Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF CTIA

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

Dated: June 19, 2017

TABLE OF CONTENTS

Before The
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY

CTIA[1] commends Chairman Pai's long-standing commitment to preventing inmates' use of contraband wireless devices in correctional facilities – a threat to the safety of the general public, witnesses, prison employees, and other inmates.[2] Wireless providers, correctional institutions, and vendors have all worked together to identify and deploy contraband interdiction systems ("CISs") that serve dual goals: preventing contraband device use while not undermining the ability of legitimate subscribers to obtain service. To that end, the record in this proceeding already shows the successful deployment of managed access systems ("MASs") across multiple states. The Commission's Report and Order in this proceeding takes further steps to facilitate

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st- century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 2336 (2017) ("R&O" and "FNPRM").

MAS deployment.[3]

The Further Notice takes the next step to consider alternative CISs.[4] Although MASs are a proven solution, CTIA welcomes the opportunity to work with the Commission and other stakeholders to advance a well-crafted, reasonable approach to cell detection systems ("CDSs"), another CIS solution. Progress demands a collaborative solution. Working together, stakeholders can identify reasonable solutions that will help prevent use of contraband wireless devices while not undermining the ability of legitimate subscribers to obtain service outside of correctional facilities. Other proposed CIS solutions, like network-based or technology-specific solutions, would be ineffective, burdensome, and costly, and the Commission should avoid focusing on these unworkable solutions.

II. THE WIRELESS INDUSTRY IS COMMITTED TO COMBATING CONTRABAND DEVICES IN CORRECTIONAL FACILITIES AND HAS BEEN A STRONG PARTNER IN ENABLING MANAGED ACCESS SYSTEMS

As the record in this proceeding demonstrates, the wireless industry has collaborated with correctional institutions and vendors to develop workable solutions to the problem of contraband wireless devices in prisons.[5] Today, there is broad recognition that MASs are effective in preventing use of contraband wireless devices inside correctional facilities.

As the Commission has explained, a MAS is a small private network placed within a correctional facility to monitor commercial wireless transmissions to or from wireless devices and determine whether any such device is authorized or unauthorized to use a commercial

[3] *See* R&O at 2344-2366, ¶¶ 17-78; *see, e.g.*, Comments of CTIA, GN Docket No. 13-111, at 1-2 (filed July 18, 2013) ("CTIA Comments").

[4] *See generally* R&O and FNPRM.

[5] CTIA Comments at 1-2.

wireless network.[6] If the device is unauthorized, the MAS blocks the transmission. Wireless providers have worked with MAS providers to ensure operability and to engage in spectrum lease agreements that permit MAS operations inside correctional facilities. Today, there are deployments and trials in numerous states, including California, Maryland, Mississippi, South Carolina, Texas, Florida, and Georgia.[7] And they are having a dramatic impact. By way of example, California's MAS solutions have intercepted nearly 12 million communications attempts from over 75,000 unauthorized wireless devices since the state began its pilot programs in some of its prisons in 2011.[8]

The Report and Order streamlined the spectrum leasing process by amending its rules so that long-term *de facto* spectrum leasing applications and spectrum manager leasing notifications for CISs will be subject to immediate processing and approval.[9] The streamlined spectrum leasing application process will better facilitate the deployment of CISs and will make it easier for the wireless industry to continue collaborating with correctional institutions and CIS vendors.

Unfortunately, some participants in the proceeding suggest that wireless providers have been "disinterested" in solving the problem of contraband devices in prison.[10] That is not so. And these comments demonstrate that the wireless industry is ready and willing to actively

---

[6] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Notice of Proposed Rulemaking, 28 FCC Rcd 6603, 6610 ¶ 14 (2013) ("2013 NPRM").

[7] *See* CTIA Comments at 1-2; *see also* Reply Comments of Verizon Wireless, GN Docket No. 13-111, at 4-5 (filed Aug. 23, 2013) ("Verizon Reply Comments").

[8] Robert Johnson, *Cut the Potentially Deadly Prison Cell Phone Connection* (May 5, 2017), http://www.postandcourier.com/opinion/commentary/cut-the-potentially-deadly-prison-cell-phone-connection/article_fe2196dc-303a-11e7-9113-67ccba21a6a3.html.

[9] R&O at 2357-58, ¶¶ 56-58.

[10] *See, e.g.*, Comments of The Association of State Correctional Administrators and Director of the North Dakota Department of Corrections, GN Docket No. 13-111, at 2 (filed May 30, 2017) ("ND DOC Comments").

engage in the development of alternative solutions that provide meaningful, reasoned approaches to ending use of contraband devices.

III. THE COMMISSION SHOULD ADOPT A SOUND FRAMEWORK FOR THE DEPLOYMENT OF CELL DETECTION SOLUTIONS

While MASs are a proven means to prevent contraband wireless device use in correctional facilities, the Further Notice seeks comment on alternative CIS solutions.[11] CTIA is committed to working with all stakeholders to pursue targeted alternate solutions that prevent contraband phone use without jeopardizing service to legitimate subscribers or imposing undue burdens on the wireless industry and American consumers. As the Further Notice recognizes, CDSs represent a meaningful alternative – if developed and implemented properly.[12] CDSs are used to "locat[e], track[ ], and identify[ ] radio signals originating from a device"[13] and, once a device's signal is located, the CDS obtains identifying information about the device. An authorized entity can then direct a wireless provider to prevent operation of that device on the network.

A. The Commission Should Clearly Define the Standards for an Eligible Contraband Interdiction Systems and a Qualified Request.

In the Further Notice, the Commission sought comment on key aspects of any cell detection proposal, including the threshold requirements for "an eligible CIS" and what constitutes "a qualifying request from an authorized party" directing action against an unauthorized device.[14] It is critical for the Commission to adopt reasonable, workable definitions of CIS eligibility, a qualified request, and an authorized party, to provide clarity and

[11] R&O at 2339, ¶¶ 5-7.

[12] *Id*.

[13] *Id*. at 2339, ¶ 7.

[14] FNPRM at 2369, ¶ 87.

certainty for CDS solutions.

CIS Eligibility. The Further Notice properly recognizes that the systems used to detect contraband wireless devices and trigger a demand to restrict use of those devices must meet certain performance standards, and be deemed eligible by the Commission, in order to minimize the risk of preventing use of an authorized wireless device.[15] This requires device certification and solution validation. First, the equipment should be certified under Part 2 of the FCC's rules because even passive cell detection systems have the potential to produce emissions.[16] Second, the Commission should validate whether the CDS is operating properly and capturing accurate, necessary information regarding phones within corrections facilities – and only phones within corrections facilities.[17] CTIA urges the Commission to develop Part 2 rules to govern this system validation process. Finally, the Commission should ensure that the provider of a certified and validated cell detection system regularly calibrates the system's operations to ensure accuracy after initial device certification and solution validation. This will provide additional assurance that the data used as the basis for the request is accurate and reliable.

Source of Request. The "authorized party" permitted to direct wireless providers to prevent use of wireless devices should be clearly defined so that it does not create uncertainty for wireless carriers in implementing a termination request. As CTIA has noted before, a court order directing wireless providers to prevent use of a wireless device is the soundest means of addressing the contraband device issue.[18] This approach would ensure a high standard for such

[15] FNPRM at 2372, ¶ 96.

[16] CTIA Comments at 8 (citing 47 C.F.R. §§ 2.801(b), 2.803, 15.01).

[17] *Id*.

[18] *Id*. at 12; CTIA Reply Comments at 7-8.

requests, provide for due process, and implement an effective enforcement mechanism in those states that prohibit use of contraband devices in correctional facilities.[19] If the Commission does not adopt this approach, the FCC itself should be the source of a qualifying request and should direct wireless providers to prevent operation of a wireless device. That way, wireless carriers are acting at the direction of the Commission, which can monitor the effectiveness of the CDS process. If the Commission determines it cannot participate, then the only reasonable alternative is that all requests come from a senior state official with oversight of the CIS operator. The rules should not require wireless providers to respond to requests by non-sworn law enforcement officials, *e.g.*, a warden at a privately owned and operated correctional facility or from the CIS itself.[20]

Content of Request. The content of the request also should be clearly defined by the Commission's rules. As the Further Notice points out, a qualifying request should include a device's International Mobile Subscriber Identity ("IMSI"), as well as the correctional facility in which the device is operating.[21] This would provide a wireless provider with the information necessary to accurately prevent use of the unauthorized device on its network.

B. The Cell Detection Solution Should Prevent Use of the Wireless Device in a Reasonable and Effective Manner.

The Further Notice recognizes there are multiple approaches to preventing use of wireless devices identified by a CDS solution.[22] One reasonable, and technically feasible, approach is for the CDS to identify the IMSI associated with an unauthorized wireless device, and for the

[19] CTIA Reply Comments at 7-8.

[20] CTIA Comments at 10.

[21] FNPRM at 2374, ¶ 101.

[22] *Id*. at 2339, ¶ 7.

wireless provider to block use of that IMSI, thereby terminating service. A fully effective and engaged CDS will allow correctional institutions to continuously or regularly sweep their facilities – rather than merely capturing IMSI use at a single point in time – so that the attempted use of swapped out SIMs in a single device will result in the identification of multiple unauthorized IMSIs, making it much more difficult for inmates to use contraband wireless devices.

CTIA recognizes the Commission's interest in a rule that would fully disable contraband devices.[23] This approach, however, requires broader stakeholder input, including participation by the original equipment manufacturers ("OEMs"), and it creates other risks including expanded cybersecurity threats as a "shut down" mechanism would be available to hackers. CTIA remains committed to ensuring that the CDS framework provides for a reasonable and sound approach that creates an effective CDS solution.

C. The Role of Wireless Providers Should be Limited to Fulfilling the Qualified Request.

CTIA submits that the wireless provider responsibility should be limited to carrying out a qualified request to prevent use of the identified device on its network. CMRS licensees should not be required to provide notification that it has fulfilled or rejected the request, as proposed by the Commission.[24] This notification requirement would potentially require wireless providers to individually consider the specific merits of each request sent by the authorized party. It also would cause delays and would be burdensome and costly for providers. Moreover, a rule requiring CMRS licensees' compliance with a qualifying request from an eligible entity would obviate the need for an affirmative confirmation from a provider that it has complied with the

[23] FNPRM at 2369, ¶ 104.

[24] *Id*. at 2376, ¶ 110.

request.

The Commission also should refrain from imposing any rules that require carriers to provide notification to CIS operators of technical changes.[25] The record demonstrates that CIS operators can and do monitor and identify carrier network changes without the need for prior carrier notifications.[26] Indeed, some lease arrangement agreements already require the CIS operator to monitor for carrier network changes. CIS operators have ample time to modify their systems as necessary, because future technology and network changes are known months or years in advance. Adopting notification requirements could result in delayed wireless deployment or upgrades. Such notification requirements also would be duplicative, costly, burdensome, and disruptive to marketplace arrangements already in place. These significant negative effects stemming from a notification requirement greatly outweigh the minimal effort of CIS operator's customary network monitoring practices. While wireless providers will continue to coordinate with vendors regarding technology and network changes, CIS operators need to monitor carrier system changes and be aware of any changes that will be taking place in the future.

D. The Commission Should Create a Policy Regime That Fosters, Not Penalizes, Good-Faith Compliance Efforts.

The wireless industry is eager to work with the Commission and stakeholders on an effective CDS framework and fully intends to comply with reasonable rules to prevent use of those devices identified by CDSs, but the Commission should recognize that the CDS approach has the potential to prevent use of authorized, non-contraband wireless devices – for example,

[25] FNPRM at 2378-79, ¶¶ 117-21.

[26] Ex Parte of T-Mobile, GN Docket No. 13-111, at 2 (filed Mar. 17, 2017) ("T-Mobile Ex Parte").

should a qualified request be issued for a misidentified device.

The unintentional termination of legitimate services could cause severe disruptions to customers and even endanger the safety of users.[27] It also could create disputes, potential liability, and harm to wireless providers' goodwill.[28] The CDS validation process discussed above is thus important to verify that a CDS is properly functioning and providing accurate and complete data.[29] And government participation in directing a qualifying request, by court order or the Commission or a top state official, should further serve to ensure that qualifying requests are targeted at unauthorized devices. These steps will protect the public.

But the Commission should do more. It should adopt a safe harbor rule under its rules for wireless providers acting in good faith to comply with the federal process for preventing the use of wireless devices in correctional facilities.[30] Further, it should provide liability protection for wireless providers that comply with the rules.

IV. THE COMMISSION SHOULD REFRAIN FROM ADOPTING FRAMEWORKS FOR OTHER SOLUTIONS

A. Beacon-Based Technologies are Costly and Would Require Substantial Changes Through Lengthy Processes.

The Commission should refrain from dictating use of a beacon system that would require software embedded in wireless devices.[31] First, implementation of these systems would require

[27] CTIA Reply Comments at 7.

[28] *Id.*; *see also* Comments of AT&T, GN Docket No. 13-111 at 7 (filed July 18, 2013) ("AT&T Comments"); Reply Comments of AT&T, GN Docket No. 13-111 at 4-5 (filed Aug. 23, 2013) ("AT&T Reply Comments").

[29] *See supra* Section III.B.

[30] FNPRM at 2377, ¶ 113-14.

[31] *Id.* at 2382-83, ¶¶ 130-32.

all existing and future wireless devices to include the software.[32] As recognized by Commissioner O'Rielly, this would be a dramatic departure from the Commission's long-standing policy to remain technology-neutral and it would involve a sweeping government mandate.[33] Further, it would be ineffective, burdensome, and costly, with a lengthy implementation process. It also would pose a cybersecurity threat to public safety by introducing a nationwide capability that could be used to block legitimate calls. Finally, as the Further Notice observes, there is a substantial question of whether mandating use of such technology would require Congressional legislation.[34]

B. Quiet Zones Would Restrict Wireless Providers' Network Design and Stymie Service in and Around Correctional Facilities.

FCC-imposed quiet zones around correctional facilities would have the effect of preventing legitimate communications, including public safety communications on commercial networks, on prison grounds and beyond.[35]

The quiet zone proposal would unnecessarily complicate wireless network design to the detriment of legitimate authorized wireless customers, because a quiet zone network design cannot stop at a barbed wire fence. Further, in rural areas, wireless service often is provided via higher power antennas on taller towers that cover great distances, and a network re-design to engineer quiet zones could easily take rural consumers near correctional facilities out of

---

[32] *Id*.

[33] FNPRM (statement of Commissioner Michael O'Rielly) ("[W]hile I support the further notice … I have concerns about some of these concepts and may not be able to support them if they were to be contained in a final order … [including] the possibility that the Commission would mandate beacon technologies, which is not a technology neutral approach."); *see also* FCC, *Strategic Plan of the FCC*, https://www.fcc.gov/general/strategic-plan-fcc (last visited June 13, 2017) (stating that Commission "policies must promote technological neutrality").

[34] FNPRM at 2382-83, ¶¶ 130-32.

[35] CTIA Reply Comments at 10; *see also* Verizon Reply Comments at 10; AT&T Reply Comments at 7.

service.[36] Even in urban areas, quiet zones would have to extend substantially beyond the bounds of the prison property. And because some correctional facilities are located near busy interstates and well-traveled state routes, and are not "relatively remote" as other parties have suggested,[37] quiet zones could take travelers out of service. Given the above drawbacks, CTIA opposes this proposal.

C. There is No Lawful Basis for the Commission to Impose Network-Based Solutions that Require Wireless Providers to Develop and Implement Their Own CIS.

The Commission sought comment on whether wireless providers should be responsible for developing and implementing CIS solutions directly in or around correctional facilities.[38] The Commission should not simply place on wireless providers the sole responsibility for solving the corrections community's contraband problem, as the network-based inquiry in the FNPRM seems to posit.[39] The Commission does not have the authority to require wireless providers to develop and implement a CIS. First, it would be inappropriate for the government to require that CMRS carriers actively track subscribers' location information. Section 222 classifies location information as customer proprietary network information ("CPNI") and prohibits carriers from using this information without prior customer authorization.[40] And second, 9-1-1 location based information is only generated in response to a consumer dialing 9-1-1, which serves as authorization to use location information. Thus, the Commission cannot

[36] CTIA Comments at 10-11; Verizon Reply Comments at 11.

[37] *See* Comments of NTCH, Inc., GN Docket No. 13-111, at 6 (filed July 18, 2013) ("NTCH Comments").

[38] FNPRM at 2381-82, ¶ 128.

[39] *Id.*

[40] *See* 47 U.S.C. § 222(h)(1) ("The term 'customer proprietary network information' means ... information that relates to the quantity, technical configuration, type, destination, *location,* ... made available to the carrier by the customer") (emphasis added).

lawfully leverage 9-1-1 systems to address the contraband phone issue. Therefore, the Commission should refrain from mandating a network-based solution.

V. CONCLUSION

CTIA is proud of the role its members have played in assisting correctional institutions in their fight against the use of unauthorized, contraband wireless devices. CTIA commends the Commission's actions to streamline that process. CTIA urges the Commission to embrace a cooperative process for wireless carriers, correctional facilities, and CIS providers to advance a meaningful, reasonable CDS solution. To the extent the Commission does adopt rules, these rules must promote clarity and certainty for wireless carriers, and remain technology-neutral.

Respectfully submitted,

/s/ *Brian M. Josef*
Brian M. Josef
Assistant Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 736-3200

Dated: June 19, 2017