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
Senior Vice President, Regulatory Affairs

John Marinho
Vice President, Cybersecurity & Technology

Michael Mullinix
Director, Regulatory Affairs

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

Dated: September 16, 2020
TABLE OF CONTENTS

I.  INTRODUCTION AND SUMMARY. ................................................................. 1

II. MAS IS THE LEADING CONTRABAND INTERDICATION SOLUTION, AND MAS- EVOLVED WILL MAKE IT EVEN MORE EFFECTIVE. ........................................ 4
    A. MAS-Evolved Will Achieve Integration that Allows It to Operate More Effectively and Efficiently, to Adjust to New Technologies, and to Reduce Costs. .......... 4
    B. The Wireless Industry is Actively Advancing Development and Deployment of MAS-Evolved................................................................. 6

III. DISABLING SERVICE TO CONTRABAND DEVICES REQUIRES A FRAMEWORK OF ACCOUNTABILITY, AND CTIA PROPOSES A NATIONWIDE, FCC RULE-BASED PROCESS................................................................. 8
    A. Accountability is Critical, Either Through Court Orders or an FCC Rule-Based Process. 8

IV.  THE WIRELESS INDUSTRY IS WORKING TO MINIMIZE THE IMPACT OF NETWORK CHANGES AND EVOLVING TECHNOLOGY ON MAS DEPLOYMENTS. 11
    A. Both Close Coordination Between the Wireless Industry and Vendors, and Evolving Technology, are Making it Easier for MAS Deployments to Adapt to Wireless Network Changes. ............................................................. 11
    B. All Parties Have a Role to Play in Addressing the Challenge of Contraband Devices. 12

V.  THE COMMISSION SHOULD REJECT CONSIDERATION OF “SELF-JAMMING.” .... 13
    A. A Self-Jamming Mandate Would be Bad Policy. .................................................. 13
    B. A Self-Jamming Mandate Would Not Avoid Legal Risks Surrounding Jamming. .... 15

VI. OTHER SUGGESTIONS MENTIONED IN THE JULY 28 PUBLIC NOTICE ARE NOT VIABLE AND WOULD BE INFERIOR TO MAS IN ANY EVENT. ................................. 16
    A. Geofencing is Not Currently a Viable Solution. .................................................... 16
    B. Other Ideas Mentioned in the July 28 Public Notice Are Inferior to MAS. .......... 18

VII. THE COMMISSION SHOULD STREAMLINE THE PROCESS FOR CELL DETECTION SOLUTIONS’ ACCESS TO COMMERCIAL SPECTRUM ........................................ 18

VIII. CONCLUSION. ............................................................................................. 19
Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF CTIA

I. INTRODUCTION AND SUMMARY.

CTIA welcomes the opportunity to refresh the record in this proceeding and to update the
Commission on the status of stakeholders’ actions to reduce the public safety threat of contraband
phones in correctional facilities.¹ Contraband devices present an appalling and multi-faceted
problem requiring action by stakeholders on a number of fronts, from halting the ongoing
smuggling of devices into facilities, to identifying contraband devices without inadvertently
targeting legitimate wireless communications, to applying an accountable framework in directing
that service be disabled to devices identified as contraband.

The wireless industry has worked diligently to assist the corrections community and federal
and state policymakers to, in Chairman Pai’s words, “determine the most effective, affordable, and
safe ways to address this problem—that is, to stop the threat of contraband cellphones without

¹ Wireless Telecommunications Bureau Seeks to Refresh the Record on Promoting Technological Solutions
28, 2020) (July 28 Public Notice). See also Promoting Technological Solutions to Combat Contraband
Wireless Device Use in Correctional Facilities, Report and Order and Further Notice of Proposed
causing harm to legitimate wireless users.”² Since the Chairman convened a contraband roundtable in early 2018, CTIA and its members have taken a number of actions to take on this critical issue. CTIA and its members established the Contraband Phone Task Force, together with state corrections leaders and the Department of Justice Bureau of Prisons; funded a Testbed conducted by the Virginia Tech Applied Research Corporation (VT-ARC) to assess both the effectiveness and the flaws of various contraband interdiction solution (CIS) technologies; instituted regular coordination and communications with CIS vendor stakeholders; worked to implement court order processes for disabling contraband phones; and arranged to use the Stolen Phone Database as a means of denying service to contraband phones across multiple networks.³

Our work has demonstrated that there are effective solutions available today to interdict contraband devices, such as Managed Access Systems (MAS) and cell detection. These two approaches provide options that can assist corrections officials in both large and small facilities.

MAS and its next generation version, MAS-Evolved, are effective at stopping calls from contraband devices while avoiding harmful spillover effects. Last year’s Contraband Phone Task Force Report and the Virginia Tech Testbed study analyzed multiple contraband interdiction systems and concluded that MAS systems are “a proven solution to the problem of contraband cell phone use in correctional facilities” and that “the CIS Testbed Administrator knows of no other

---


technical solution that is as effective.” 4 For many correctional facilities, we anticipate that MAS-
Evolved will be the most effective path to achieving Chairman Pai’s goal of stopping the threat of 
contraband cellphones without harming legitimate wireless users.

Cell detection systems, or “IMSI sniffers,” offer another effective option for disabling 
phones.5 These systems can detect phones within a corrections facility and capture the 
international mobile subscriber identities (IMSIs) of those devices. Once the IMSIs have been 
collected, service to the devices can be shut down via court order or other process, such as the rule-
based framework discussed below and at Attachment A. One important advantage of cell 
detection systems is that they are portable and can be moved from one corrections facility to 
another, thereby spreading out the cost of operation and making them a more economical option. 

By contrast to MAS and cell detection, other options that have been suggested, such as 
jamming and geofencing, pose real risks that public safety and other legitimate users will get 
captured and harmed by the inherent inaccuracies of those approaches. Moreover, they are not as 
simple to implement as some stakeholders believe, and some of these suggestions threaten to 
impose undue burdens on corrections officials and wireless providers.

CTIA understands that corrections officials are concerned about the cost of MAS and are 
looking for less expensive alternatives, but no precision solutions that both stop contraband use 
and protect legitimate users are simple and free. There is a role for federal, state, and local 
policymakers in ensuring the availability of funding for effective contraband interdiction systems.

4 Contraband Interdiction System Testbed Report & Best Practice Recommendations, GN Docket No. 13-
Report) (filed by CTIA and the Association of State Correctional Administrators).
5 See, e.g., id. at 2-12.
And CTIA has worked with Congress to secure dedicated funding for MAS and supports continued efforts to support state and local corrections officials.

The wireless industry has worked in good faith to address the challenges identified by corrections officials. In these comments, CTIA offers yet another constructive solution, a proposed rule-based termination system, with the goal of making the MAS approach still more efficient and effective. CTIA remains open and committed to working with corrections officials and federal, state, and local policymakers to develop and implement effective methods of addressing this complex challenge.

II. MAS IS THE LEADING CONTRABAND INTERDICTION SOLUTION, AND MAS-EVOLVED WILL MAKE IT EVEN MORE EFFECTIVE.

A. MAS-Evolved Will Achieve Integration that Allows It to Operate More Effectively and Efficiently, to Adjust to New Technologies, and to Reduce Costs.

MAS systems are operational and successful today, and MAS-Evolved systems will be even more effective at combatting contraband devices by allowing for more seamless automated interoperation with commercial wireless networks. Deployments in multiple states are expected in the next few months.

Following extensive testing of various contraband interdiction technologies, VT-ARC concluded in 2019 that it “knows of no other technical solution that is as effective” as Managed Access.6 As the Commission is aware, MAS operates as a mini-network within the correctional facility, causing cellphones in the MAS coverage area to attach to the MAS network by overpowering the signals from the surrounding commercial networks. The MAS network then prevents the transmission of calls from contraband devices while passing on 9-1-1 calls and those

---

6 Id. at 4-54.
from a “white list” of permitted devices (such as employees’ phones) to the commercial wireless networks. And as VT-ARC concluded, MAS systems protect nearby communities by stopping calls from contraband devices with little risk of interfering with legitimate wireless users’ calls outside the correction facility.⁷

As an added benefit, and unlike other solutions, MAS systems are also useful for investigative purposes. MAS enables the collection of critical analytics and information about the contraband devices being used and the communications being attempted. With proper court authorization, corrections and law enforcement officials can monitor illicit conversations, and the data provided can develop evidence for prosecuting crimes. No other proferred solutions match the benefits of MAS.

Notably, however, existing MAS deployments require manual coordination with surrounding commercial wireless networks, whereas MAS-Evolved allows for more seamless automated interoperation without human intervention or resultant delay. This offers significant, additional benefits.

First, MAS-Evolved’s use of Software Defined Radio allows the system to adapt, in real time and on an automated basis, to changes in the surrounding commercial wireless networks and technologies. This allows MAS-Evolved to adjust to changes in wireless providers’ signal strength caused by network updates, and changing power level conditions due to weather conditions or changing seasons. And importantly, it enables MAS-Evolved to support multiple cellular bands and evolving generations of technologies and standards. MAS-Evolved can thus “future proof” for newer generations of technology, capturing more contraband calls regardless of the wireless technology that an inmate’s device uses.

In addition, MAS-Evolved’s technology allows the coverage footprint to be “fine-tuned,” as the system and the surrounding commercial wireless networks exchange information in an automated fashion, reducing coverage “holes” in corrections facilities and limiting any MAS “spillover” beyond prison walls, whether the correctional facility is in urban or rural settings. MAS-Evolved also improves the ability to locate contraband devices and unauthorized callers in correctional facilities.

And notably, MAS-Evolved will be easier and less expensive to administer than current systems. Existing Managed Access requires human intervention and resources to coordinate between isolated systems in correctional institutions and the surrounding commercial wireless networks. MAS-Evolved, by contrast, relies on roaming agreements with the surrounding public wireless networks that employ automated protocols for the exchange of traffic. MAS-Evolved leverages industry standards and best practices to provide real-time active coordination. This drives efficiencies and improved performance, while enhancing the system’s reliability to interdict calls from contraband devices. And MAS-Evolved will be less costly than traditional MAS deployments. By operating within the surrounding commercial wireless networks, MAS-Evolved keeps pace with the evolution of technology and takes advantage of the hardware and software volumes generated by the world-wide, standardized, and competitive mobile wireless industry.


Wireless providers are fully committed and actively engaged with MAS vendors and correctional officials to advance MAS-Evolved. We expect to see MAS-Evolved implemented in Mississippi and California within the next few months, and those implementations will allow the vendor to expand readily to other facilities it serves.
First, CTIA’s nationwide provider members have reached initial roaming agreements with a MAS-Evolved vendor to facilitate the coordination that MAS-Evolved envisions and are working with others. While developing the initial roaming agreements for this new use case required resolution of a variety of novel issues, now that the details have been worked out, these initial agreements provide a ready prototype for expanding expeditiously to the remaining vendors.

In addition, to help inform corrections officials about the benefits and technical aspects of MAS-Evolved, CTIA developed and distributed a Managed Access Systems Stakeholder Checklist. The Checklist addresses specific issues to aid corrections officials in their acquisition and implementation of MAS systems, and to help MAS vendors and wireless providers in the deployment of these systems. It provides guidance on best practices for coordination among stakeholders, emphasizing the importance of coordinating at the earliest possible stages. It also provides guidance on what information and commitments corrections officials should expect from vendors and what support wireless providers should be expected to provide. CTIA has shared the Checklist with the Correctional Leaders Association to encourage dissemination among state correctional officials, as well as sharing it directly with identified corrections officials and vendors.

And finally, to help address corrections officials’ financial concerns about CIS solutions, the wireless industry has worked with Congress to secure funding for MAS. The Edward Byrne Memorial Justice Assistance Grant Program provides hundreds of millions of dollars that can be

---

8 CTIA has also created and distributed other educational materials to corrections officials, such as a fact sheet explaining the capabilities of MAS and MAS-Evolved and another document highlighting the federal funding available to pay for contraband interdiction systems.

9 Given security concerns related to public disclosure of the guidance and best practices included in the Checklist, CTIA has refrained from distributing the Checklist as a public document.
used for criminal justice purposes, including paying for CIS solutions such as MAS.\textsuperscript{10} In addition, last year Congress designated two million dollars specifically for MAS deployments as part of that grant program.\textsuperscript{11} CTIA has also engaged with outreach to corrections officials about the federal funding and how to obtain a grant.

\textbf{III. DISABLING SERVICE TO CONTRABAND DEVICES REQUIRES A FRAMEWORK OF ACCOUNTABILITY, AND CTIA PROPOSES A NATIONWIDE, FCC RULE-BASED PROCESS.}

\textbf{A. Accountability is Critical, Either Through Court Orders or an FCC Rule-Based Process.}

As noted above, Chairman Pai made clear that the contraband initiative must work to stamp out illegal inmate calls “without causing harm to legitimate users.”\textsuperscript{12} The risk that legitimate users’ service is cut off is real, and any process for disabling devices must ensure that: (i) the systems used to identify contraband phones are accurate; (ii) the procedures used to request the disabling of specific phones are reliable; and (iii) the disabling requests passed on to wireless providers are clear and unambiguous. Court orders are one means of providing this accountability and have been effective where they are available. Wireless providers have worked closely with state corrections officials to create standard court order language and efficient systems for provider/institution communications. So far, thousands of devices have been shut down in a number of states, as well as through the Department of Justice, which obtained its first court order to stop cell service to contraband devices in a federal correctional facility earlier this year.


\textsuperscript{12} FCC News Release at 1.
CTIA fully supports the court order approach, and wireless providers are continuing to work with multiple jurisdictions interested in developing court order processes. At the same time, some jurisdictions have indicated that they do not have the time and resources to pursue court orders. To help fill the gap, CTIA is putting forward as an alternative a proposed framework for a nationwide, FCC rules-based approach that can provide similar accountability.

**B. An FCC Rule-Based Framework Can Provide an Efficient, Accountable, and Nationally-Available Method for Responsibly Disabling Contraband Devices.**

In the 2017 Further Notice, the Commission sought comment on “a Commission rule-based process regarding the disabling of contraband wireless devices where certain criteria are met, including a determination of system eligibility and a validation process for qualifying requests.”

Based upon CTIA’s consultations with federal and state law enforcement officials, Attachment A to these comments sets out CTIA’s proposed termination framework, which tracks and implements the FCC’s vision and will aid in the effective deployment of solutions like MAS and cell detection.

In short, the FCC would direct wireless providers to terminate service to a list of specified devices that have been identified by an FCC-certified CIS solution as contraband and forwarded to the FCC by a designated official; wireless providers would then act to terminate service at the explicit direction of the FCC, which would oversee the effectiveness of the CIS process and order service terminations. Particulars of CTIA’s proposed framework include the following (as set forth in Attachment A):

---

13 2017 R&O and Further Notice, 32 FCC Rcd at 2367 ¶ 83.
14 Id. at 2366-78 ¶¶ 79-116.
• The FCC adopts performance standards for CIS solutions and certifies CIS solutions to ensure appropriate functionality and reliability, and these standards should include data security and privacy safeguards to ensure that information collected that may be from legitimate non-contraband devices is protected;15

• The FCC establishes a process by which designated state or local law enforcement agencies are authorized to make requests to the FCC to direct wireless providers to terminate service to contraband devices identified by certified CIS solutions;17

• If the FCC concludes that a termination request is valid, has a good faith basis, and has met the FCC’s procedural and validation requirements, the FCC directs wireless providers to terminate service to a list of specified devices;18

• Wireless providers then terminate service to the identified devices at the explicit direction of the FCC.

This framework would be efficient, providing a straightforward and consistent process for use by corrections officials across the country, and it would replicate the accountability of the court order process.19 It would provide rigorous FCC oversight of the CIS solution used to identify contraband devices, which will also benefit corrections officials selecting and relying on these systems. And the framework’s clear FCC directives to wireless providers will impose accountability while providing them with liability protection for carrying out those directives. The FCC rule-based framework will thus allow for the rapid, efficient, and responsible termination of devices identified as contraband.

15 See id. at 2372-73 ¶¶ 96-97 (“We seek to ensure that the systems detecting contraband wireless devices first meet certain minimum performance standards in order to minimize the risk of disabling a non-contraband wireless device.”).

16 Data security and privacy safeguards are especially important, as this proposal will require wireless providers to contract with third party service providers selected by the correctional authorities without providers having had any opportunity to provide input into the vendor selection, vet these companies’ processes, or require them to make changes.

17 See id. 2373-75 at ¶¶ 98-105 (seeking comment on what would constitute a qualifying request for termination, and by whom such a request could be made).

18 See id. 2375-76 at ¶¶ 106-109 (seeking comment on the specifics of the disabling process).

19 Jurisdictions that have or in the future adopt a contraband device court order framework could continue to use those processes.
IV. THE WIRELESS INDUSTRY IS WORKING TO MINIMIZE THE IMPACT OF NETWORK CHANGES AND EVOLVING TECHNOLOGY ON MAS DEPLOYMENTS.

A. Both Close Coordination Between the Wireless Industry and Vendors, and Evolving Technology, are Making it Easier for MAS Deployments to Adapt to Wireless Network Changes.

CTIA’s members share the Commission’s desire to minimize the impact of network changes and evolving technologies on MAS deployments and have been working closely with solutions vendors to provide early information and limit the effort needed to adjust to network changes.

For instance, the nationwide wireless providers generally meet separately, and at least monthly, with the current MAS vendors to share information. This close coordination, conducted since early 2019, has paid off, allowing MAS vendors to prepare for the deployment of new spectrum bands and for the rollout of 5G. The provider/vendor coordination process is working, and we urge the Commission to allow it to continue to develop through collaborative—and not prescriptive—engagement.

Moreover, as noted above, one of the significant benefits of MAS-Evolved is the introduction of automated capabilities that adjust to many types of commercial wireless network changes. For instance, if a wireless provider installs a new cell tower causing its signal strength to increase at a correctional facility, an interconnected MAS-Evolved system can detect that increase and automatically adjust to ensure that the MAS signal remains strong enough to capture calls made within the facility. This happens seamlessly, without human intervention. And even if active intervention and adjustment of the MAS-Evolved system is necessary to respond to a network change, a MAS-Evolved system connected to commercial wireless networks will alert the operator that action is needed, eliminating the risk of an unidentified gap in the operation of the MAS.
B. All Parties Have a Role to Play in Addressing the Challenge of Contraband Devices.

The effort to put a stop to contraband devices in correctional facilities requires multiple initiatives and multiple stakeholders. Fundamentally, too many contraband devices are finding their way into inmates’ hands, and we share the view that more must be done to restrict the flow of contraband into correctional facilities. CIS solutions providers must continue to evolve their systems and build in excess capacity to best address the needs of correctional officials and accommodate evolving wireless technology; policymakers need to support these efforts; and the wireless industry has and will continue to play a critical role in combatting contraband devices.

It is important to put the wireless industry role in context. First, communications policymakers constantly challenge the industry to expand coverage throughout the country and to make the latest technologies available to all consumers. But in the contraband device context, some advocates have identified options that could significantly undermine these efforts by risking disruption of legitimate calls, including 9-1-1 calls; by calling upon wireless providers to deploy inferior service to consumers in the vicinity of corrections facilities; and by forcing providers to bear increased costs in making service available to consumers.

The wireless industry has been working diligently with all stakeholders to help solve this public safety crisis, but it would be unreasonable for the FCC and other policymakers to expect wireless providers to degrade services to legitimate users or bear all of the costs of eliminating the contraband phones problem. The wireless industry has no input into the decisions made by corrections policymakers, such as the extent of initiatives to keep contraband devices out of facilities in the first instance, the location of correctional facilities that require CIS solutions, or the enactment and enforcement of penalties to address contraband phones. Although efforts are underway, the wireless industry has limited input into the deployment of CISs and the extent to
which they are designed from the start to accommodate inevitable network and technology changes. Wireless providers will continue to invest in their networks and to fund testing, outreach, and other initiatives, but we oppose the suggestion in the *July 28 Public Notice* that wireless providers absorb the costs of third parties, such as CIS vendors, for upgrading their systems to adjust to network changes.\(^{20}\) These costs are a public responsibility and should not be shifted to one industry sector. Nevertheless, the wireless industry will continue to work with all stakeholders to help solve this public safety problem. For example, as noted above, CTIA has worked and will continue to work with Congress to help identify funding for corrections institutions’ use of CIS.

Further, wireless providers are working with vendors to minimize the need for CIS upgrades to the extent possible. MAS vendor OmniProphis acknowledged this cooperation in its recent comments and notes as examples two specific cases in which wireless providers were able to adjust their power or antenna placement to avoid impacting nearby MAS.\(^{21}\) It is not possible, however, to eliminate the need for some CIS upgrades in response to network changes. We emphasize that wireless providers should not be restricted or disincented to make network upgrades—or to put it another way, legitimate customers near correctional facilities should not be deprived of the benefits of network improvements.

V. **THE COMMISSION SHOULD REJECT CONSIDERATION OF “SELF-JAMMING.”**

A. **A Self-Jamming Mandate Would be Bad Policy.**

The *July 28 Public Notice* asks for comment on “self-jamming,” which it describes as carriers deploying base stations to block their own signals.\(^{22}\) But such self-jamming would have

\(^{20}\) *July 28 Public Notice* at 3.


\(^{22}\) *July 28 Public Notice* at 5.
all the same drawbacks as third-party jamming—indiscriminately blocking all calls caught up in the sweep of the jammer, with no ability to permit legitimate calls, including 9-1-1 or other public safety communications. Wireless providers work tirelessly to reduce any noise within their service areas to ensure that calls go through. Asking them to jam their own signals would be fundamentally antithetical to sound network design.

First, the risks of jamming are well documented. Unlike CIS solutions, jamming is indiscriminate, endangering legitimate and critical communications within a corrections facility and beyond. The VT-ARC Testbed found that jammers used inside a correctional facility can disrupt legitimate, lawful communications beyond prison walls. And a study conducted last year by the National Telecommunications and Information Administration (NTIA) in coordination with the Federal Bureau of Prisons in South Carolina confirmed the risks to the nearby public.23 That testing took measurements at both 20 and 40 meters (66 and 132 feet) away from the jamming solution and showed a risk of harmful interference at both of those distances,24 and NTIA did not attempt to determine how far away one would have had to be for that risk to dissipate completely.

And further, self-jamming would be costly. Jamming is quick and cheap only when done in an unsophisticated, brute force manner—exacerbating many of the drawbacks identified above. In contrast, precision jamming is complicated to design and on a par with MAS in terms of cost, but still with the negative, indiscriminate consequences described above.25

---

24 Id. at 30.
Moreover, if the FCC were to order wireless providers to self-jam, each individual wireless provider in the vicinity of a correctional facility would have to set up its own sophisticated, precision jamming system at each correctional institution, further increasing the expense. Requiring wireless providers to undertake such efforts and expense would be unjustified, particularly when MAS/MAS-Evolved provides an effective alternative.

**B. A Self-Jamming Mandate Would Not Avoid Legal Risks Surrounding Jamming.**

The *July 28 Public Notice* makes an unwarranted assumption that self-jamming would “*not result[] in a violation of section 333*” of the Communications Act.26 The Fourth Circuit, however, has rejected the notion that self-jamming is permissible. In *Johnson v. American Towers*, the plaintiff argued that the section 333 prohibition against interference does not apply if a wireless service provider is interfering with its own signals.27 The court, however, took the view that the better reading of section 333 is that no person shall interfere with any radio communications, “*including his or her own.*”28

Further, the Commission has taken the position that Section 333 bars activities beyond radio interference if they have the effect of disrupting communications and has taken or threatened enforcement action under section 333 in cases that did not involve radio interference.29

Thus, the legal issues with respect to jamming provide yet another compelling reason the Commission should abandon the idea of self-jamming as a contraband solution.

---

26 *July 28 Public Notice* at 5 (emphasis added).
28 *Id.* (emphasis added).
VI. OTHER SUGGESTIONS MENTIONED IN THE JULY 28 PUBLIC NOTICE ARE NOT VIABLE AND WOULD BE INFERIOR TO MAS IN ANY EVENT.

A. Geofencing is Not Currently a Viable Solution.

The July 28 Public Notice invited comment on other technological options, asking specifically about the concept of geofencing. That term is not clearly defined, but the July 28 Public Notice observed that the 2017 Further Notice “previously sought comment on the idea of creating a geo-fence within which contraband wireless devices would be inoperable, and relatedly, the concept of requiring wireless providers to identify and disable contraband devices within the geo-fence using their own network elements, including base stations and handsets/devices, as well as the costs and benefits of such a process.”

As an initial matter, MAS technology as it exists today effectively accomplishes the same things that the Commission hopes geofencing might accomplish—it locates phones, identifies those that are inside a correctional facility and are contraband, and then prevents those devices within that boundary from making calls.

In fact, the July 28 Public Notice’s specific questions about geofencing highlight the benefits of MAS-Evolved as the preferred solution for stopping contraband phone traffic. The July 28 Public Notice asks whether the Commission should require wireless providers not to exceed a specific signal strength in the proximity of a correctional facility, for example by requiring wireless providers to treat the walls of a correctional facility the same as the edge of the license area. It is, of course, not feasible to ensure that a signal will dissipate entirely before reaching the edge of a license area. Wireless providers address this issue not by restricting service so as to

---

30 July 28 Public Notice at 3.
31 Id. at 3 n.9.
32 Id. at 3.
leave customers near the edge without service but by negotiating signal strength agreements with
adjacent market providers and entering into roaming agreements to establish automated protocols
for handling signals at the border. MAS-Evolved would effectively treat correctional facility walls
as the edge of the license area and put in place automated protocols for handling signals at the
border. In other words, MAS-Evolved would do just what the Commission hopes that geofencing
could do.

As for whether geofencing is a viable option for addressing contraband phones, network-
based geofencing is only a theoretical concept today, and CTIA has previously identified technical
concerns with the concept in an attachment submitted in connection with the April 2019
Contraband Task Force Status Report.33 To the extent that geofencing might rely on GPS-based
location measurements, GPS is not consistently reliable within corrections facilities, with its
effectiveness depending on the construction of the buildings and the location of the phones. To the
extent that geofencing might rely on cell tower triangulation, it would be inaccurate in rural areas.
Geofencing to the necessary level of accuracy for contraband interdiction would likely require
additional location positioning information from the device (e.g. Wi-Fi) that may not be reliably
available in a correctional facility and, further, can be disabled on the contraband device.

In addition to these technical concerns, CTIA and its members do not support geofencing,
or any other solution, that requires them to continually track their customers and puts the burden
on wireless providers to make their own determinations as to whether devices are contraband and
should be disabled. Law enforcement officials, not wireless providers, are best positioned to make
decisions about what devices are contraband; that obligation should not be shifted to wireless
providers.

33 Task Force Status Report, Attachment B.
Given that MAS-Evolved essentially accomplishes the same goals as geofencing, and that MAS-Evolved is well along in development and can effectively be implemented with an accountability framework, CTIA believes that it makes little sense to change course to develop a new and untested concept of geofencing.

B. Other Ideas Mentioned in the July 28 Public Notice Are Inferior to MAS.

Other ideas mentioned in the July 28 Public Notice are also inferior to MAS. Quiet zones, for instance, would interfere with providers’ ability to meet customer capacity demands. And because networks are designed to provide ubiquitous coverage, significant infrastructure changes would be required in order to deliberately create coverage holes and legitimate users living and/or working near these facilities would face gaps in their coverage. Some adaptations, such as adjusted power levels, may be possible in rural areas without negatively affecting legitimate customers, but this cannot be viewed as a wide-scale solution. By contrast, MAS provides a tested and effective solution today.

VII. THE COMMISSION SHOULD STREAMLINE THE PROCESS FOR CELL DETECTION SOLUTIONS’ ACCESS TO COMMERCIAL SPECTRUM.

From the wireless industry’s perspective, the 2017 leasing rules appear generally to be effective. There is one issue we would ask the Commission to consider, however, which relates to facilitating the use of mobile cell detection systems discussed above, which provide a less costly option to corrections officials. Given the large number of possible mobile deployments at multiple correctional facilities and the need to keep the timing and location of those deployments confidential in order to maintain the element of surprise, implementing more streamlined methods

34 See July 28 Public Notice at 3.
for permitting mobile deployments may be appropriate. CTIA welcomes the opportunity to work with the Commission to consider how it might do so.

VIII. CONCLUSION.

The wireless industry has consistently demonstrated its commitment to helping the corrections community stop the threat of contraband cellphones and will continue to do so. As the Commission considers its options in this proceeding, we encourage the agency always to keep in mind Chairman Pai’s recognition that our collective goal is to stop the threat of contraband cellphones without causing harm to legitimate wireless users. We appreciate this opportunity to share our experiences and recommendations with the Commission.

Respectfully submitted,

/s/
Michael Mullinix
Director, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Senior Vice President, Regulatory Affairs

John Marinho
Vice President, Cybersecurity & Technology

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

Dated: September 16, 2020
ATTACHMENT A
FCC-led Service Termination Framework for Contraband Devices

• **CIS Eligibility.**
  
  o The FCC adopts performance standards for CIS solutions and certifies CIS solutions to ensure certain functionality and reliability;
  
  o These standards should include data security and privacy safeguards to ensure that information collected that may be from legitimate non-contraband devices is protected; and
  
  o The FCC also requires CIS vendors to keep records sufficient to enable troubleshooting if non-contraband devices are mistakenly identified as contraband.

• **Authorized Party and Qualifying Request.**
  
  o The FCC identifies and publishes a list of designated state or local law enforcement agencies in each state that will facilitate termination requests from corrections facilities.
  
  o The designated state or local law enforcement agency:
    
    ▪ Makes a qualified request (i.e., made by an FCC-designated law enforcement agency, based on the use of an FCC-certified CIS, and subject to the standards noted below) to the FCC to direct wireless providers to terminate service to the devices identified by the certified CIS solution. The request must include:
      
      • A list of contraband devices operating at a correctional facility, as identified utilizing a certified CIS solution;
      
      • The name and geographic location of the correctional institution in question; and
      
      • The factual details that establish that the devices have been determined to be contraband, and documentation demonstrating that the equipment and process used complies with the FCC’s certification and validation procedures.

    ▪ The qualified request must include each device’s IMSI and IMEI, the correctional facility in which the device is operating, and any other verified information the FCC believes it needs to assure itself that the process used
complies with the FCC’s certification and validation procedures and has a valid, good faith basis.

- The qualified request must also contain contact information that wireless providers can provide to customers who question the service termination.

- **Disabling Process.**

  - If the FCC concludes that the request is valid, has a good faith basis, and met the FCC’s procedural and validation requirements, the FCC orders the wireless provider to terminate service.

  - The FCC expressly states that the wireless provider must terminate service pursuant to the FCC’s express direction, that the provider has no discretion to choose not to terminate service, and that the FCC’s express direction is an act of public authority and failure to comply would put the provider in violation of a federal requirement.

  - The FCC’s direction to the wireless provider, which will be by letter order or similar clearly mandatory instruction, will include the following information, in an electronic format in addition to any written document.

    - The IMSI and IMEI of the contraband device.

    - Contact information to provide to customers that contact the carrier to question the termination of service.

  - The wireless provider terminates service to the device.

  - The FCC develops a process for correcting any instances in which a consumer’s service is erroneously identified as contraband and terminated.