

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS OF AT&T SERVICES, INC.

Jessica B. Lyons
Michael P. Goggin
Gary L. Phillips
David L. Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036
(202) 457-2100

June 19, 2017

Its Attorneys

TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY.....	1
II.	AT&T HAS BEEN AN ACTIVE PARTNER IN THE FIGHT AGAINST CONTRABAND PHONE USE.....	3
III.	AT&T SUPPORTS A FRAMEWORK THAT SUPPORTS BOTH PUBLIC SAFETY AND CONSUMER STAKEHOLDERS.	5
IV.	USE OF A COURT ORDER PROCESS WILL CURB CONTRABAND DEVICE USE WHILE PROTECTING LAWFUL USERS.....	9
	A. The Court Order Process Will Ensure a High Degree of Accuracy in the Termination Process and is Familiar to Stakeholders.....	9
	B. An Accurate List With Strong Evidentiary Support Protects Stakeholders and Promotes the Public Interest.	13
V.	AT A MINIMUM, A QUALIFYING REQUEST SHOULD INCLUDE CERTAIN CERTIFICATIONS TO PROTECT LAWFUL USERS.....	14
VI.	CONCLUSION.....	17

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS OF AT&T SERVICES, INC.

I. INTRODUCTION AND SUMMARY

AT&T Services, Inc., on behalf of its affiliates, (“AT&T”) respectfully submits these comments in response to the *Further Notice of Proposed Rulemaking* (“*Further Notice*”) in the above-captioned proceeding. In the *Further Notice*, the Commission seeks comment on proposed mechanisms to combat the use of contraband wireless devices by inmates in correctional facilities.¹ In particular, the *Further Notice* seeks comment on a process under which wireless providers would be required to disable contraband wireless devices once they have been identified.²

AT&T shares the Commission’s serious concerns regarding the public safety threat posed by the possession and use of contraband wireless devices by inmates in correctional facilities. It is for this reason that AT&T has been an active participant in efforts to address this problem, and

¹ *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, FCC 17-25 (2017) (“*Further Notice*”).

² *Id.* at ¶ 83.

has collaborated with key stakeholders in taking steps to combat contraband device use. AT&T, together with other wireless carriers, has worked with corrections officials and providers of contraband interdiction systems (“CIS”) to deploy CISs in state correctional facilities nationwide. Through these efforts, state corrections facilities have been able to prevent the unlawful use of mobile phones in prison while allowing lawful – and sometimes critical – use by individuals authorized to use wireless communications services on prison grounds.

AT&T supports rules that aggressively prevent and terminate the use of contraband wireless devices in correctional facilities, but these rules must not come at the expense of law-abiding wireless consumers. The Commission in the *Further Notice* has proposed a regime that would require wireless carriers to disable wireless devices detected by an eligible CIS when the wireless carrier receives a qualifying request from an authorized party.³ AT&T is concerned that the Commission’s proposed rules in this area have the potential to not only go far beyond the managed access systems the rules seek to emulate, but also to impact law-abiding consumers whose devices are falsely flagged as contraband. AT&T therefore urges the Commission to proceed carefully in developing additional rules, as no solution to the problem of contraband device use should come at the expense of law-abiding wireless consumers.

AT&T believes that the Commission can curb contraband device use – while protecting lawful users – by employing a process by which court orders are used to effectuate device disabling and/or termination of service where a CIS has identified a wireless device as contraband. Use of a court order process will ensure a high degree of accuracy in the termination process, as any request will be required to meet an evidentiary standard sufficient to ensure that

³ *Id.* at ¶ 87.

lawful device users have not been erroneously captured. An accurate list of identified devices with strong evidentiary support will protect stakeholders while promoting the public interest and the Commission's objectives. This process will have the added benefit of helping enforce state criminal law in states that have criminalized the possession and/or use of a wireless device by an inmate in a correctional facility. And, because both wireless carriers and law enforcement officials are familiar with the court order process, implementation should be relatively simple.

However, if the Commission adopts a different threshold for a "qualifying request," AT&T submits that certain minimum criteria must be met. First, the "qualifying request" should come from somebody with the authority and incentive to ensure that a list of identified contraband devices is correct and has not erroneously identified a law-abiding user as an inmate. The official should also be required to make certain certifications, including a certification that the list of devices submitted to a carrier has been scrubbed of devices that likely are not in the possession of inmates. These certifications will help to promote the development of requests that are well-vetted and less likely to erroneously capture a lawful user.

II. AT&T HAS BEEN AN ACTIVE PARTNER IN THE FIGHT AGAINST CONTRABAND PHONE USE.

AT&T agrees with the Commission and the corrections community that the possession and use of contraband wireless devices by inmates in correctional facilities poses a great threat to public safety, both inside and outside of correctional facilities. It is for this reason that AT&T has played a leading role in the fight against contraband phone use. AT&T has undertaken numerous efforts to assist corrections officials with the deployment of managed access systems and other technical solutions.

AT&T leases its licensed spectrum to CIS vendors for free, and works with managed access systems vendors to address technical challenges and prevent interference to commercial networks while helping corrections facilities fight this scourge. Thus far, AT&T has provided free access to its spectrum and extensive technical support to more than 30 prisons across 8 states. AT&T also is willing to work with providers of managed access and detection systems to fine-tune these systems in cases where corrections officials believe systems are not as accurate as they should be.

AT&T has also provided legal, regulatory, and other human support to the corrections community. A large number of AT&T employees with varying areas of specialty have dedicated time and resources to fighting contraband phone use. For example, AT&T's in-house and outside counsel alike dedicate substantial time to initiating and executing spectrum leases, making required FCC filings, and paying applicable fees. This includes efforts to ensure that AT&T's unrelated secondary market transactions do not impact the operation of managed access systems in the geographic area covered by a particular transaction. Thanks to the efforts of AT&T and other wireless carriers around the country, state corrections facilities have deployed managed access systems that allow them to prevent the unlawful use of mobile phones in prisons while allowing lawful use.⁴

⁴ AT&T notes that by deploying managed access systems, corrections officials already have the ability to effectuate the termination of communication to and from a device identified as contraband. The regime proposed by the Commission in the *Further Notice* thus serves as an *alternative* to the tools already available to corrections officials; it is not the only means by which communications to and from contraband devices can be terminated.

III. AT&T SUPPORTS A FRAMEWORK THAT SUPPORTS BOTH PUBLIC SAFETY AND CONSUMER STAKEHOLDERS.

While AT&T supports law enforcement efforts to keep contraband phones out of correctional facilities, it is also committed to ensuring that its law-abiding wireless customers maintain quality and continuity of service – and that their service is not wrongfully terminated or interrupted because a CIS falsely identifies a legitimate device as contraband. AT&T urges the Commission to adopt rules in this proceeding that not only support the corrections community in tackling contraband phone use, but also protect the interest of lawful wireless users.

As a general matter, AT&T supports the termination of service to devices that are being used unlawfully. Indeed, AT&T’s terms of service empower AT&T to terminate service in any case where a subscriber is using their device and/or their wireless service unlawfully.⁵ AT&T employs a team of personnel whose job function includes addressing violations of AT&T’s terms of service – including unlawful use of AT&T’s service – and terminating service in cases of terms of service violations. Once AT&T has completed necessary investigations to determine that a terms of service violation in fact has taken place, the process of actually terminating service is an extremely quick one.

AT&T is concerned, however, that the proposals set forth in the *Further Notice* would require AT&T to terminate service to a device (or disable a device entirely)⁶ where there is risk

⁵ See AT&T Wireless Customer Agreement § 1.2, at <https://m.att.com/shopmobile/legal/terms.wirelessCustomerAgreement.html> (last visited June 19, 2017) (“AT&T may interrupt, suspend or cancel your Services and terminate your Agreement without advance notice for any reason including, but not limited to, the following . . . You use your Device/Equipment and/or our Services for an unlawful or fraudulent purpose.”).

⁶ AT&T continues to support a requirement that involves the termination of service to a device, not the complete disabling of a device. First, as AT&T notes in these comments, a service termination requirement still goes above and beyond what a managed access system

that a device has been flagged in error. For example, individuals who live near corrections facilities may habitually find that their devices (or devices that enter their home) have been wrongfully captured by a CIS. These individuals may be unable to move – nor should they be required to move to enjoy unfettered wireless use.⁷ Lawyers who visit their clients in prison and require connectivity to serve their clients “on the go” may have their cell phones flagged as belonging to an inmate because they frequently visit a correctional facility. Communications that such an attorney might initiate from outside the prison (such as from the parking lot) might cause her device to be flagged. Prison employees and/or contractors (such as drivers of delivery trucks) similarly could have their phones identified in error. Family members visiting their loved ones in prison, who may be far from home and cannot readily communicate with their wireless carrier, may find that their service has been disabled pursuant to the Commission’s proposed rules – and their only source of connectivity with their carrier may be their now-disabled phone. Motorists who drive by corrections facilities could have their device flagged, and they may have no idea that their chosen driving route may place them at risk of having their service terminated or device disabled. All of these individuals are as deserving of protection under the Commission’s rules as the stakeholders identified in the *Further Notice*.

currently accomplishes. Under the regime proposed by the Commission, the termination of service would persist until a carrier restored it, even if the affected user is not an inmate and moves outside the range of the CIS. Second, a service termination requirement would enable a law-abiding customer who has been flagged in error to get their service restored without damage to their device, and with less disruption.

⁷ In a similar vein, Commissioner Clyburn has expressed concern that a public park in which she used to exercise could be affected by the deployment of a CIS in a nearby correctional facility. *Further Notice*, at Statement of Commissioner Mignon L. Clyburn Approving in Part, Concurring in Part.

These examples are not purely hypothetical. There have been several real-world examples of law-abiding users being erroneously flagged by a managed access system. After a managed access system was installed at Mississippi State Penitentiary in Parchman, Mississippi, a local farmer tending his field attempted to make a phone call while on his tractor, and found his call intercepted by the managed access system.⁸ In 2014, multiple users walking and/or driving near the Baltimore City Detention Center reported that their calls were blocked.⁹ While these scenarios appear to have been remedied through technical adjustments to managed access systems,¹⁰ they demonstrate that managed access systems are not perfect. The Commission must

⁸ Eric Grommon, Ph.D. et al, *A Case Study of Mississippi State Penitentiary's Managed Access Technology* at 54 (Aug. 2015), at <https://www.ncjrs.gov/pdffiles1/nij/grants/250262.pdf> (“One example was provided by MSP personnel where a local farmer was tending his field near the facility and attempted to make a call while on his tractor. The farmer contacted MSP officials after receiving the automated recording generated by the system alerting the user of their illegal call attempt. This situation was remedied as MSP personnel reviewed his situation and included his number on the approved list.”).

⁹ See Carrie Wells, *Drivers report problems with cell phone blocking near Baltimore jail*, THE BALTIMORE SUN, Feb. 9, 2014, available at <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-jail-cellphone-blocking-issues-20140208-story.html> (describing the experience of multiple motorists whose calls were blocked while driving near the Baltimore City Detention Center, and who upon redialing were notified that their calls were unauthorized and subject to monitoring); Len Lazarick, *Inmate calls are blocked, and so are some outside the jail walls*, MARYLANDREPORTER.COM, Feb. 9, 2014, at <http://marylandreporter.com/2014/02/09/inmate-calls-are-blocked-and-so-are-some-outside-the-jail-walls/> (“Inside the jail, I had already heard the ominous recorded message you’re supposed to get if you’re an unauthorized user inside the detention center. . . . That’s the same message I got about 100 feet outside the high prison wall as I tried to call AAA for road service. And then the call disconnected. Repeatedly. That’s the message I got a half-block further south on Graves Street. I had to go a full block away from the jail to East Monument before my Blackberry could get through.”).

¹⁰ See, e.g., Carrie Wells, *Drivers report problems with cell phone blocking near Baltimore jail*, THE BALTIMORE SUN, Feb. 9, 2014, available at <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-jail-cellphone-blocking-issues-20140208-story.html> (“The company has said that the blocking technology would be contained to the inside of the jail and that cell phone users on the streets would not be affected.

take care not to compound this problem by adopting a regulatory regime that unfairly injures those whose phones may generate a “false positive” for a contraband interdiction system.

AT&T provides these examples of lawful use not as an exhaustive list, but rather to illustrate that the Commission’s proposed action has the potential to affect far more than just wireless carriers, corrections officials, CIS vendors, and inmates. The Commission must consider the needs of everyday consumers, how they have the potential to be impacted by the proposed rules, and how it can protect these consumers while still achieving the critical objective of this proceeding: to prevent and stop the use of cell phones by inmates in correctional facilities.

This is particularly important because a consumer whose service is terminated (or whose device is disabled) because of errors in the contraband phone enforcement process is in a far worse position than a consumer whose device is merely flagged by a CIS capable of blocking transmissions. Under the current framework, when a lawful device is wrongly flagged as unauthorized by a CIS capable of blocking transmissions, any service disruption will be temporary and service will automatically resume once the consumer moves out of the CIS’ range. While this is undoubtedly an inconvenience for such affected customers – particularly if it is their residence that is within the CIS’ range – it is a less severe result than what is now proposed by the Commission. Specifically, what the Commission proposes is either a termination of service or disabling of consumer devices that would persist until the consumer informs their carrier of the error and the carrier restores service and/or replaces the user’s device.

After The Sun relayed the complaints to Tecore, the company then tested cell phone calls made outside the jail walls, an official said. . . . In a test, a Baltimore Sun reporter drove around the city jail Saturday while making calls on a Verizon cell phone and an AT&T cell phone. All the calls went through normally.”).

Simply moving out of range of the CIS would not be sufficient to restore normal device or service operations if the device is associated with a lawful user with freedom of movement. The restoration of service would take more time and would place an unfair burden upon a law-abiding user. Such an outcome clearly is not in the public interest. On countless occasions, the Commission has enumerated the many essential everyday functions supported by wireless connectivity, ranging from communicating with one's children to facilitating proper use of medication. For this reason, any rule that risks erroneously and wrongly terminating law-abiding consumers' wireless service is extremely harmful to the public interest.

IV. USE OF A COURT ORDER PROCESS WILL CURB CONTRABAND DEVICE USE WHILE PROTECTING LAWFUL USERS.

A better way to address usage of contraband devices without risking improper termination of service for lawful consumers is to utilize the court order process for service termination. This process should ensure a high degree of accuracy in the list of contraband devices identified. Furthermore, the court order process is an extremely familiar one for law enforcement and wireless carriers alike and, despite claims to the contrary, can be implemented with minimal burden. Finally, the development of an accurate list of identified devices with strong evidentiary support protects stakeholders and promotes the public interest.

A. The Court Order Process Will Ensure a High Degree of Accuracy in the Termination Process and is Familiar to Stakeholders.

AT&T's support of a court order process can be explained with two words: accuracy and familiarity. Use of a court order will help ensure that a list of identified contraband devices is *accurate* because it will be supported by a court's finding of sufficient evidence. And, because this process utilizes existing criminal and civil procedures, it is *familiar* to the law enforcement community and wireless carriers alike.

By requiring a court order, the Commission would help ensure that any request to terminate service to a suspected contraband device (or disable the device) meets an evidentiary standard sufficient to ensure that lawful device users have not been erroneously captured. The Commission has asked for specific comment on the particulars of the requested court-ordered process.¹¹ AT&T envisions that a corrections institution would conduct an investigation based on the devices identified by their CIS to confirm that they are, in fact, contraband and that lawful users have been excluded.¹² These corrections officials would then present their evidence to a court of relevant jurisdiction, which would issue an injunction or similar order. AT&T would be willing to comply with appropriate subpoenas that may need to be issued by the court in the course of making its determination.¹³ Upon receipt of a valid court order, the relevant wireless carrier would promptly terminate service to the device. Because the court order will be supported by an evidentiary finding, corrections officials and carriers alike would have a reasonable assurance that they have targeted only prohibited uses.

A court order process will also facilitate accuracy because it will enable carriers to share information that could be relevant to a determination of whether a phone is contraband. CIS

¹¹ *Further Notice* at ¶ 84.

¹² Outside of the court order process, AT&T is happy to work with corrections officials who request AT&T's assistance to ensure that their CISs are generating accurate results.

¹³ To the extent that corrections officials require supplementary information from carriers regarding their subscribers and their wireless use, a court order process would likely be required due to the need to protect customer privacy and to comply with the restrictions on the disclosure of information relating to the location of a telecommunications service made available to a customer and other Customer Proprietary Network Information ("CPNI") under Section 222 of the Communications Act. *See* 47 U.S.C. § 222(c) (allowing the disclosure of CPNI where "required by law").

operators' visibility into wireless device operation is necessarily limited – they will only receive information regarding devices that register on the CIS, and will not know if those same devices regularly move in and out of the CIS' range. If a device regularly registers on carrier towers outside the range of a CIS, that suggests that the device may have been identified in error.¹⁴ It is likely that wireless carriers will be in possession of evidence that disputes a CIS vendor's finding that a particular device is unauthorized. By requiring a court order, the Commission will create a framework within which wireless carriers can share relevant evidence with law enforcement without violating rules governing customer privacy. Absent a court order process, due to consumer privacy concerns wireless carriers likely will not be able to share information that could be highly relevant to whether a device is actually contraband, or whether it has been identified in error. This "feedback loop," which is only possible when judicial procedures are used, could be critical in eliminating false positives and creating an accurate list of unauthorized devices.

In addition to promoting accuracy, a court order process is logical because it serves as a means of enforcing existing state criminal law. Use of a court order process would allow those states that have elected to criminalize the use of wireless devices in correctional facilities to enforce such laws. And, by enforcing criminal laws, states will help fulfill a key purpose of criminal law – to prevent criminal behavior in the first place. As the Commission notes in the *Further Notice*, the majority of states, plus the District of Columbia, have enacted state laws

¹⁴ Of course, a device could move freely in and out of a correctional facility and still be used for an unauthorized (and potentially illegal) purpose while inside the correctional facility.

making possession and/or use¹⁵ of wireless devices in correctional facilities a crime.¹⁶ To the extent a state has not criminalized the use of wireless devices by inmates in correctional facilities, but the phone is being used in furtherance of a crime, this process similarly would preserve the relevant state's authority to enforce its criminal laws. And, to the extent that use of a contraband device by an inmate is a criminal violation in a state – or the inmate is using the device in furtherance of a crime – this process will help to facilitate the prosecution of those individuals found to be in violation of applicable state statutes, *including* individuals or groups responsible for smuggling contraband phones into prisons in the first place.

The court order process is a highly familiar one for wireless carriers and law enforcement officials alike. All of the key stakeholders in this proceeding are extremely familiar with the process of obtaining and responding to a court order. AT&T, in fact, employs a team of personnel who routinely review and respond to lawful subpoenas and court orders. In 2016, AT&T received and responded to over 27,000 court orders for historic or real-time customer

¹⁵ To the extent a state has criminalized not only the use of a wireless device in a correctional facility, but also the *possession* of such a device, AT&T notes that this process supports only the enforcement of the former, not the latter. Even after service is terminated to an identified device and/or the device is disabled, the inmate will still presumably be in physical possession of the device unless and until a corrections facility implements a program to physically locate and confiscate the device.

¹⁶ *Further Notice* at n. 36. Additional states are in the process of adopting their own criminal laws. *See, e.g.*, H.B. 207, 99th Gen. Assem., First Reg. Sess. (Mo. 2017) (proposing that “[a] person commits the offense of possession of unlawful items in a prison or jail if such person knowingly delivers, attempts to deliver, possesses, deposits, or conceals in or about the premises of any correctional center . . . [a]ny two-way telecommunications device or its component parts”); S.B. 99, 53rd Leg. Sess. – First Sess. (N.M. 2017) (proposing that possession of contraband – including electronic communications devices – by a prisoner is a misdemeanor).

records and over 36,000 search warrants or probable cause court orders.¹⁷ And also in 2016, AT&T received and responded to over 174,000 criminal subpoenas.¹⁸ Similarly, corrections officials and other law enforcement/public safety officials are extremely familiar with the process of obtaining a court order. As such, the additional burden on corrections facilities and officials should be minimal. As noted above, AT&T has dedicated staff in place to process requests in connection with the court order process and can expeditiously process requests as needed. And, in any event, the public interest benefits of using a court order process far outweigh any additional administrative burden imposed. The termination of service to or disabling of a device due to a violation of a state law barring possession or use of a device in a state correctional facility is essentially a law enforcement activity—it is not unreasonable to require that a court consider the evidence of such crimes before requiring third parties to take such actions.¹⁹

B. An Accurate List With Strong Evidentiary Support Protects Stakeholders and Promotes the Public Interest.

Thus far in the instant proceeding, the debate over whether a court order should be a required to terminate service or disable a device has centered around concerns of civil liability by wireless carriers.²⁰ In the *Further Notice*, the Commission has asked for specific comment on why a court order process would address liability concerns while termination pursuant to a

¹⁷ AT&T Transparency Report, at <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html> (last visited June 19, 2017).

¹⁸ *Id.*

¹⁹ AT&T also notes the potential for the Commission’s proposed framework – which would not use formal legal processes – to violate the due process rights of affected wireless users.

²⁰ *Further Notice* at ¶ 82.

Commission directive would not.²¹ While a court's finding of sufficient evidence to justify termination of service certainly helps shield carriers and CIS operators from liability in the event a lawful device is flagged in error, this process also serves to prevent the sorts of injuries that would give rise to civil litigation in the first place.

With respect to the liability protection afforded by a court order process, the answer is simple: a court order will not be issued unless a court reviews relevant evidence and determines that the evidence supports the assertion that a device is contraband. And, as a practical matter, if an assertion that service is being used in violation of state criminal law serves as the basis for a carrier's authority to terminate service to a device (or disable a device), then it is not unreasonable to require that a court consider the evidence of the assertion. The alternative process proposed by the Commission would require instead that wireless carriers act upon another party's representation that they believe a device to be contraband or, in the alternative, conduct their own independent investigation. A court order is a clear-cut directive that serves to provide clarity and certainty to stakeholders regarding the actions required in connection with a specified wireless device.

V. AT A MINIMUM, A QUALIFYING REQUEST SHOULD INCLUDE CERTAIN CERTIFICATIONS TO PROTECT LAWFUL USERS.

If the Commission nonetheless adopts a rule requiring carriers to disable devices without a court order, any qualifying request under that rule should be required to meet certain criteria and include certifications that will help promote the development of an accurate list of identified devices.

²¹ *Id.* at ¶ 83.

First, a qualifying request should be issued by somebody with the authority and incentive to ensure that a list of identified contraband devices is correct. The Commission appears to agree, noting that a “state or local official responsible for the correctional facility” “arguably has more responsibility and oversight in the procurement of a CIS for correctional facilities than a warden or other prison official or employee.”²² The official issuing a qualifying request should be a corrections official and not a CIS vendor, and should be a corrections official of sufficiently high rank to be invested in the accuracy of the list. In addition, this individual should be required to make a series of certifications as part of the qualifying request.

In the *Further Notice*, the Commission asks whether a qualifying disabling request should include “a number of certifications by the [Designated Correctional Facility Official ‘DCFO’]” and provides a list of proposed certifications.²³ As a general matter, AT&T believes that the individual issuing the qualifying request should be required to certify that they have undertaken reasonable efforts to ensure that the list of devices submitted to a carrier is valid and has been scrubbed of devices that likely are not in the possession of inmates. At a *minimum*, AT&T believes that certification as to the following “reasonable efforts” would help to promote an accurate list:

- The DCFO has articulated the law being violated by the use of the phone;
- The DCFO has determined that the device has been identified by the CIS on multiple occasions over a specified period of time, thus minimizing the possibility that a mere passer-by has been captured by the CIS;
- The DCFO has taken all available steps to ensure that the device does not belong to a prison employee or contractor;

²² *Further Notice* at ¶ 99.

²³ *Id.* at ¶ 100.

- The DCFO has determined that to the extent a device has been captured by the CIS on multiple occasions, there are not significant temporal gaps consistent with the device moving on and off the property (which would suggest the device is not in the possession of an inmate);
- The DCFO has determined that the device was not detected in location(s) that are off-limits to inmates (i.e., the parking lot); and
- The DCFO has supplied contact information and/or a process for customers and carriers who wish to dispute the finding that their device was unauthorized.

This proposed list of certifications is not intended to be exhaustive, but rather illustrative of the importance of accuracy in the list generated by the DCFO. By requiring the DCFO to make a series of certifications, the Commission will create strong incentives for the DCFO to thoroughly vet the list of identified contraband devices and ensure that steps have been taken to exclude devices not accompanied by supporting evidence of their contraband nature, or that are supported by evidence that they are *not* contraband. This, in turn, will protect law-abiding wireless customers and the public interest.

VI. CONCLUSION

AT&T has fought and will continue to fight the use of contraband phones in correctional facilities, and will continue to devote substantial resources to this effort. As the Commission considers additional rules, it should take care to ensure that any processes adopted be efficient, feasible, and protective of the rights of lawful users. It is for this reason that AT&T favors a court order as a condition precedent to any required intervention by a carrier, as well as rules that focus on termination of service instead of device disabling. AT&T believes that the policies articulated herein will greatly assist in the identification and cessation of contraband phone use and promote the public interest.

Respectfully Submitted,

/s/ Jessica B. Lyons

Jessica B. Lyons
Michael P. Goggin
Gary L. Phillips
David L. Lawson
AT&T Services, Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
202-457-2100
Its Attorneys

June 19, 2017