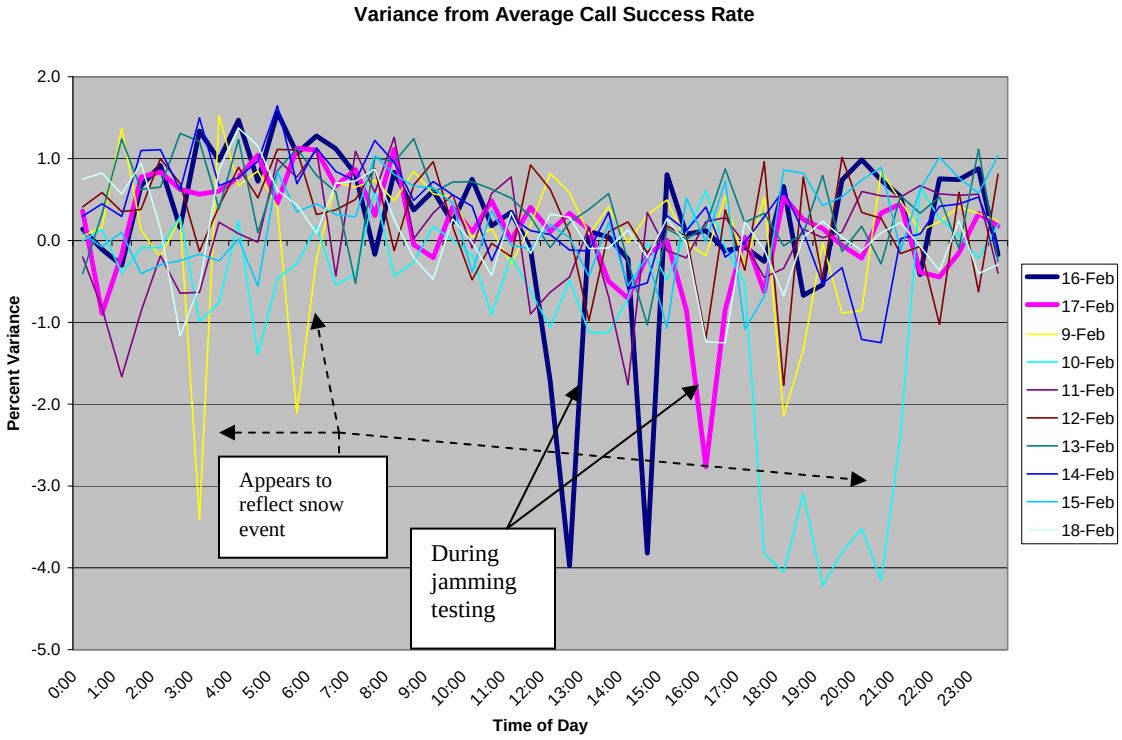
We understand that the jamming system was turned on, and NTIA took readings, on both days during 15-20 minute intervals. Our cell sites collect information on several performance parameters, such as successful call completion, minutes of use, and dropped calls in 30 minute intervals, so it is it not possible to precisely coordinate any interference with the timing of the jamming testing. However, during the testing period there was a definite trend upward in the rate of dropped calls and a trend downward in successful call attempts.

Analysis of data gathered during the jammer testing period was compared to data gathered during a two-week period surrounding the testing. Such data was limited to Monday-Friday operations, since weekend traffic patterns tend to differ significantly from work-week day traffic. The following graph shows the variance from the average call success rate by time of day for the period from February 9-18.

---

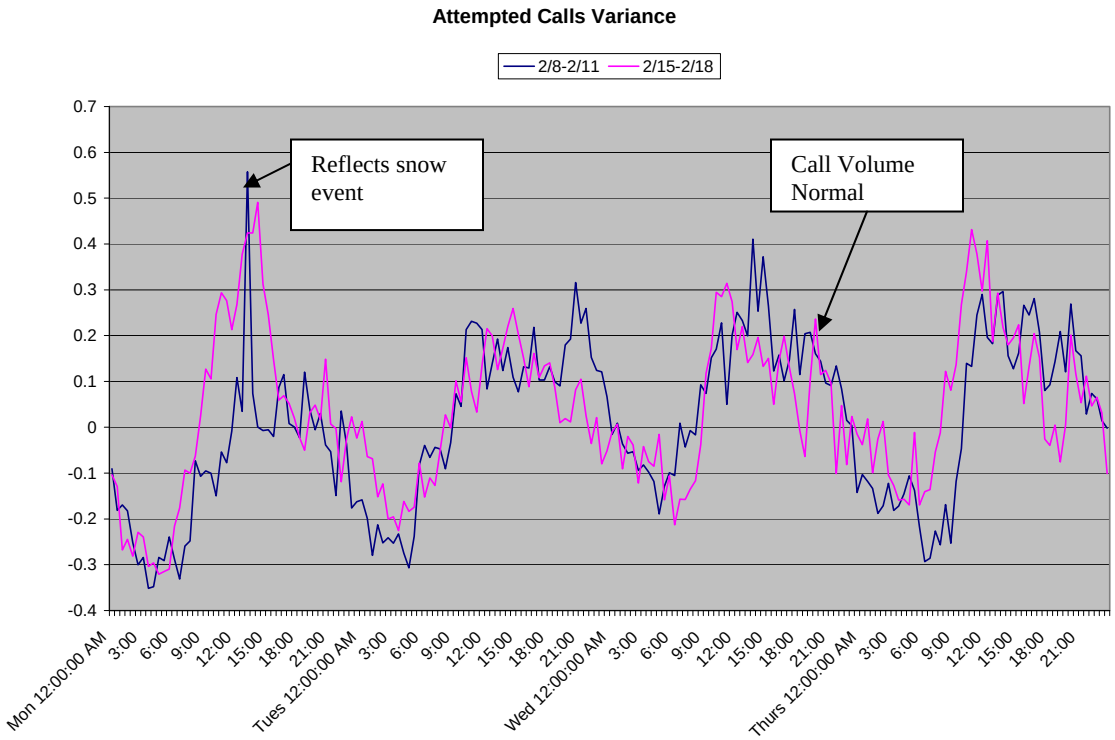
[2] See Figures 20 and A-18 of NTIA Report TR-10-466. In that Report, the measured signal level with the jamming system on was 3-6 dB higher than with the jamming signal off. A 3 dB increase in measured signal level would indicate that the jamming signal was approximately equal in power to the cell phone signal.

[3] In fact, as discussed herein, Sprint's PCS network in Cumberland, MD experienced a higher than normal amount of dropped calls and a lower than normal call success rate during the time periods the jamming was conducted.

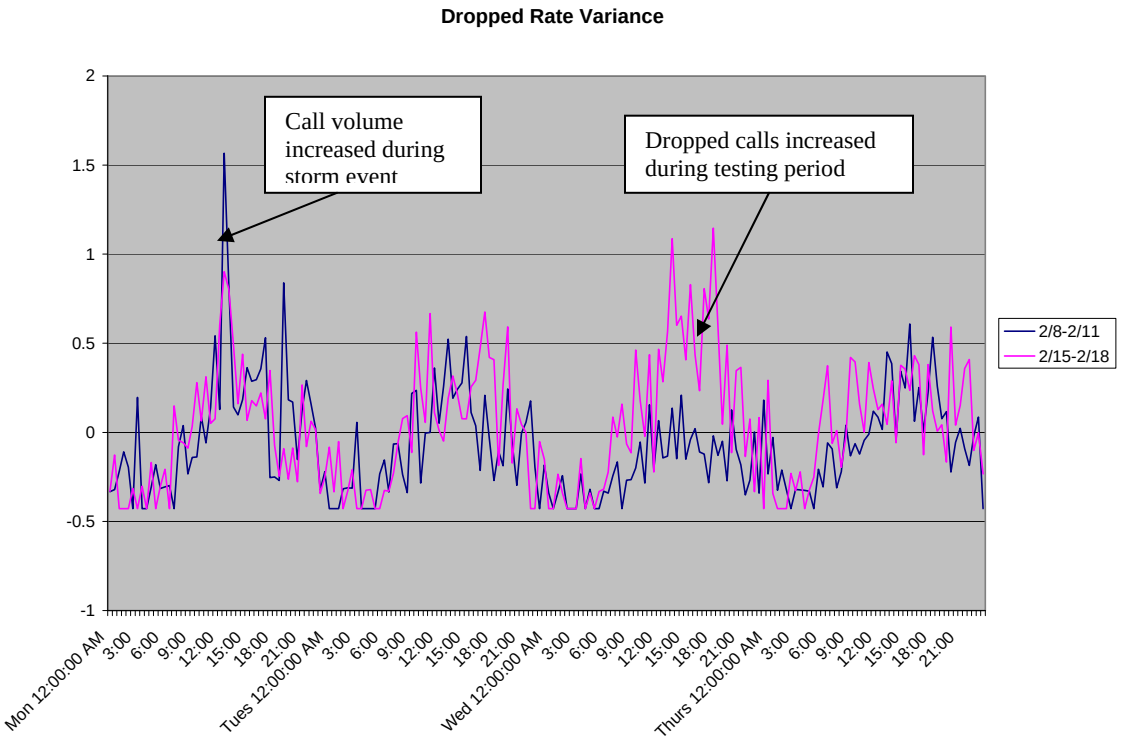


This graph illustrates major issues in the afternoons of both of the jammer testing days, February 16-17, as points in the negative below zero are poorly performing compared to the average, and points in the positive are better than average. The other two poorly performing days in this data collection period occurred during the early morning and evening hours of February 9-10, during a period of significant snow in the Cumberland area.

Similar analysis was made of attempted call volumes during this two-week period. The graph below shows that call volume was 50% higher that normal on February 9, during the snow event, which could have resulted in the decreased call success rate on that day. However, call volume during the jammer testing was within the normal range (which varies depending on time of day). In other words, the data indicates that, with normal call volumes during the testing period, call completion rates dropped significantly thus suggesting that the jamming testing may have caused interference with normal network operations.



Additionally, the dropped call rate shows a significant increase during the period the prison performed the cell jamming tests. The dropped call rate could be reflective of the jamming tests taking place at the prison, as drops reflect the mobile no longer being able to communicate with the cell site, which would imply that the cell signal had been blocked by the jamming signal. While call attempts in the graph above reflected normal patterns, there was a significant increase in the amount of dropped calls during the afternoon of February 17. The dropped call amounts were elevated from 1pm to 6pm on February 17, when the success rate in the previous graph also showed a negative trend. Finally, the success rate at 12:30pm and 2:30pm on February 16 also reflect a definite network interruption.



It is impossible to determine definitively *after the fact* whether the cell phone jamming conducted at Cumberland resulted in interference only to the operations of cell phones by prisoners or whether such interference also occurred outside the prison. NTIA measurements were only made on the ground in the vicinity of the jamming zone. Furthermore, the NTIA Report clearly indicates that "Analysis of the in-band (cellular and PCS) potential for harmful interference, if any, of the jammer emissions that were observed outside the jamming zone was beyond the scope of this report." Given the strong jamming signals that NTIA measured at a significant distance from the jamming zone, the mountainous terrain surrounding that zone, the long distances that cell sites in that area are attempting to serve, and the network data provided above, it is quite possible that NTIA's jamming testing caused interference well outside the jamming zone.

The NTIA Report clearly shows that the jamming signal for this test was not able to be contained to the jamming zone. Furthermore, the Report indicates that the RF environment that would occur from the deployment of jamming systems could vary greatly from installation to installation. Thus, interference to legitimate commercial and public safety communications from jamming systems is a distinct possibility at many prison facilities. Given the availability of alternative technologies that are not likely to cause interference, Sprint supports the strong preference that was given in the Conference Report to the Department of Commerce FY 2010 Appropriations for non-jamming technology solutions.[4]

[4] H.R. Conf. Rep. No. 111-336 (2009), Division B, Title 1, Page 619. "The conferees strongly urge the NTIA, in coordination with the FCC, to investigate and evaluate detection or other technologies that do not pose a risk of negatively affecting commercial wireless and public safety services in areas surrounding prisons."

Conclusion. Sprint appreciates the opportunity to comment on possible technical solutions to the problem of contraband cell phones in prisons. We believe that several technologies are available that can effectively address this problem without negatively affecting commercial wireless and public safety operations; however, current jamming technology is likely to cause a significant negative impact to a variety of communications users and be an ineffective solution to the problem.

Respectfully submitted,

/s/

Lawrence R. Krevor
Vice President, Government Affairs
Richard B. Engelman
Director, Government Affairs

SPRINT NEXTEL CORPORATION
2001 Edmund Halley Drive
Reston, VA 20191
(703) 433-8124

June 11, 2010