Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In the Matter of	)	
	)	
Notice of Inquiry Regarding Contraband Cell Phone Use In Prisons	)	Docket No. 100504212-0212-01
	)	

COMMENTS OF VERIZON WIRELESS

Verizon Wireless hereby submits comments in response to the National Telecommunications and Information Administration's ("NTIA") Notice of Inquiry ("NOI") seeking comment regarding technical approaches to preventing contraband cell phone use in prisons.

As discussed herein, managed access systems are far superior to jamming systems for controlling contraband cell phone use by prisoners. Managed access is the only technical choice that can properly balance the needs of prison officials, the public, public safety users of wireless telecommunications, and wireless service providers without causing harmful interference to wireless networks in the vicinity of the prison. For this reason, NTIA should recommend managed access as the superior technology choice in its report to Congress.

I. BACKGROUND

Last December, Congress included language in the Conference Report to the Department of Commerce fiscal year 2010 appropriations directing NTIA, in coordination with the FCC, Bureau of Prisons ("BOP") and 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."[1] Congress "strongly urge[d] 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."[2]

On February 17, 2010, NTIA, in conjunction with the BOP, conducted a test of jamming equipment at a Federal prison in Cumberland, Maryland. For the test, a jammer transmitter and antennas were installed inside a two-story cinderblock building with several windows. The jammer used was designed to operate on cellular (869-894 MHz) and PCS (1930-1990 MHz) frequency bands. Measurements of the jammer emissions were taken at 4 locations inside the building and 7 locations outside the building. After the test, NTIA published a technical report analyzing the emission levels of the jammer,[3] and a technical memorandum making an "initial assessment" of the potential impact of the jammer on selected receivers.[4]

In the Emission Report, NTIA noted that jammer power was measurable at the furthest point (127 meters) where measurements were taken away from the building and at all other sites where measurements were taken inside and outside the prison building.[5] In the Technical Memorandum, NTIA found that the jammer could cause some impact to LMR receivers at the

---

1 H.R. Conf. Rep. No. 111-336 (2009), Division B, Title I, at 619.

2 *Id.*

3 Frank H. Sanders and Robert T. Johnk, "Emission Measurements of a Cellular and PCS Jammer at a Prison Facility," NTIA Report TR-10-466, May 2010 ("Emission Report").

4 Edward F. Drocella, "Initial Assessment of the Potential Impact from a Jamming Transmitter on Selected In-Band and Out-of-Band Receivers," NTIA Technical Memorandum 10-468, May 2010 ("Interference Memorandum").

5 Emission Report at xi, 1, 6-7, 17 (Figure 19).

prison and GPS receiver use in and around the facility. NTIA noted that by using a diplexer, the risk of interference to these receivers would be minimized. NTIA did not analyze the impact of the jammer on cellular and PCS receivers, stating that there are no currently adopted standards for in-band interference to such receivers. NTIA, however, found that based on the field measurements observed outside the facility, variations in the measure signal levels of the jammer transmitter "can make it difficult to distinguish the jammer transmitter signal in the environment. Moreover, depending on the relative signal levels it can be difficult to differentiate between the measured jammer transmitter signal and the Cellular and PCS signals."[6] NTIA also found that factors such as variations in jammer configurations, the effects of multiple jamming transmitters, structural characteristics of the buildings, propagation factors, and the area where the prison is located (for example, locating jammers in a metropolitan area with a high density of cellular and PCS users) can also affect the interference potential of jammers.[7]

II. DISCUSSION

Verizon Wireless shares the concerns of prison officials, Congress, and others regarding the use of contraband cell phones by inmates in Federal and State prisons. Verizon Wireless, along with CTIA, has been a willing and active participant in efforts to find solutions to the inmate cell phone usage problem and supports NTIA's effort to study technical solutions and report the findings to Congress.

To assist in this effort, Verizon Wireless asked telecommunications engineering consultant, VComm, L.L.C. ("V-Comm"), to review the NTIA test results, Emission Report and

---

6 Technical Memorandum at iv.

7 *Id.*, at iii and iv.

Technical Memorandum, and analyze the potential impacts to commercial wireless operations. V-Comm also assessed jamming[8] and managed access[9] technical alternatives for preventing inmate cell phone use.[10] V-Comm's analysis leads to three primary points relative to jamming and managed access: (1) the NTIA jamming test shows that even a simple, small scale jammer can create a significant threat of harmful interference to wireless carrier and public safety networks outside the grounds of a prison facility; (2) that the impacts of jamming wireless signals become more complex when considering the impacts to multiple frequency bands and network configurations employed in commercial wireless and public safety networks; and (3) the best way to stop contraband cell phone use and avoid the harms associated with jamming is to implement managed access.

---

[8] The NOI describes jamming as the intentional radiation of electromagnetic energy on the same radio frequencies as the cell phone for the purpose of disrupting the use of the cell phone. NOI at 4.

[9] The NOI describes managed access as a system of receivers that capture calls and prevents unauthorized transmitters from accessing carrier networks. Calls from authorized devices would be allowed to access carrier networks based on parameters set by prison officials working with the system operator. Such systems can be set up to allow 911 calls to be completed and can be equipped to gather intelligence about the calls being attempted, depending on State laws. NOI at 5.

[10] V-Comm's analysis is the basis for much of these comments and is attached as Appendix A to these comments. Mike Katra and Sean Haynberg, "NTIA Prison Jammer Study," June 11, 2010 ("V-Comm Study"). V-Comm has extensive experience in analyzing interference in various spectrum bands and working with all commercial wireless technologies. For this reason, V-Comm has been relied upon by carriers and the FCC for analyzing interference in a number of FCC and court proceedings. *Id.*, at 16.

A. The NTIA Jamming Test Results Prove that Jammers Will Cause Harmful Interference to Commercial Mobile Networks.

V-Comm concludes that the signal measurements from the NTIA jamming test taken at the furthest distance outside the prison from the jammer location are strong enough to cause harmful interference to commercial mobile subscriber devices. To reach this conclusion, V-Comm noted that signal levels measured were -50 dBm/MHz at a distance of 430 feet away from the jammer. VComm also noted that measurements were not taken at points further away from the prison, but that the jammer signal levels will continue to propagate well beyond 430 feet.[11]

Cellular devices operate with low noise figures and in high fading environments. Because cellular device sensitivities are very low, they typically operate at signal levels well below the -100 dBm level. This is particularly true in rural areas, where devices operate at lower signal levels (both because cell towers tend to be farther apart in such areas and because external noise tends to be lower). Moreover, broadband data devices operate with higher order modulation making them even more sensitive to interference.[12]

The signal levels measured 430 feet from the prison are therefore strong enough to easily overpower and jam the signals that devices typically receive from cellular base stations. Because the jamming signal will propagate at levels stronger than commercial wireless network signals at distances well beyond 430 feet, a simple jammer configuration similar that used in the NTIA test will cause harmful interference to wireless signals well beyond prison boundaries.

---

[11] V-Comm Study at 3.

[12] *Id.*

B. The Impacts of Jamming Are Even More Significant Considering the Complex Environment in which Jammers Will Operate.

V-Comm analyzed the likely impacts that jamming wireless signals in prisons will have on wireless networks operating in the vicinity of prisons and concluded that those impacts will be far-reaching, and that jamming is far more complex than prison officials and others may realize. In particular, V-Comm made the following findings:

- For jammers to be effective, they need to block all spectrum bands used today and in the future – otherwise savvy prisoners will migrate to devices that use un-blocked bands.[13]
    - For example, some smart phone devices will automatically switch to wi-fi when commercial wireless signals are not available, so wi-fi signals must also be blocked.
    - Some wi-fi bands, however, are shared with other services, such as Government Radar Service (which shares 5 GHz bands with wi-fi), so jamming these bands will interfere with Government Radar Service.
- Public Safety radios operate in the 800 MHz spectrum adjacent to the cellular A band and interleaved with the SMR/LMR 800 MHz bands used by Sprint Nextel.[14]
    - Jamming the cellular A band therefore can cause interference to Public Safety and jamming the bands used by Sprint Nextel will also jam the signals used by Public Safety radios.
    - Public Safety radios also operate in the 700 MHz bands, so jamming those bands will also interfere with Public Safety radios.
- Prisons are not designed or able to prevent jamming signals from propagating outside prison boundaries.[15]
    - Prisons typically have windows, door openings, air ducts, and open air courtyards, all of which will be sources of high potential signal leakage.

---

[13] *Id.*, at 4.

[14] *Id.*, at 5.

[15] *Id.*, at 6.

- This leakage will result in harmful interference to wireless networks operating in the vicinity of the prison.

- Jamming signals effectively is made more complex by the variability of wireless networks.[16]

  - Wireless networks are constantly evolving; using more and more frequency bands, technologies, and configurations.
  - Wireless networks also operate at different signal strengths depending on system loading conditions at different times of the day.
  - Wireless networks are configured with different RF designs with base stations that may be close to or far away from prison facilities, resulting in signal strength variances for each provider network.
  - Wireless technologies have different interference tolerances.
  - Jammer systems will have to overcome each of these variances in order to be effective.

- Jammers cannot block service from nearby base stations.[17]

  - Base stations located near prisons will result in strong signals in the -30 to -10 dBm range.
  - To block such signals, jammers will have to transmit at very high power levels and will require a significant number of antennas located throughout the prison facility, thereby increasing complexity and cost.
  - These high power levels needed to overcome a single nearby base station, will cause harmful interference to co-channel and adjacent channel operations inside and outside the prison.
  - The jammer transmit power levels needed to overcome signals from nearby base stations will be well above federal safety limits for maximum permissible exposure to RF energy.

- If base stations are far away from the prison, signals near the prison will be weak and therefore much more susceptible to interference from the jammer.[18]

  - This interference will prevent calls such as 911 calls from going through.

- Prisons located near highways or congested urban areas magnify the harmful impact of jamming.[19]

---

16 *Id.*, at 7-8.

17 *Id.*, at 9-10.

18 *Id.*, at 11.

- Jamming in locations such as these with thousands of nearby commercial wireless users could result in significant harmful interference.
- V-Comm includes two slides showing actual prisons in Baltimore, Maryland and Philadelphia, Pennsylvania that are located 200 and 80 feet respectively from nearby highways, each of which is used by over 100,000 cars per day.

V-Comm's findings and analyses demonstrate that wireless networks are complex and variable and evolving constantly. Claims commonly made by jamming proponents that jamming is a simple and low-cost solution either ignore or fail to understand these complexities. Jamming will not work to block all of the wireless signals in the vicinity of the prison that may be used by prisoners to communicate with the outside world.[20] Moreover, to even come close to jamming effectively within the prison while minimizing harmful interference outside the prison, a jamming system would have to separately evaluate each frequency band used in the vicinity of prison and design the jamming system to account for the different signal levels, technologies and interference tolerances of those technologies. Designing a jamming system in this manner, however, will drastically increase the complexity and cost of building and maintaining the system.

---

[19] *Id.*, at 12-13.

[20] Even assuming a jamming system could be designed in a manner to block all frequencies in the vicinity of a prison facility, the effectiveness of that system will change over time. For example, a commercial wireless or public safety network operator that receives complaints of harmful interference near the prison caused by the jamming system may decide to make network changes to boost power near the prison to overcome that interference. Such changes may render the jamming system ineffective unless the jamming system, in turn, boosts its power. The end result may be a battle of power increases between the prison system and outside networks that will only end once maximum power levels or exposure levels are reached.

For all these reasons, jamming is not a viable alternative for addressing inmate contraband cell phone use within prisons and does not satisfy Congress' direction that technologies used to control contraband cell phone use by prisoners "do not pose a risk of negatively affecting commercial wireless and public safety services in areas surrounding prisons."

C. Managed Access Is Far Superior to Jamming and Avoids Causing Harmful Interference to Wireless and Public Safety Networks.

Managed access systems enable calls within range of the managed access network – a network of low-power base stations and antennas operated by a third party in cooperation with surrounding wireless network operators and located throughout a prison complex – to be captured before they reach the appropriate wireless carrier network and then either blocked, if the caller is not using a device on an approved list or sent on to the carrier network, depending on the parameters established for the system. While no technology for preventing wireless calls by inmates is perfect, managed access addresses and resolves many of the problems presented by jamming.

The advantages of managed access systems over jammers stem primarily from three features: (1) managed access uses low power base stations to capture calls rather than high power signals that block calls; (2) managed access systems operate on spectrum leased from surrounding commercial wireless providers and are designed in cooperation with such providers; and (3) managed access enables prison officials and carriers the flexibility to design the system in

a way that minimizes the possibility that emergency, pubic safety, and approved calls will be blocked.[21]

V-Comm highlights many of the advantages of managed access systems in its study.[22] For example, managed access systems can be designed to allow 911 and calls on public safety networks to be completed. 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 completed rather than blocked. Jamming systems, on the other hand, block all signals that are not stronger than the jamming signal and are not capable of allowing 911, public safety calls (including calls on public safety spectrum interleaved with or adjacent to commercial wireless spectrum), or calls from approved users to be completed. Managed access systems, because they are designed in cooperation with surrounding licensees and can be adjusted to account for changes in surrounding licensee networks, do not suffer from the problems associated with nearby or far away base stations or changing network conditions and technologies. Finally, managed access systems, because they do not block commercial wireless

---

[21] 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 and try again.

[22] V-Comm Study at 13.

signals from reaching smart phone devices, will prevent such devices from switching to wi-fi or other spectrum bands to complete calls.[23]

Recently, Verizon Wireless submitted an application for approval of a spectrum lease to Tecore Government Services ("Tecore") to enable Tecore to operate a managed access system on frequency bands licenced to Verizon Wireless at a state prison in Parchman, Mississippi.[24] Verizon Wireless believes that the successful installation and operation of the managed access system in Parchman will further demonstrate the advantages of managed access over jamming for controlling inmate contraband cell phone use.

For these reasons, managed access systems are far superior to jamming systems for controlling and preventing contraband cell phone use in prisons. Verizon Wireless encourages NTIA to recommend managed access as the superior technology for preventing contraband cell phone use in prisons and which satisfies Congress' preference for "technologies that do not pose a risk of negatively affecting commercial wireless and public safety services in areas surrounding prisons."

---

[23] *Id.*

[24] FCC Application or Notification for Spectrum Leasing Arrangement/ Notification of a Private Commons Arrangement, FCC Form 608, File No. 0004263928 (filed June 8, 2010).

III. CONCLUSION

Both the NTIA jamming test and the V-Comm analysis of that test prove that jamming is not a viable solution for controlling contraband cell phone use in prisons, because jamming is inflexible, indiscriminate, and will cause significant harmful interference to public safety and commercial wireless networks. Managed access is far superior to jamming in each regard and should be recommended by NTIA as the preferred technological solution to inmate cell phone use.

Respectfully submitted,

VERIZON WIRELESS

By: John T. Scott, III

John T. Scott, III
Vice President and Deputy General
Counsel – Regulatory Law

Andre J. Lachance
Assistant General Counsel

Verizon Wireless
1300 I Street, N.W., Suite 400-West
Washington, D.C. 20005
(202) 589-3760

Dated: June 11, 2010

APPENDIX A

NTIA Prison Jammer Study

Mike Katra – Staff RF Engineer
Sean Haynberg – Director RF Technologies

June 11, 2010

Overview

- Jammers Will Cause Harmful Interference to Commercial Mobile Service Outside Prisons
- Jammers Are Not Effective - Cannot Block All Spectrum Bands
- Jammers Can Interfere with Public Safety Radios
- Jamming Signals Propagate Outside Prisons
- Variability & Complexity of Cellular Networks Complicate Jamming Systems
- Jammers Cannot Block Service From Nearby Base Stations
- Weak Signals Near Prisons, More Sensitive to Interference
- Prisons in Congested Areas - Near Highways
- Jammer Alternatives Work Better

Jammers Will Cause Harmful Interference to Commercial Mobile Service Outside Prisons

- NTIA's Emission Measurement of a Cellular and PCS Jammer at a Prison Facility (Report # TR-10-466) demonstrates very high leakage of jammer signals outside prison facilities in cellular and PCS spectrum
  - Jammer signals were measured in the -50 dBm/MHz range at 430 feet away from prison (this was the furthest distance measured)
  - Jammer signals will cause significant harmful interference to cellular devices operating outside prison facilities
  - Jammer signal levels will continue to propagate well beyond 430 ft range and cause harmful interference to cellular devices for miles outside the prisons
  - Cannot stop jamming signals from propagating outside prison facilities
  - Will block cellular calls outside prisons including E911 and other emergency calls, and CALEA calls – Many nearby homes may only have cellular phone service
- Commercial mobile devices are very sensitive to interference
  - Cellular devices operate with low noise figures and in high fading environments
  - Cellular device receive sensitivities are very low (i.e. -110 dBm level), and typically operate levels below -100 dBm, and fade to even lower levels
  - Broadband devices operate with higher order modulation, which are more sensitive to interference (more fragile signal)
  - Rural markets operate at lower desired signal levels, which are very sensitive to interference
  - Any impairments will cause gaps in cellular service, dead zones around prisons

Jammers Cannot Block All Bands

- Wireless voice and data messaging can operate on too many spectrum bands for jammers to block wireless services in prisons
  - Users will simply migrate to any bands not jammed – need to jam all bands to be effective, but there are too many bands that can carry voice & data services
    - Jamming only 1 or 2 bands will not be effective when there are dozens of others
    - Voice (VOIP) & data messaging are supported on wireless data networks
- Spectrum Bands for wireless voice and data services include:
  - Existing Commercial Mobile Bands
    - Cellular 850 MHz bands (A & B blocks), PCS 1950 MHz bands (A to G blocks), AWS 2.1/1.7 GHz Bands, SMR 800 & 900 MHz Bands, LMR 800 & 900 MHz bands, 700 MHz bands (698-806MHz), WCS 2.3 GHz bands, BRS/EBS 2.5 GHz bands, Satellite Mobile Service Bands, and Two-way Paging Bands
  - Future Commercial Mobile Bands
    - AWS III Band, PCS H & J Blocks, White space devices (WSD) in UHF TV spectrum, future auctioned broadband spectrum
  - Wi-Fi and other Unlicensed Spectrum Bands
    - 2.4 GHz, 5.2-5.8 GHz, 3.6 GHz (light-licensed), and WSD in UHF TV spectrum
    - 5 GHz bands shared with Government Radar Service – jamming 5 GHz Wi-Fi bands could interference with government radar services
    - Smartphones switch to Wi-Fi bands automatically
  - Two-way Radio Bands
    - FRS band, GMRS band, CB Radio band, LMR bands, Amateur Radio bands
    - Some Nextel SMR phones can operate off-network in this mode
    - Jammers can only block receiving signals within prisons, but not transmitting signals out of prisons (would require jamming outside prisons for this)

Jammers Can Interfere with Public Safety Radios Inside and Outside of Prisons

- Public Safety radios operate in 800 MHz spectrum adjacent to Cellular A band and intermixed/shared within SMR/LMR 800 MHz bands
  - In-band jamming signals can cause harmful interference to Public Safety radios inside and outside prisons
  - Cannot filter out narrowband (i.e. 25 kHz) Public Safety channels that are intermixed within commercially licensed SMR/LMR 800 MHz spectrum
  - Cannot block Nextel phones without interfering with Public Safety
  - Cannot stop jamming signals from propagating outside prison property
- Public Safety voice and broadband radios operate in 700 MHz spectrum shared within commercially licensed spectrum blocks in 700 MHz spectrum, and plan to roam to commercially licensed 700 MHz blocks.
  - Cannot block 700 MHz commercial mobile bands without interfering with Public Safety

Jamming Signals Propagate Outside Prisons

- Prison facilities are not designed or able to prevent jamming signals from propagating outside facilities – can result in harmful interference to cellular and public safety devices operating outside facilities
  - Many prisons have windows, which can provide little to no attenuation of signal propagation to outside areas
  - Prison courtyards with outdoor jamming antennas can provide little to no attenuation of signal propagation outside of prison facilities (i.e. due to open roofs, chain-link fences with little to no attenuation of signal propagation)
    - Cannot stop RF propagation at prison facility boundaries
  - Prisons without windows are also problems
    - Buildings have variable signal attenuation losses
    - Commercial Industry Standards assume 12 dB for average building penetration loss with a standard deviation of approx. +/- 8 dB
    - High variability include lower loss conditions with high leakage outside
      - Windows, door openings, air ducts, etc. will be sources of high signal leakage
      - Attempting to address all these leakage points with shielding materials will drive up costs
    - Building penetration losses will not attenuate jammer signals enough to prevent harmful interference to outside cellular systems

Variability & Complexity of Cellular Networks Complicate Jamming Systems

- Jamming systems are complicated by the variability and complexity of commercial cellular networks
  - Many different spectrum bands can be used for voice and data services
  - Many different wireless technologies are used today, and will continue to change into the future (i.e. 2G, 3G, 4G, etc., each generation with different technologies)
  - Various wireless technologies operate at different frequencies, bandwidths, and signal levels, which have different interference tolerances
  - Various systems operators have different RF designs with base stations close or far from prisons – results in very high or very low signals inside and/or outside prisons
  - Commercial networks continue to change their RF design over time (i.e. adding more base stations, down-tilting or re-orienting antennas, etc.)
  - Commercial mobile signals vary depending on system loading conditions and time of day
  - Signals operate in high fading environments with reflections, cancellations and obstructions in and around prison facilities
  - Each prison application will have its own issues of variability to overcome – cannot apply results of one application to another
- Jammer systems would need to overcome all variability to prevent calls within prisons

Variability & Complexity of Cellular Networks Complicate Jamming Systems

- Commercial mobile bands consist of multiple blocks, or band segments, in markets having different network operations in each band (i.e. PCS A through G blocks, A-D-B-E-F-C-G)
  - In some cases, strong and weak cellular signals will be operating on adjacent band segments
  - For example, PCS E and PCS C blocks can be operating at strong signals from nearby base stations, and PCS F block can be operating at low levels from base stations far away from prisons
  - Signals from PCS E & C networks would be difficult to block due to operating at strong signal levels, while PCS F block would be more sensitive to harmful interference due to operating at low levels
  - In addition, some blocks are partitioned further and subleased to different network operations (i.e. A1-3, C1-3, B1-3 blocks), resulting in many different band segment combinations that can exist in markets and change over time
- Jammer systems would not be able to adjust power levels in each band segment over the range of signals that is required, and would not be able to prevent high emissions leaking into adjacent blocks

Jammers Cannot Block Service From Nearby Base Stations

- Nearby base stations result in strong cellular signals near prisons in the -30 to -10 dBm range (from actual measurements nearby base stations)
  - 3GPP standards conservatively assume -27 dBm nearby base stations, with base to mobile minimum coupling loss of 70 dB and 43 dBm BTS output power, however some measurements exceed this level by up to 17 dB
- Jammer signal levels required to block all CDMA & UMTS calls are -15 to +5 dBm/1.25MHz (D/U=-15 dB for unloaded system, Eclo=-5 to -20 dB) for outdoor jammer systems or calls made within prisons at windows
- This requires jammer transmissions of +75 to +95 dBm/1.25 MHz EIRP, per transmit antenna, to block all CDMA & UMTS calls
- This is a Jammer transmit power level of 32,000 to 3.2 Million Watts EIRP
  - This assumes jammer system maximum link budget of 90 dB (40 to 70 dB coupling loss, 10 dB for 90% fade margin, 10 dB for obstacle/body losses)
  - To maintain this link budget the jammer system requires a significant number of transmit antennas throughout the facility, which increases costs, complexity, maintenance, and vulnerability (prisoner vandalism) of these jammer systems
- These high jammer levels would result in harmful interference to co-channels and adjacent channels inside and outside the prison facility

Jammers Cannot Block Service From Nearby Base Stations

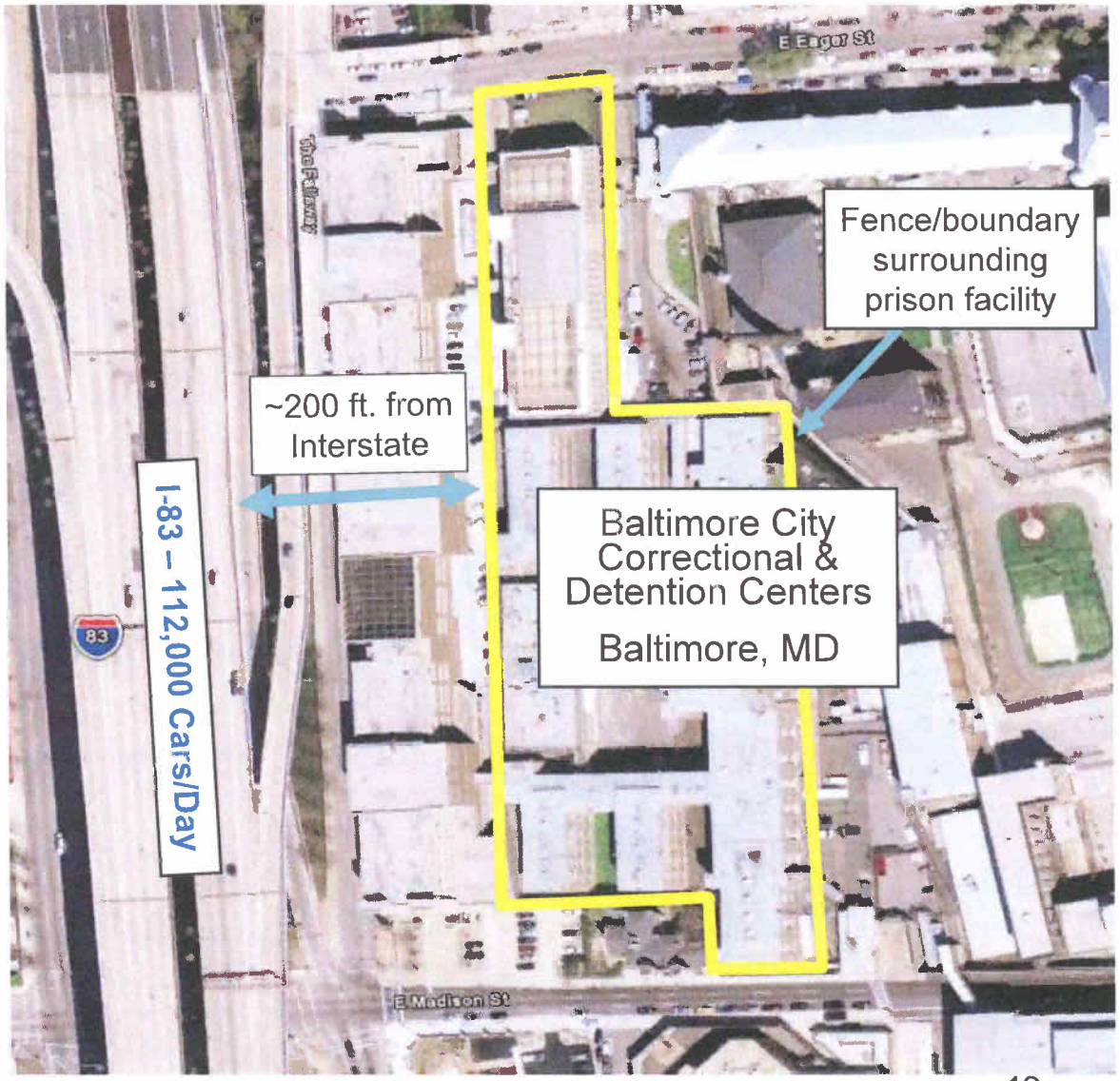
- For indoor jammer systems, not including calls made at windows, the jammer signal levels required to block all CDMA & UMTS calls are -27 to -7 dBm/1.25MHz per transmit antenna
  - This assumes the industry standard 12 dB for building penetration loss, which reduces the required cellular & jammer signals by 12 dB
- This requires jammer transmissions of +63 to +83 dBm/1.25 MHz EIRP per transmit antenna, to block all CDMA & UMTS calls
- This is an indoor Jammer transmit power level of 2,000 to 200,000 Watts EIRP per antenna
- Results in RF exposures within prisons well above federal safety limits for Maximum Permissible Exposure (MPE) of RF energy
  - Assuming a minimum coupling loss of 40 dB near indoor transmit antennas, the jammer signal will be *received* at +23 to +43 dBm, which exceed FCC/OSHA MPE levels by a large margin
- Jamming at high transmit levels are not practical and not permitted under federal safety standards -- jamming systems cannot block service from nearby base stations with strong cellular signals

Base Stations Far Away Result in Weak Signals Near Prisons, More Sensitive to Interference

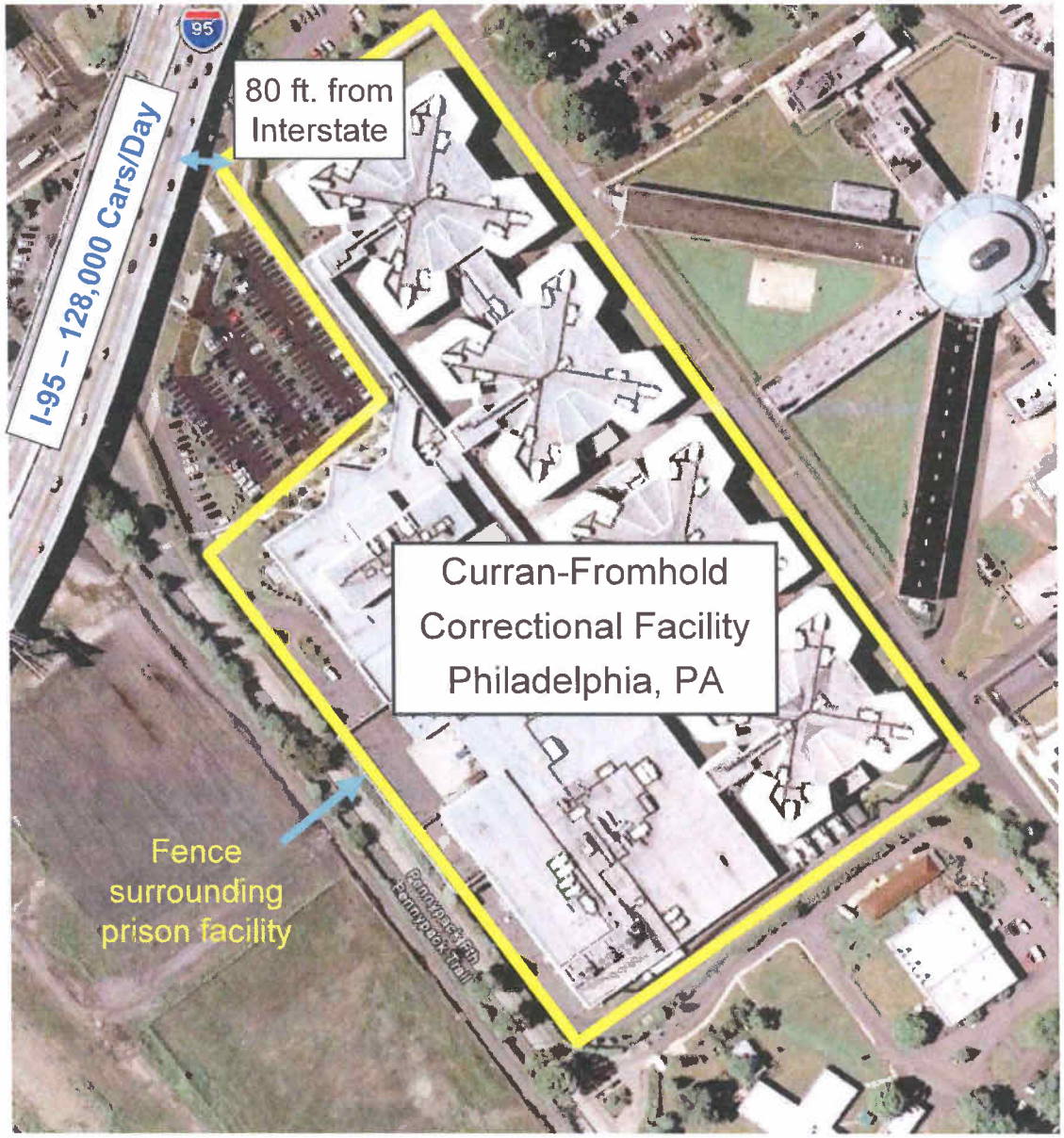
- Represents another incompatibility of the jammer & cellular systems
  - Strong cellular signals are difficult to block inside prisons
  - Weak cellular signals can be blocked inside prisons, but are more sensitive to interference outside prisons
  - Weak signals can also occur due to signal path obstructions, clutter and/or terrain effects around prisons. This creates weak signals outside prisons and in some cases will be unobstructed (strong) into the prisons
- Any impairments to weak cellular signals will cause gaps in service, dead zones around prisons to commercial mobile users
  - Some rely on cellular phones as only phones for E911, and other voice and broadband data communications
- Rural areas more likely to receive harmful interference from prison jamming systems due to operating at lower receive signal levels

Prisons Near Highways

- Some prisons are located in urban and congested areas with highways, homes, buildings, and public areas that can be impacted by jammer interference propagating outside the prison facility.
- This case shows a city prison within 200 feet of an Interstate that carries 112,000 cars per day, and is adjacent to buildings, public areas and other streets.
- This will impact a significant number of cellular calls a day.



Prisons Near Highways



- This case shows a prison facility within 80 feet of an Interstate (I-95) that carries 128,000 cars per day.
- This will impact a significant number of cellular calls a day.

Jammer Alternatives Work Better

- Managed Access Systems can mimic cellular systems and offer advantages over jamming systems:
  - Allows monitoring calls, giving announcements, directing calls accordingly
  - Allows E911 calls & other emergency calls, and CALEA calls within prison and outside
  - Allows white-listing of approved cellular phone devices within and nearby prisons
  - Setup similar to roaming systems where devices roam onto prison systems
  - Transmit at lower levels to capture phones – do not need high levels required to jam calls
  - Controls calls within prisons even when strong signals exist from nearby base stations
  - Can prevent phones from switching to other bands (i.e. Wi-Fi bands, AWS band, etc.), would not need to intercept as many spectrum bands within prisons
  - Can intercept Nextel/SMR calls within prisons without interfering with Public Safety radios

Jammer Alternatives Work Better

- Location systems can identify cellular calls made within prison facilities
  - Can be used in conjunction with Managed Access Systems to control access of cellular phone calls within prison facilities, or independently to locate phones within prisons
- Jammer Alternatives Work Better
  - More advanced capabilities & flexibility in controlling access and handling calls within prisons
  - Do not interfere with E911 and CALEA calls made within and outside prisons
  - Do not need rule changes or Congressional action – they are permitted today
  - Subleasing options with licensed carriers – fully cooperative arraignments with licensed carriers managing the system and impact to outside network, adapting and adjusting the system over time in step with changes made to their outside network
  - More effective in preventing unauthorized calls within prisons – jammers are not effective when base stations are nearby
  - Prevents harmful interference to cellular devices and Public Safety radios outside prisons

V-COMM is a leading provider of quality engineering and engineering consulting services to the worldwide wireless telecommunications industry with offices in Cranbury, NJ and Blue Bell, PA. V-COMM's engineering staff is experienced in Cellular, Personal Communications Services (PCS), Enhanced Specialized Mobile Radio (ESMR), Paging, Wireless Broadband Data, 2-Way radio, Microwave and Broadcast Mobile TV networks. We have provided our expertise to wireless operators in engineering, system design, implementation, performance, optimization, and evaluation of new wireless technologies.

We have extensive experience in analyzing interference in various spectrum bands including Cellular, SMR, PCS, AWS, Air-to-ground, Public Safety, and 700 MHz spectrum. We have engineering experience in all commercial wireless technologies, including HSPA, UMTS, EVDO, CDMA, GSM, MediaFLO, DVB-H and Analog technologies, and Public Safety wireless technologies including analog and digital Project 25, EDACS & Opensky, and many trunking and conventional radio networks. Further, V-COMM was selected by the FCC & Department of Justice to provide expert analysis and testimony in the Nextwave and Pocket Communications Bankruptcy cases.

For additional information, visit V-COMM's web site at www.vcomm-eng.com.