VENABLE LLP

600 MASSACHUSETTS AVE., NW WASHINGTON, DC 20001
T 202.344.4000 F 202.344.8300 www.Venable.com

James Arden Barnett, Jr., RDML USN
t 202.344.4695
f 202.344.8300
jbarnett@venable.com

June 30, 2017

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Contraband Cell Phones in Correctional Facilities
GN Docket No. 13-111

Dear Ms. Dortch:

John Fischer, CEO of Cell Command, Inc., Rob Smyjunas, Chairman of Cell Command, Inc., and I were present to demonstrate Cell Command's continuous wave beacon technology to Chairman Ajit Pai, Brendan Carr, FCC General Counsel, and Rachel Bender, Wireless Legal Advisor to the Chairman on June 29, 2017. Other persons attending included Eric L. Schultz, Jr., Director of Government and Public Affairs for the American Correctional Association (ACA), the Commissioners of Corrections from several states listed in Exhibit A, Josh Tewalt, Director of Operations for the Association of State Correctional Officials, and staff members from Congressional offices, also listed in Exhibit A.

The demonstration consisted of 16 cell phones with different generations of technology (2G, 3G, 4G) with service from each of the four major wireless carriers. Three of those phones were in 'airplane mode' so that they would only connect using Wi-Fi. John Fischer showed the two types of beacons that can be used with the system, fixed and mobile, depending on the needs and budget of the prison.

Within approximately 3 seconds of activating the beacon, all of the cell phones sounded a loud alarm and warning and then shut down all systems of each cell phones, including voice, text, camera and all installed applications.

All of the cell phones, including those operating only on Wi-Fi, were rendered completely unusable in any way. When FCC and correctional officials tried to turn the cell phones back on (in the presence of the beacon), the alarm and warning occurred again and each cell phone shut off.

Mr. Fischer noted that the system had been developed over many years after in-depth research and discussions with carriers, correctional officials and the FCC. This technology can be licensed to anyone for services, but in Cell Command's plan it is called Cell Warden®. Cell Warden will:

a. Make the device a 'brick', unlike all other systems (and the correctional officials do not even have to retrieve it which can be very dangerous)
b. Be vastly less expensive than other systems.
c. Not become obsolete, because the software will be updated over-the-air as wireless carriers upgrade systems (no expensive hardware upgrades for correctional facilities)
d. Not interfere with wireless carriers' spectrum or the performance of their customers' cell phones outside the prison
e. Does not violate the law against jamming
f. Follows current rules for 9-1-1
g. After set-up, work automatically with little required human interaction from either the carriers or each prison.

Cell Command urged a voluntary program by the wireless carriers, facilitated by the FCC; Cell Command does not advocate for a mandatory program. A copy of a handout that was distributed at the meeting is attached as Exhibit B.

Following the demonstration of the beacon technology by John Fischer and questions answers, the group discussed the importance of the FCC taking actions to defeat contraband cell phones for the safety of their correctional officers and employees and for public safety at large. Eric Schultz of ACA

noted the comments filed by ACA advocating, not for any particular company, but strongly for beacon technology as meeting 100% of ACA's requirements.

One member of the correctional community present stated that his state system was dropping managed access as being too expensive and not effective enough to warrant continued expense. Several members of the correctional community present also voiced their support for beacon technology, but reserved their option to push for jamming if the FCC did not take positive action in the near future on technological solution to contraband cell phones in correctional facilities.

After completion of the demonstration, the members of the correctional community thanked Chairman Pai and Brendan Carr for their leadership on the public safety crisis of contraband devices.

This ex parte notice submission is being filed for inclusion in the public record of the referenced proceedings pursuant to Section 1.1206(b) of the Commission's Rules.

Respectfully submitted,

James Arden Barnett, Jr.
Rear Admiral, USN (Retired)

cc: Ajit Pai, Chairman
Brendan Carr, General Counsel
Rachel Bender, Wireless Legal Advisor to the Chairman

Exhibit A

Attendees at the Cell Command Technology Demonstration on June 29, 2017

Cell Command

1. John Fischer, CEO of Cell Command, Inc.
2. Rob Smyjunas, Chairman of Cell Command, Inc.
3. Jamie Barnett, partner at Venable LLP for Cell Command, Inc.

Correctional Community

4. Jeff Dunn, Commissioner, Alabama Department of Corrections
5. Eric Schultz, American Correctional Association, Director of Government and Public Affairs
6. Josh Tewalt, Association of State Correctional Administrators, Director of Operations
7. Scott Kernan, Secretary of California Department of Corrections
8. Quincy Booth, Director of DC Department of Corrections
9. Wendy Kelley, Director, Arkansas Department of Corrections
10. Tony Parker, Commissioner, Tennessee Department of Corrections
11. Randall Mathena, Deputy Director, Virginia Dept. of Corrections
12. Brian Stirling, Director, South Carolina Department of Corrections
13. Jon Ozmint, former Director of South Carolina Department of Corrections
14. Lee Dotson, Tennessee Chief Interdiction Officer
15. Gary McLhinney, Maryland Department of Public Safety & Corrections
16. David Reitz, Maryland Department of Public Safety & Corrections

Congressional attendees

17. Anna R. Bartlett, Representative Trey Gowdy of South Carolina
18. Addie Patterson, Rep. Jeff Duncan of South Carolina
19. Elise Krekorian, Rep. Jeff Duncan of South Carolina
20. Andrew Hogin, Rep. David Kustoff of Tennessee
21. Al David Saab, Rep. David Kustoff of Tennessee

Exhibit B

Handout

Cell Command, Inc. June 29, 2017

Meeting with ASCA, ACA, and Cell Command, Inc.
(John Fischer, Founder and CEO and Rob Smyjunas, Board Chairman)

1. **Contraband cell phones in prisons are a serious, deadly epidemic.** Every state in the Union reports rampant cell phone use to run criminal enterprises and gang activities from prison, to perpetrate attacks on correctional personnel and to intimidate or kill witnesses. This is a public safety crisis.
2. **Cell Command's continuous wave beacon technology is the only one that is 100% effective.** Law enforcement and correctional officials demand a technology that can render the phone completely unusable without significant human intervention or danger to officers. (See ACA requirements on back).

> **How Cell Command's Cell Warden Works**
> Cell Warden's software is installed or updated on all phones. Cost effective beacons installed in prisons emit a special, non-interfering signal. When the cell phone hears the signal, it sounds an alarm and then shuts down all cell phone systems, including voice, text, camera and all apps. The phone cannot even be used to record messages and be passed physically.

3. **No other technology works and meets all of the requirements.** Jammers are illegal, expensive and not uniformly effective (with dead spots and also interference outside the prison). Legalizing jammers poses risks to law enforcement and homeland security. Other systems are expensive and require lots of human interaction for the wireless carriers and for correctional personnel. (See ACA requirements on back).
4. **No direct costs to carriers.** CW beacon technology does not interfere with carriers' spectrum, does not cost the carriers and is much less trouble than Managed Access Systems. The carriers would lose some sales but would help defeat this crisis.
5. **Affordable by prisons.** The technology is vastly more affordable than other technologies, especially since it is vastly more effective. The result is that all correctional facilities in the U.S. will be able to have CW beacon technology. Cell Command is will to license to anyone on a "Fair, Reasonable and Non-Discriminatory" basis (FRAND).
6. **The FCC's proceeding to find ways to defeat contraband cell phones is a timely vehicle for defeating contraband cell phones.** Chairman Pai has been clear in his leadership and public positions that he intends to take action.
7. **But, the software has to be on ALL cell phones to be effective.** The FCC does not like to designate technology (except when public safety is involved such as LTE to ensure interoperability for FirstNet) and the FCC will want to find a way to have carriers support the program voluntarily.

REQUEST: Make defeating contraband cell phones in prison (and the criminal, gang and drug activities they enable) a signature initiative of the Chairman of the FCC and convene the wireless carriers to adopt voluntarily and unanimously continuous wave beacon technology within one-year.

Contraband Cellphone Suppression System Required Characteristics (excerpt from American Correctional Association)

1. **Render unusable.** The technology must be able to completely render the wireless device unusable, with the possible exception of 9-1-1, preventing all other voice calls, data usage, memory function, photography or any other function or application that can be used to transmit or record any form of communications, even by passing the device physically.

2. **Ubiquity and interoperability.** The technology must work on all wireless devices for all carriers. It must work throughout the facility, which has been a problem for jammers and other systems.

3. **Cost-effectiveness.** The technology must be affordable for all correctional facilities, which has been a problem for the other proposed technologies. The technology must be flexible enough to be updated without undue expense or the expenditure of capital funds to keep the capabilities functional. The best technology is useless if it is unaffordable.

4. **Non-interference.** The technology must not interfere with communications signals outside the correctional facility, which has been a problem with jammers and other systems.

5. **Ease of operation.** The technology must work quickly and almost automatically without significant human intervention, from either correctional personnel, carrier personnel or contractors. It should not require much supervision, oversight or manual input to disable the device. The system should ideally work passively and automatically. Other systems require a great deal of human activity and time, as does some of the detection systems.

6. **Secure.** The technology must be secure from tampering or interference by inmates or any non-authorized personnel and it must have strong protections against breaches in cybersecurity from hacking or disruption.

7. **Compliant.** The technology must be legal and compliant with state and federal law and with the regulations of the FCC.