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

SECOND REPORT AND ORDER AND SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: July 12, 2021 **Released: July 13, 2021**

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

By the Commission: Acting Chairwoman Rosenworcel issuing a statement.

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 3
III. SECOND REPORT AND ORDER 9
A. Disabling Contraband Wireless Devices in Correctional Facilities 12
1. Designated Correctional Facility Official Requirements 17
2. Authorization of Contraband Interdiction Systems 21
a. CIS Certification Process 22
b. Site-Based Testing and Self-Certification Requirement 30
3. Qualifying Requests 39
4. Disabling Process 49
B. Notification to Managed Access System Operators of Wireless Provider Technical Changes 63
IV. SECOND FURTHER NOTICE OF PROPOSED RULEMAKING 75
A. Quiet Zones 77
B. Geolocation-Based Denial and Carrier Network-Based Solutions 80
C. Beacon Technology 84
D. MAS Evolved and Future CIS Use Cases 86
V. PROCEDURAL MATTERS 90
VI. ORDERING CLAUSES 94
Appendix A—Final Rules
Appendix B—Final Regulatory Flexibility Analysis
Appendix C—Initial Regulatory Flexibility Analysis
Appendix D—List of Commenters

I. INTRODUCTION

1. Congress has long focused on the need to address use of contraband devices to engage in activity that endangers prison employees, other incarcerated people, and members of the public.[1] In an Explanatory Statement to the 2021 Consolidated Appropriations Act, Congress urged the Commission to act on its 2017 *Further Notice of Proposed Rulemaking* in this proceeding[2] and "adopt a rules-based approach . . . that would require immediate disabling by a wireless carrier upon proper identification of a contraband device."[3] Furthermore, Congress encouraged the Commission to explore additional measures to address this important issue.[4]

2. In this *Second Report and Order*, we act upon this Congressional concern by taking further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. We adopt a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria, and we address issues involving oversight, wireless provider liability, and treatment of 911 calls. We adopt rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness. Consistent with Congress's guidance in the 2021 Consolidated Appropriations Act Explanatory Statement, in the *Second Further Notice of Proposed Rulemaking*, we seek further comment on the relative effectiveness, viability, and cost of additional technological solutions to combat contraband phone use in correctional facilities previously identified in the record.[5]

II. BACKGROUND

3. For decades, wireless devices, including cell phones, have been smuggled into correctional facilities nationwide.[6] In some cases, incarcerated people use these devices to engage in a variety of criminal activities posing serious threats to officials and incarcerated people within the facility and innocent members of the public.[7] Federal, state, and local correctional administrators have recognized the need to address the contraband problem in correctional facilities. In 2010, Congress passed the Cell Phone Contraband Act, which prohibited the possession of cell phones in federal prisons by unauthorized persons.[8] Many states have passed laws designating wireless devices in correctional

---

[1] *See, e.g.*, Cell Phone Contraband Act of 2010, Pub. L. No. 111-225 (2010) (amending 18 U.S.C. § 1791) (Cell Phone Contraband Act); Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, 134 Stat. 1182 (Dec. 21, 2020) (2021 Consolidated Appropriations Act).

[2] *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017) (*Report and Order and Further Notice*).

[3] *See* Explanatory Statement to 2021 Consolidated Appropriations Act, Book IV, 166 Cong. Rec. H8311, H8440 (daily ed. Dec. 21, 2020) (2021 Explanatory Statement).

[4] *See id.* ("The FCC should consider all legally permissible options, including the creation, or use, of 'quiet or no service zones,' geolocation-based denial, and beacon technologies to geographically appropriate correctional facilities."); Letter from Senator James Lankford et al., to The Honorable Chairman Pai, Chairman, FCC, GN Docket No. 13-111 (Sept. 16, 2020) (Sept. 2020 Senators' Letter).

[5] *See* 2021 Explanatory Statement at H8440.

[6] U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspections Division 16-05, Review of the Federal Bureau of Prisons' Contraband Interdiction Efforts, at 1 (June 2016), https://www.oversight.gov/sites/default/files/oig-reports/e1605.pdf (2016 Department of Justice Contraband Report); U.S. Department of Justice, U.S. Attorney's Office, District of New Jersey, Former Inmate Arrested in Scheme to Use Drones to Smuggle Contraband into Fort Dix Federal Prison, Oct. 13, 2020, https://oig.justice.gov/sites/default/files/2020-10/2020-10-16.pdf.

[7] 2016 Department of Justice Contraband Report at 5; U.S. House of Representatives, H.R. Rep. 115-704, 43 (May 24, 2018). *See* Sept. 2020 Senators' Letter at 2.

facilities as contraband, and a substantial majority impose criminal penalties for possessing contraband wireless devices within correctional facilities. The federal government and various states have been conducting trials and investing in technologies that will enable them to combat contraband wireless device use in correctional facilities.[9]

4. In 2017, the Commission released a *Report and Order and Further Notice of Proposed Rulemaking* that streamlined the process of deploying Contraband Interdiction Systems (CISs) to prevent contraband wireless device use in correctional facilities.[10] The Commission also named a Contraband Ombudsperson to serve as the single point of contact for issues related to contraband wireless devices in correctional facilities and the deployment of technologies used to combat this critical public safety problem.[11] The *Report and Order* eliminated certain filing and regulatory requirements and provided for immediate approval of the lease applications needed to operate these systems.[12] In addition, the *Report and Order* provided for community notice of CIS deployment, required good faith lease negotiations between wireless providers and solutions providers, and addressed enhanced 911 (E911) issues.[13] The *Further Notice* sought additional comment on a broad range of steps the Commission could take to help eliminate the threat to public safety caused by contraband devices.[14] In particular, it sought comment on a process for wireless providers to disable contraband wireless devices once they have been identified.[15] The *Further Notice* also sought comment on additional methods and technologies that might prove successful in combating the use of contraband devices in correctional facilities and on various other proposals related to the authorization process for CISs and the deployment of these systems.[16] The Commission received 18 comments and 10 reply comments in response to the *Further Notice*.[17]

5. In February 2018, the Commission convened a diverse group of stakeholders—including state corrections officials, solutions providers, public safety experts, the wireless industry, and the Federal Bureau of Prisons—to address ways to leverage technological solutions to combat contraband devices in

(Continued from previous page)

[8] *See* Cell Phone Contraband Act. The Cell Phone Contraband Act became law on Aug. 10, 2010.

[9] *See* U.S. Department of Justice, Office of Public Affairs, Prison Test Shows Micro-Jamming May Counter Criminal Threat of Contraband Cell Phones (June 15, 2018), https://www.justice.gov/opa/pr/prison-test-shows-micro-jamming-may-counter-criminal-threat-contraband-cell-phones; U.S. Department of Justice, Office of Public Affairs, Bureau of Prisons Tests Micro-Jamming Technology in South Carolina Prison to Prevent Contraband Cell Phones (April 12, 2019), https://www.justice.gov/opa/pr/bureau-prisons-tests-micro-jamming-technology-south-carolina-prison-prevent-contraband-cell. Recently, the Federal Bureau of Prisons conducted pilot tests of micro-jamming technology to determine if cellphone detection and interdiction technologies could prevent wireless communication by incarcerated people using contraband cellphones. Technological solutions currently used by state correctional facility administrators to combat contraband wireless devices include: managed access, a technology capable of intercepting calls and dropping those made from contraband phones, and detection systems, that either passively obtain identifying information only when a contraband phone is in use, or that actively cause the contraband phone to provide identifying information even when not in use.

[10] *See Report and Order*, 32 FCC Rcd at 2348, 2356-57, paras. 28, 52-53.

[11] *See id.* at 2365-66, para. 78 (creating the Contraband Ombudsperson); *see also Wireless Telecommunications Bureau Names Ombudsperson for Issues Related to Combating Contraband Wireless Devices*, Public Notice, 32 FCC Rcd 2053 (2017) (*Ombudsperson Public Notice*) (naming Charles Mathias as the Contraband Ombudsperson; he can be reached at combatcontrabanddevices@fcc.gov or 202-418-1030).

[12] *Report and Order*, 32 FCC Rcd at 2337, para. 1.

[13] *Id.* at 2353-54, 2360, 2364, paras. 44-45, 63, 74.

[14] *Further Notice*, 32 FCC Rcd at 2337, para. 2.

[15] *Id.*

[16] *Id.*

[17] Parties that filed comments and reply comments in the proceeding are listed in Appendix D.

correctional facilities.[18] Participants were asked to provide input regarding effective, affordable, and safe ways to address the contraband device problem.[19]

6. In April 2018, CTIA, together with the Association of State Correctional Administrators (ASCA) and the Federal Bureau of Prisons, formed the Contraband Phone Task Force to examine potential technological, legal, and administrative challenges and solutions to combat contraband devices while accounting for the interests of legitimate wireless users.[20] In April 2019, the Contraband Phone Task Force submitted to the Commission a Status Report providing a summary of its activities to date related to the Task Force's charge.[21] The Status Report included the "Contraband Interdiction System Testbed Report and Best Practice Recommendations," which was prepared by the Virginia Tech Applied Research Corporation and which provided technical assessments of different CIS technologies used to reduce or prevent the unlawful use of contraband devices in correctional facilities.[22]

7. On June 19, 2019, the Commission submitted to the House and Senate Appropriations Subcommittees on Financial Services and General Government a review of the Contraband Phone Task Force Status Report,[23] highlighting recent industry developments related to the issue of preventing contraband cell phone use in our nation's correctional facilities.[24] On April 27, 2020, the Commission submitted to the Senate Committee on Appropriations its "Report on Developments in Addressing Contraband Phone Use in Correctional Facilities"[25] to comply with the Senate Report accompanying the Financial Services and General Government Appropriations Bill of 2020.[26] The Commission's April 2020 Contraband Phone Report described coordination among the Contraband Task Force, managed access system (MAS) vendors, and wireless providers on "MAS Evolved" developments,[27] and described recent Commission actions to facilitate next steps.[28]

---

[18] *See* Press Release, FCC, Chairman Pai Convenes Meeting to Discuss Combatting Contraband Wireless Devices in Correctional Facilities (Feb. 7, 2018), https://docs.fcc.gov/public/attachments/DOC349082A1.pdf.

[19] *Id*.

[20] The Contraband Task Force is comprised of CTIA, the Correctional Leaders Association f/k/a ASCA, the Federal Bureau of Prisons (an ex officio member), various wireless providers, and state corrections officers from various individual states. The Task Force has been examining the technological, legal, and administrative challenges and solutions to combat this serious problem.

[21] CTIA and ASCA, Contraband Phone Task Force Status Report, at 1 (Apr. 26, 2019), https://api.ctia.org/wp-content/uploads/2019/04/Contraband-Phone-Task-Force-Status-Report-Combined.pdf (Contraband Phone Task Force April 26, 2019 Status Report).

[22] *Id.*

[23] Federal Communications Commission, Review of the Contraband Phone Task Force Status Report (June 19, 2019) (FCC June 2019 Contraband Phone Status Report).

[24] FCC June 2019 Contraband Phone Status Report. The Commission's June 2019 Report detailed recent industry developments to prevent contraband cell phone use in our nation's correctional facilities; summarized the 2019 Task Force Report submitted by CTIA, the Wireless Association, and the Association of State Correctional Administrators (ASCA); and provided an update on ongoing Commission efforts in this area.

[25] Federal Communications Commission, Report on Developments in Addressing Contraband Phone Use in Correctional Facilities (April 27, 2020) (FCC April 2020 Contraband Phone Report).

[26] S. Rep. 116-111 at 64 (2019) (Senate Report).

[27] MAS Evolved systems are designed to work with wireless networks that use advanced 4G and 5G technologies. A MAS Evolved system becomes a roaming partner to the network it monitors and blocks calls by keeping them from authenticating on the network—just as any network would block a device without appropriate credentials. These systems can be easily upgraded as service providers add new technologies and frequency bands.

[28] *See* April 2020 Contraband Phone Report. The Commission explained that it had conducted a series of separate conference calls with major MAS vendors and CTIA members on the status of MAS Evolved and other relevant

(continued….)

8. In July 2020, the Wireless Telecommunications Bureau (the Bureau) issued a Public Notice to refresh the record on the proposals and questions raised in the *Further Notice*, and it invited comment on the successes and challenges of currently employed solutions and those under further review and development.[29] The Commission received 12 comments and four reply comments in response to the *July 2020 Refresh PN*.[30] On December 27, 2020, the Consolidated Appropriations Act of 2021 was signed into law.[31] The Explanatory Statement to the 2021 Consolidated Appropriations Act urges the Commission to act on the *Further Notice* and adopt a rules-based approach to cellphone disabling that would require immediate disabling by a wireless carrier upon proper identification of a contraband device.[32] The Explanatory Statement also encouraged the Commission to consider all legally permissible options to combating contraband cellphone use, including the creation, or use, of "quiet or no service zones," geolocation-based denial, and beacon technologies to geographically appropriate correctional facilities.[33] As of March 2021, Commission records reflect the approval for operation of CIS through lease arrangements for 230 correctional facilities across 27 states.[34]

III. SECOND REPORT AND ORDER

9. In this *Second Report and Order*, we establish rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopt a framework to enable designated correctional facility officials (DCFOs) relying on an authorized CIS to submit qualifying requests to wireless providers to disable contraband wireless devices in qualifying correctional facilities. We find that a rules-based disabling process will provide a valuable additional tool for departments of corrections to address contraband wireless device use in correctional facilities.[35]

10. The framework includes a two-phase authorization process for CIS applicants seeking to deploy CISs that will provide the information necessary for DCFOs to submit qualifying requests to disable contraband devices at correctional facilities consistent with this *Second Report and Order*. In phase one, CIS applicants[36] will submit applications to the Bureau describing the legal and technical qualifications of the systems. In phase two, CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification with the Commission. After both phases are complete, DCFOs will be authorized to submit qualifying requests to wireless providers to disable

(Continued from previous page)
issues, including action items and next steps, and that it had discussed additional issues with state corrections officials. *See also* Letter from Ajit V. Pai, Chairman, FCC, to the Honorable Senator James Lankford (Jan. 15, 2021) (responding to Sept. 2020 Senators' Letter), https://docs.fcc.gov/public/attachments/DOC-369220A1.pdf.

[29] *See Wireless Telecommunications Bureau Seeks to Refresh the Record on Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Public Notice, 35 FCC Rcd 7910 (2020) (*July 2020 Refresh PN*); 85 Fed. Reg. 49998 (Aug. 17, 2020).

[30] Parties that filed comments and reply comments in the proceeding are listed in Appendix D.

[31] *See* 2021 Consolidated Appropriations Act.

[32] *See* 2021 Explanatory Statement at H8440.

[33] *Id.*

[34] *See* https://www.fcc.gov/contraband-wireless-devices (last updated Mar. 16, 2021).

[35] In contrast to our preemption of state tort law liability for certain actions taken pursuant to the rules adopted herein, *see infra* para. 15, our action today does not preempt existing state laws, regulations, or procedures permitting other mechanisms for disabling of contraband wireless devices, and departments of corrections retain the discretion to seek disabling of contraband wireless devices through separate court order processes or other pre-existing state law mechanisms.

[36] The term CIS applicant refers to any entity—including, but not limited to, a solutions provider, equipment manufacturer, or correctional facility—that seeks system-level certification of a CIS and/or authority to operate a CIS at a correctional facility pursuant to the authorization process described in this *Second Report and Order*.

contraband devices using approved CISs at each correctional facility. We also describe the qualifications for DCFOs and establish clear requirements for the submission and processing of qualifying requests.

11. In addition, we require wireless providers to notify certain types of CIS operators of major technical changes, as described below, to ensure that CIS effectiveness is maintained. These rules will provide law enforcement with the tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threats posed by the illegal use of such devices.

A. Disabling Contraband Wireless Devices in Correctional Facilities

12. In this *Second Report and Order*, we adopt an approach whereby wireless providers will be required to disable devices identified by authorized CIS facilities upon receiving a qualifying request from a DCFO. To implement this approach, we: (1) define the necessary qualifications for DCFOs; (2) describe a rigorous two-step certification process for CIS use at qualifying correctional facilities; and (3) establish a clear and efficient process for submitting qualifying requests to disable contraband devices to the appropriate wireless providers. We find that this approach will facilitate rapid and efficient disabling of contraband phones, while also maintaining high standards for disabling requests to ensure the integrity and accuracy of the process.

13. In the *Further Notice*, the Commission sought comment on a rule-based process for disabling contraband wireless devices provided certain criteria are met, including a determination of system eligibility and a validation process for qualifying requests that is designed to address many wireless provider concerns.[37] While the Commission in the *Further Notice* recognized that wireless providers commenting in the record at that time favored a court-ordered disabling process, it anticipated that court orders might be unnecessarily burdensome and might not provide a viable nationwide solution. The Commission therefore sought comment on how a court-order process could be implemented efficiently, given that such an approach would require CIS providers and wireless providers to "navigate the myriad fora through which requests for termination might flow, potentially requiring engagement with a wide variety of state or federal district attorneys' offices; federal, state or county courts; or local magistrates."[38] The Commission sought comment on why disabling pursuant to a federal requirement would not address any concerns as well as disabling pursuant to a court order. It also asked commenters to provide specific examples of successful court-ordered disabling and to demonstrate that court orders could be effective at scale without becoming overly burdensome or time-consuming.[39]

14. CIS providers and the corrections community overwhelmingly support a rules-based disabling process as the most effective and efficient approach.[40] Although wireless providers continue to prefer a court order process,[41] more recently they have acknowledged that certain jurisdictions do not have the time or resources to issue court orders and that a rule-based framework could be designed in a way that is efficient, straightforward, and that replicates the accuracy and accountability of the court order process.[42] CenturyLink responded to wireless providers' concerns by arguing that "Commission rules

[37] *Further Notice*, 32 FCC Rcd at 2367-68, paras. 83-84.

[38] *Id.* at 2368, para. 84.

[39] *Id.* at 2367-68, paras. 83-84.

[40] Correctional Leaders Association Refresh PN Comments at 2-4; OmniProphis Refresh PN Comments at 4-5; ShawnTech Refresh PN Comments at 1; ACA FNPRM Comments at 3; ASCA FNPRM Comments at 2; Arizona Department of Corrections FNPRM Comments at 1; Tennessee Department of Corrections FNPRM Comments at 1; ShawnTech FNPRM Comments at 1; Global Tel*Link FNPRM Comments at 10; CoreCivic FNPRM Comments at 2.

[41] T-Mobile Refresh PN Comments at 4-6; T-Mobile Refresh PN Reply at 2-3; AT&T Refresh PN Comments at 4; AT&T Refresh PN Reply at 4; AT&T FNPRM Comments at 2-3; CTIA FNPRM Comments at 5-6; CTIA FNPRM Reply at 3; T-Mobile FNPRM Comments at 5-8; T-Mobile FNPRM Reply at 10-14; Verizon FNPRM Comments at 4; *see also* Cell Command FNPRM Comments at 15 (arguing that court orders should be used, at least initially, until liability and privacy concerns can be addressed through a rule-based approach).

defining a qualifying request and identifying who is authorized to make such requests would provide sufficient protection against the risk that those lawfully using wireless devices will have their service terminated or devices disabled."[43]

15. We find that the rule-based disabling process we adopt today provides an efficient and effective means for stakeholders to address the issue of contraband device use and that such an approach includes the same safeguards against erroneous disabling and potential wireless provider liability as would a more burdensome and time-consuming court order process. Although it is not clear from the record that wireless providers are in fact exposed to any such form of liability, we agree with commenters that argue that a federal rule requiring wireless providers to disable devices identified pursuant to a Commission-established process would provide the same protection from such liability as a court order requiring the same action.[44] Where states have criminalized contraband wireless device possession or operation, the rules we adopt here will require wireless providers to treat all qualifying requests that comport with the Commission's rules as valid and, within two business days of receiving the request, without further review, disable such devices at both the subscription- and device-level.[45] In light of this mandate that wireless providers must act upon, and pursuant to the Commission's well-established authority, we preempt any state liability for wireless provider disabling actions that comply with our rules.[46] Such preemption would extend not only to state and local statutes and rules but also to state common-law tort duties.[47]

16. Furthermore, as commenters suggest, we have replicated the aspects of the court-order process—e.g., evidentiary standards, law enforcement participation, validation by state officials—in the rule-based approach we adopt today in order to "balance public safety against the risk of terminating service for legitimate users."[48] We adopt requirements for DCFOs designed to ensure that parties making

(Continued from previous page)

[42] CTIA Refresh PN Comments at 8-10; CTIA Refresh PN Reply at 10-11; Verizon Refresh PN Comments at 1-3; T-Mobile Refresh PN Comments at 6-8; T-Mobile Refresh PN Reply at 3-4; AT&T Refresh PN Comments at 8-9; AT&T Refresh PN Reply at 4-6.

[43] CenturyLink FNPRM Reply at 4-5.

[44] GTL FNPRM Comments at 12; GTL FNPRM Reply at 4-5; CenturyLink FNPRM Reply at 4-5; *see also* GTL FNPRM Comments at 12 (arguing that wireless providers would be under no greater liability for terminating service to contraband cell phones than they are for terminating service to stolen wireless devices, as they already do under existing initiatives); *see also* CTIA Refresh PN Comments at 8-9 (arguing that a rules-based framework that replicates the accountability of a court order process would provide wireless providers with liability protection for carrying out the Commission's directives); AT&T Refresh PN Reply at 6 ("A clear, unambiguous directive from the Commission will impose accountability on the process, while making it clear that wireless carriers are acting at the direction of law enforcement and a Federal regulator, not performing their functions on an ad hoc basis.").

[45] These rules lie well within the Commission's broad Title III spectrum-management authority, including to prescribe the terms and conditions of spectrum licenses and the nature of the service to be rendered by wireless providers, to establish areas or zones to be served, and to make rules and prescribe restrictions and conditions as may be necessary to carry out the provisions of the Act. 47 U.S.C. §§ 301, 303(b), (h), (r); *Cellco Partnership v. FCC*, 700 F.3d 534 (D.C. Cir. 2012).

[46] *See, e.g.*, *City of New York v. FCC*, 486 U.S. 57, 63-64 (1988).

[47] *See, e.g.*, *Johnson v. American Towers, LLC,* 781 F.3d 693, 705-06 (4th Cir. 2015) (explaining that state common-law duties that conflict with federal laws or regulations are preempted). We do not extend this liability protection to CIS providers, and, consistent with the requirements we adopt for CIS certification below, emphasize that CIS providers should exercise due care and design their systems and data analysis methodologies in a manner that minimizes to the greatest extent possible the risk of disabling a non-contraband device. *See* Prelude FNPRM Comments at 3-4, 10 (seeking liability protection through a safe harbor for CMRS and CIS providers for issues related to identification, capture, and denial of wireless communication devices captured in the course of normal operations at a correctional facility).

[48] Verizon FNPRM Comments at 4.

disabling requests have the necessary authority and accountability to safeguard the integrity of the process. Further, the rigorous, two-phase process for CIS authorization will ensure that CISs are designed to support operational readiness and to reduce the risk of interference or the disabling of non-contraband devices. Finally, the requirements we adopt for qualifying disabling requests will enable a uniform, streamlined process that clearly establishes criteria necessary to trigger wireless providers' obligation to take action to disable contraband devices. We find that these procedural safeguards will promote the efficiency, accuracy, and integrity of the disabling process.

1. Designated Correctional Facility Official Requirements

17. We adopt requirements for qualifying DCFOs that will ensure parties making disabling requests have the necessary authority and accountability to safeguard the integrity of the contraband device identification and disabling process. Specifically, we require that qualifying disabling requests be submitted by a government official with responsibility for administration of the correctional facility. We also adopt a process for certification of DCFOs that will provide certainty to wireless providers that disabling requests are duly authorized by the relevant federal, state, or local government entities.

18. In the *Further Notice*, the Commission sought comment on whether to require that qualifying requests be transmitted to a wireless provider either by the Commission, upon the request of a DCFO, or by the DCFO directly.[49] The Commission further sought comment on whether to define the DCFO as a state or local official responsible for the facility where the contraband device is located.[50] Some commenters argue that qualifying disabling requests should come directly from the Commission in order to protect wireless providers from potential liability.[51] Other wireless providers, CIS providers, and the correctional community support a process whereby the DCFO may send disabling requests directly to wireless providers, and they argue that the DCFO should be someone with the authority and incentive to ensure that the list of identified contraband wireless devices is correct.[52] Some commenters argue that the definition of DCFO should be limited to state, local, or federal officials with oversight of the correctional facility and the CIS provider,[53] while others argue that CIS providers or wardens and other officials at private prisons also should be eligible to act as DCFOs.[54]

19. We find it in the public interest and more efficient to adopt a rule-based process under which DCFOs transmit qualifying requests directly to wireless providers. Although certain commenters argue that direct transmission from the Commission would give wireless providers greater confidence in the validity and accuracy of the termination request, we find that interposing the Commission in the process at the request transmission stage may cause unnecessary delay, particularly during an exigent circumstance where expedient disabling is justified due to an imminent threat to public safety or the security of the correctional facility or its staff. Furthermore, the two-step process we adopt for CIS certification, coupled with a Commission rule requiring that wireless providers act expeditiously upon

[49] *Further Notice*, 32 FCC Rcd at 2373-74, para. 98.

[50] *Id.* at 2374, para. 98.

[51] CTIA FNPRM Comments at 6; CTIA FNPRM Reply at 3; Verizon FNPRM Comments at 6; AT&T Refresh PN Reply at 6; T-Mobile Refresh PN Reply at 3.

[52] AT&T FNPRM Comments at 15; T-Mobile FNPRM Comments at 8-9; ShawnTech FNPRM Comments at 3; CenturyLink FNPRM Reply at 4; GTL FNPRM Comments at 10; Prelude FNPRM Comments at 7; CoreCivic FNPRM Comments at 2-3 (arguing that requiring a separate Commission order or transmission of the request would "significantly hamper the speed of the termination process"); ADOC FNPRM Comments at 1; FDOC FNPRM Comments at 1; *see also* CTIA FNPRM Reply at 4 (if the Commission allows requests to come directly from DCFOs, such requests must come from a "certified senior state official with oversight of the CIS operator").

[53] CTIA FNPRM Comments at 6; CTIA FNPRM Reply at 4; AT&T FNPRM Comments at 15; T-Mobile FNPRM Comments at 9.

[54] GTL FNPRM Comments at 10; CenturyLink FNPRM Reply at 4; CoreCivic FNPRM Comments at 3.

such requests, provide protections similar to the safeguards that wireless providers argue would be provided if the Commission transmitted the request to the wireless provider. We agree with commenters that argue that qualifying requests should be made by individuals with the authority and incentive to ensure the accuracy of devices identified as contraband. We therefore define an eligible DCFO as an official of the state, local, or federal government entity responsible for administration and oversight of the relevant correctional facility.[55] In government-run correctional facilities, this definition would require the DCFO to be, at a minimum, the official with responsibility for oversight of the relevant facility (e.g., the warden) or higher ranking official; in privately run correctional facilities, the DCFO must be a government official with responsibility for oversight of the facility's performance through contract.

20. We also agree with those commenters suggesting that wireless providers should not be required to conduct an independent investigation to verify the qualifications of the individual transmitting the request.[56] For wireless providers' reference, the Commission will therefore maintain a publicly available list of approved DCFOs who are authorized to transmit qualifying disabling requests. Individuals that seek to be recognized on the Commission's DCFO list must send a letter to the Commission's Contraband Ombudsperson, signed by the relevant state attorney general or, if a federal correctional facility, the relevant Bureau of Prisons Regional Director, that provides the individual's name, official government position, and a list of correctional facilities over which the individual has oversight and management authority. We find that these requirements for DCFOs eligible to send qualifying requests to wireless providers will ensure an efficient process that safeguards the integrity and accuracy of the disabling process. We direct the Bureau to issue a public notice providing additional guidance on the timing and process for adding authorized individuals to the DCFO list.

2. Authorization of Contraband Interdiction Systems

21. A CIS is a system comprised of one or more stations that is used only at a permanent correctional facility and that is designed exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or obtain identifying information from such contraband wireless devices.[57] In this *Second Report and Order*, we establish a two-phase authorization process for CISs that will provide the requisite information necessary for DCFOs to submit qualifying requests to disable contraband devices in correctional facilities. In phase one, CIS applicants will submit applications to the Bureau describing their legal and technical qualifications of the systems they seek to use. The Bureau will review the applications and approve applications that meet the requirements set forth herein. In phase two, CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification to the Commission. Such testing must be consistent with the test plans approved in phase one. After both phases are complete, DCFOs will be authorized to submit qualifying requests, based on information obtained from approved CISs, to wireless providers to disable contraband devices located at applicable qualifying correctional facilities.

[55] *See* AT&T FNPRM Comments at 15; T-Mobile FNPRM Comments at 9; CTIA FNPRM Reply at 4.

[56] T-Mobile FNPRM Comments at 9.

[57] In the 2017 *Report and Order*, the Commission defined Contraband Interdiction Systems as any system "that transmits radio communication signals comprised of one or more stations used only in a correctional facility exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or obtain identifying information from such contraband wireless devices." *See* 47 CFR § 1.9003. This definition was adopted in the context of facilitating lease arrangements required to authorize RF transmitting systems. In this *Second Report and Order*, we adopt a revised definition in the contraband device disabling context that does not specifically require transmission of radio signals, recognizing that certain non-transmitting, passive receive CIS systems may be used to obtain contraband device identifying information for use by DCFOs in submitting a qualifying request for disabling.

a. CIS Certification Process

22. In the *Further Notice*, the Commission sought comment on whether a disabling process for contraband devices should include a required Commission determination of CIS eligibility to ensure the systems detecting contraband wireless devices are designed to minimize the risk of disabling a non-contraband wireless device.[58] The Commission sought further comment on the criteria for determining eligibility, as well as the costs, benefits, and burdens to potential stakeholders of requiring CIS eligibility before qualifying disabling requests can be submitted to wireless providers.[59] Commenters widely support a certification requirement.[60]

23. After review of the record and consistent with the *Further Notice*, we adopt a CIS certification process for approval of CISs to be used in the submission of qualifying requests for disabling. We clarify that this certification process is separate and distinct from the equipment authorization process managed by the Commission's Office of Engineering and Technology.[61] To obtain CIS certification for use in submitting qualifying requests, a CIS applicant must submit an application to the Bureau for review and approval.[62] The application must demonstrate, at a minimum, that: (1) all radio transmitters used as part of the CIS have appropriate equipment authorizations pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility; (3) the methodology to be used in analyzing data collected by the CIS is adequately robust to ensure that a particular wireless device is in fact located within a correctional facility (including specific data analysis benchmarks designed to ensure successful detection, such as rate of detection of contraband versus non-contraband devices, relevant sample size (e.g. number of devices observed and length of observation period); (4) the CIS will secure and protect all information or data collected as part of its intended use; and (5) the CIS will not interfere with emergency 911 calls. The application also must include a description of whether the CIS requires a spectrum or network access agreement (e.g., a spectrum leasing arrangement or roaming agreement) to be authorized to operate. Finally, the application must include a test plan for subsequent site-based testing of each CIS, that must include detailed descriptions and technical specifications to facilitate Commission review of whether the system satisfies its legal requirements and technically functions as anticipated.

24. We direct the Bureau to issue a public notice announcing the date of acceptance of initial filings, describing in detail the information CIS applicants must include as part of their proposed test plans and the procedures for submitting applications, as well as procedures for accepting applications following the initial filing date. The public notice will provide specific filing instructions and additional details on the information that will be required as part of the Phase 1 showing. While we anticipate that input from wireless providers and correctional facilities will be valuable to the Bureau's review of applications, we also recognize that applications are likely to include proprietary or confidential information, as well as sensitive material related to law enforcement. We therefore further direct the Bureau to include in the public notice a process for review of CIS applications by interested stakeholders

[58] *Further Notice*, 32 FCC Rcd at 2372-73, paras. 95-97.

[59] *Id.* at 2372-73, paras. 96-97.

[60] *See, e.g.*, ACA FNPRM Comments at 2-3; AT&T Refresh PN Reply at 5; CellBlox Refresh PN Comments at 6; CTIA FNPRM Comments at 5; CTIA FNPRM Reply at 2; CTIA Refresh PN Comments, Attach. A at 1; Prelude FNPRM Comments at 5-6; ShawnTech FNPRM Comments at 3; T-Mobile FNPRM Comments at 8; Verizon FNPRM Comments at 5.

[61] *Further Notice*, 32 FCC Rcd at 2369, para. 88.

[62] We note that any CIS equipment that requires FCC certification or a Supplier's Declaration of Conformity must also comply with the Commission's rules regarding equipment authorization. *See* 47 CFR § 2.901 *et seq.*

and establish procedures that maintain the confidentiality, to the extent appropriate, of certain categories of sensitive information (e.g., via a Protective Order).[63]

25. We anticipate that applications will reflect a diverse range of technologies and business plans adopted by CIS applicants and, therefore, in determining whether to approve or deny an application for certification, the Bureau will individually review each application to ensure all requirements have been satisfied. After review of the required filings and the comments filed in response to the application, if the Bureau finds that the applicant has satisfied the eligibility criteria and application requirements and that approval of the application is otherwise in the public interest, it will approve and authorize the marketing and sale of the CIS, as certified for ultimate use in qualifying requests for disabling of contraband devices. Such CISs may only be marketed to correctional facilities or entities that will provide contraband interdiction services to such facilities.[64] In addition, we direct the Bureau to maintain a publicly available list of certified CISs on the Commission website.

26. We find that the technical CIS certification requirements will help ensure that the systems for detecting contraband wireless devices are designed to support operational readiness and minimize the risk of disabling a non-contraband device. The Bureau shall base each certification determination on a demonstration that the CIS's overall methodology for system design and data analysis ensures, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling. Commenters support a certification requirement.[65] ShawnTech states that CIS providers should not only be required to attest to compliance with the rules, but also to demonstrate to the Commission such competency.[66] T-Mobile and CellBlox support adopting precise technical and performance standards as part of the eligibility determination to promote CIS accuracy and minimize the CIS's impact on operations outside the facility.[67] We agree that it is in the public interest to ensure the accuracy of CIS for use in requests for disabling of contraband wireless devices. We find, however, that there are a range of possible CIS technical and data analysis approaches to accurately identify contraband devices, and we therefore decline to mandate specific standards in order to allow CIS operators the flexibility to craft technical solutions that can be effective in a variety of correctional facility environments, so long as they can demonstrate that the method ensures against erroneous contraband identifications. Indeed, neither T-Mobile nor CellBlox provide specifics in the record regarding the appropriate technical and performance standards the Commission should apply, and the industry has largely recognized the need for CIS operators to tailor their systems and methodologies to the particular needs and physical characteristics of each correctional facility where a CIS is deployed.[68]

---

[63] *See, e.g.*, 47 CFR §§ 0.459; 0.461.

[64] Phase 1 certification is only required once for a given CIS.

[65] *See, e.g.*, ACA FNPRM Comments at 2-3; AT&T Refresh PN Reply at 5; CellBlox Refresh PN Comments at 6; CTIA FNPRM Comments at 5; CTIA FNPRM Reply at 2; CTIA Refresh PN Comments, Attach. A at 1; Prelude FNPRM Comments at 5-6; ShawnTech FNPRM Comments at 3; T-Mobile FNPRM Comments at 8; Verizon FNPRM Comments at 5.

[66] ShawnTech FNPRM Comments at 2; *see also* T-Mobile FNPRM Comments at 12-13 (recommending that CIS operators should be required to provide the Commission with an engineering study demonstrating that the system, as deployed, can detect a contraband device within a correctional facility and not misidentify phones as contraband that are outside the facilities).

[67] *See* T-Mobile FNPRM Comments at 8 (supporting a certification process "based on precise technical and performance standards designed to ensure the accuracy of the CIS and to prevent interference to service and devices outside the prison"); CellBlox Refresh PN Comments at 6 (recommending "development of a comprehensive and reliable method to ensure each suspected device is actually a contraband device versus one that is simply captured during a short-term test"). *See also* AT&T Refresh PN Reply at 5; CTIA Refresh PN Comments, Attach. A at 1.

[68] *See, e.g.*, Prelude FNPRM Comments at 6; GTL FNPRM Comments at 4; ShawnTech FNPRM Comments at 3.

27. The *Further Notice* envisioned a certification process that would focus on a CIS's overall methodology and would not assess the CIS's characteristics related to a deployment at a specific correctional facility. We will require the proposed test plan section of the application for CIS certification to include a general plan that can be adapted to the specific circumstances of each planned deployment, rather than a specific plan for each correctional facility. We require, at a minimum, that the proposed test plan include detailed descriptions and technical specifications to facilitate review by the Commission and wireless providers. We find that requiring a description of the proposed test plan will ultimately promote efficient CIS deployment and will facilitate Commission review of the systems for operational readiness prior to actual deployment. As stated, subject to the process established by the Bureau for submission and review of confidential filings, stakeholders also will have an opportunity early in the certification process to review and comment on the proposed test plan prior to testing or deployment at a facility.

28. A certification process provides several public benefits. First, the certification process will enable targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan. Second, the certification process will ensure a high level of CIS accuracy by requiring that CIS applicants submit detailed showings and representations establishing that the systems are designed to minimize the risk of disabling a non-contraband wireless device. Third, the certification process will provide greater certainty to officials seeking to contract for these services by validating that eligible CISs have been certified by the Commission and are qualified to be subsequently deployed at specific facilities. Fourth, the certification process will facilitate contracts between stakeholders, including departments of corrections and CIS providers, and appropriate spectrum leasing arrangements where required, typically between CIS providers and wireless providers. The process will provide interested stakeholders an opportunity to review and provide input on CISs and their proposed test plans prior to deployment and will help ensure that operators comply with the terms of their agreements. Verizon agrees that a CIS eligibility requirement will ensure that correctional facilities and their vendors deploy and operate their systems per the terms of their spectrum leases and lease agreements.[69] CTIA also agrees that a CIS certification requirement would ensure that solutions providers abide by the terms of their spectrum leases.[70]

29. We reject Cell Command's argument that an initial determination of eligibility "would be burdensome for CIS providers and correctional facilities seeking to deploy CIS."[71] We find that the disclosures that we require will not impose a significant burden on CIS providers or correctional facilities and in fact the required information, including technical specifications and proposed test plans, should be readily available to a prepared applicant. Moreover, we find that this approval process will further the public interest by ensuring that CISs comply with applicable statutory requirements and Commission rules and by providing interested stakeholders with the opportunity to provide feedback on each CIS prior to deployment. These significant public interest benefits outweigh any minor inconvenience that applicants may experience in preparing their submissions. The certification process we adopt should ensure that CISs are designed to minimize the risk of disabling a non-contraband device, while refraining from imposing additional burdens, such as requiring that CIS operators fully deploy or test the systems prior to obtaining CIS certification.

b. Site-Based Testing and Self-Certification Requirement

30. In the *Further Notice*, the Commission sought comment on whether to require testing or demonstrations at a specific correctional facility prior to making a CIS eligibility determination.[72] The Commission sought further comment on the type of tests that would be appropriate, if commenters supported a testing component for CIS certification.[73] Commenters generally support a requirement that

[69] Verizon FNPRM Comments at 5; *see also* CTIA FNPRM Reply at 3.

[70] *See* CTIA FNPRM Reply at 3.

[71] Cell Command FNPRM Comments at 13.

[72] *Further Notice*, 32 FCC Rcd at 2373, para. 97.

CIS operators test their systems at a given correctional facility in order to become certified for use in the submission of qualifying requests.[74] Prelude further supports periodic re-testing of systems to ensure ongoing accuracy of the CIS, arguing that such additional testing would not be unduly burdensome and should "always be part of a new solution deployment as well as periodic review when dealing with active base stations."[75]

31. We find that implementing an on-site testing and self-certification requirement will help ensure that qualifying requests identify contraband wireless devices accurately and in accordance with relevant legal authorities. We also find it in the public interest to require that a self-certification include the fact that an applicable state or federal criminal statute prohibits the possession or operation of a contraband wireless device within the correctional facility where the CIS is deployed for use. We note that, in some states, possession or operation of mobile devices in correctional facilities may not be explicitly prohibited as a violation of criminal statute.[76] In addition, some states address the possession or operation of mobile devices in correctional facilities pursuant to prison regulations, rather than criminalization under the penal code.[77] Although some commenters argue that CIS operators should be authorized to identify contraband wireless devices for disabling so long as there is at least a state or local agency rule or correctional facility policy prohibiting the use of contraband wireless devices,[78] we agree with commenters that argue that a more stringent policy requiring a state or federal criminal statutory prohibition is appropriate in this context.[79] Given the substantial implications of requiring wireless

(Continued from previous page)
[73] *Id.*

[74] Prelude FNPRM Comments at 6; CTIA FNPRM Comments at 5; T-Mobile Comments at 12-13; Verizon FNPRM Comments at 5; ShawnTech FNPRM Comments at 2-3; *but see* Cell Command FNPRM Comments at 13 (commenting that requiring certification would be unduly burdensome for CIS providers and correctional agencies).

[75] Prelude FNPRM Comments at 6.

[76] For example, in Missouri, South Dakota, and Vermont, possession of wireless devices by incarcerated people in correctional facilities is addressed solely within prison codes of conduct or inmate handbooks and a violation does not carry statutory criminal penalties. *See* Missouri Department of Corrections, Offender Rulebook, https://doc.mo.gov/sites/doc/files/2018-01/offender-rulebook-9-12-14.pdf, at 21 (while not specifically identifying wireless devices as contraband, Conduct Violation 24.1 prohibits "possession of any unauthorized article or substance"); South Dakota Department of Corrections, Policy 1.5.D.4 – Inmate Access to Telephones and Tablets, https://doc.sd.gov/documents/Inmate%20Access%20to%20Telephones%20and%20TabletsT882019.pdf, at 6 (prohibiting possession or use of any unauthorized telecommunication devices by an inmate); Vermont Agency of Human Services, Department of Correctional Services, Directive 410.01 – Facility Rules and Inmate Discipline, https://doc.vermont.gov/sites/correct/files/documents/policy/correctional/410.01-facility-rules-and-inmate-discipline.pdf, at 18 (designating possession of a communications device such as a cell phone as a major inmate rule violation).

[77] For example, the Code of Massachusetts Regulations specifically identifies possession of an unauthorized electronic device as a violation of the Department of Correction's inmate rules, but no state statute criminalizes the possession or use of contraband wireless devices in correctional facilities. *See* 130 C.M.R. § 430.24; *see also, e.g.*, OHIO ADMIN. CODE 5120-9-06, 5120-9-55 (2019) (making possession of contraband a violation of inmate rules of conduct, which pursuant to section 2921.36 of the Ohio Code, OHIO REV. CODE ANN. § 2921.36(E) (2019), includes any "cellular telephone, two-way radio, or other electronic communications device"); 68 NE ADC Ch. 5, § 005 (Nebraska Administrative Code making possession of unauthorized cellular telephones or other electronic communications devices an inmate behavior violation subject to disciplinary action). Similarly, the Minnesota Administrative Code directs correctional facilities to define items considered as contraband, and the Minnesota Department of Corrections' Directives and Instructions Manual defines contraband to include wireless devices. *See* MINN. R. 2920.6000 (2020); Policy Number 301.030(A)(8) (2019).

[78] FDOC FNPRM Comments at 1; CLA Refresh PN Comments at 3-4 (noting that courts in certain states where possession of a contraband device is not illegal are unwilling to issue court orders and arguing that an advantage of a rules-based approach is that phones could be disabled even where possession is not a violation of state law).

providers to disable a contraband device, we find it reasonable to require CIS self-certifications to demonstrate that they are identifying a device used in violation of state or federal criminal statutes. CIS providers operating at correctional facilities located in states where possession or use of contraband devices has not been criminalized in the penal code will not be eligible to make the self-certification required to facilitate the submission of a qualifying request for contraband device disabling. We find that this approach gives appropriate deference to state law determinations on the dangers to public safety associated with use of wireless phones by incarcerated people.[80]

32. *Testing and Self-Certification Process.* In this second phase, a CIS operator—which could be a CIS solutions provider, or a DCFO or other responsible party that deploys its own CIS at a correctional facility[81]—seeking to use the CIS to submit qualifying requests for disabling must test a certified CIS at each location where it intends to operate.[82] Thereafter, the CIS operator must file a self-certification with the Bureau confirming that the testing at that specific correctional facility is complete and successful. We direct the Bureau to issue a public notice establishing the form and procedure for: (1) CIS operators to file CIS certification applications, self-certifications, and periodic re-certification; (2) CIS operators to serve on wireless providers notice of testing and copies of self-certification; and (3) wireless providers to file objections to self-certifications, including required service on CIS operators and DCFOs.

33. Prior to initiating testing at a correctional facility site, the CIS operator must serve notice of the testing on all relevant wireless providers and provide each such provider a reasonable opportunity to participate in the tests. For this purpose, we define relevant wireless providers to include any wireless provider holding a spectrum license that: (1) authorizes operation on the frequencies on which the CIS seeks to detect contraband use; and (2) authorizes service in the geographic area (e.g., census tract, county, PEA, EA, CMA, REAG) within which the correctional facility is located. We direct the Bureau to issue a public notice providing guidance regarding the details of service on a relevant wireless provider, including, for example, the contents, method, and timing of service.

34. Following the testing, and to be eligible for use in conjunction with qualifying requests for disabling, the CIS operator must prepare a self-certification that: (1) identifies the correctional facility where it seeks to deploy; (2) attests that applicable federal or state criminal statutes prohibit the possession or operation of contraband devices within the correctional facility (and includes the applicable federal or state criminal statutory provision); (3) describes the results of on-site tests of the certified CIS conducted at the correctional facility; (4) attests that the on-site testing was performed consistent with the

(Continued from previous page)

[79] AT&T FNPRM Comments at 15; ShawnTech FNPRM Comments at 3. Many commenters argue that a key advantage of the court order process is that it relies on and enforces existing state laws criminalizing possession and/or use of contraband wireless devices. *See* AT&T FNPRM Comments at 2-3; Verizon FNPRM Comments at 4; T-Mobile FNPRM Comments at 14; ShawnTech FNPRM Comments at 1; Corrections.com FNPRM Comments at 5-6.

[80] Although federal law prohibits the possession or use of contraband wireless devices in correctional facilities, *see* 18 U.S.C. § 1791, only CIS providers seeking to deploy at federally-run correctional facilities for use in conjunction with disabling requests may use this provision of the United States Code to meet this specific self-certification criterion. *See id.* § 1791(d)(4) (defining *prison* for purposes of the federal prohibition as "a Federal correctional, detention, or penal facility or any prison, institution, or facility in which persons are held in custody by direction of or pursuant to a contract or agreement with the Attorney General"). CIS providers seeking to deploy at state and local correctional facilities for use in conjunction with disabling requests must demonstrate that a relevant state law criminalizes the possession or use of contraband devices in correctional facilities.

[81] *See* Appendix A, Final Rules (adding definition to section 20.3 of the Commission's rules, 47 CFR § 20.3). Our definition of a CIS operator here seeks to facilitate, where desired, the operation of CIS by the correctional facilities themselves, rather than requiring ongoing involvement of CIS solutions providers.

[82] CIS operators must have authorization to conduct such testing through, for example, a lease to operate on wireless provider spectrum, or a grant of Special Temporary Authority from the Bureau.

approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device; (5) identifies whether any relevant wireless providers participated in the testing and provides proof that the relevant wireless providers were given notice regarding the testing and a reasonable opportunity to participate; and (6) includes proof of any spectrum and/or network access agreement (e.g., a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate at this correctional facility and/or for the system to function effectively. The self-certification submitted by a CIS operator must be accompanied by an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.

35. A CIS operator must serve via electronic means a copy of the self-certification on all relevant wireless providers, and it must subsequently submit the self-certification to the Bureau in accordance with filing procedures to be established by the Bureau. A self-certification submitted to the Bureau must include proof of electronic service on all relevant wireless providers. We find it appropriate to afford wireless providers that receive a self-certification five business days from the certification filing date to submit objections to the Bureau, and any such objections must be served on the DCFO and the CIS operator. Absent objections, the DCFO may submit qualifying requests to wireless providers beginning on the sixth business day after the filing of the self-certification with the Bureau. If an objection is submitted, the DCFO may not submit qualifying requests until the Bureau addresses the objection. After that five-day period lapses, a wireless provider may submit an objection to the Bureau but, until such objection is resolved, it must act on qualifying requests. We direct the Bureau to issue a public notice establishing filing requirements for self-certification filings, as well as procedures for reviewing the filings and for addressing any objections raised by any wireless providers holding a spectrum lease in the geographic area occupied by the correctional facility, consistent with the general requirements we adopt herein.

36. In order to ensure the ongoing accuracy and reliability of a given CIS at a particular facility, we find it appropriate to require periodic re-certification pursuant to the process we adopt today. At least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO for contraband device disabling must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

37. Completion of the on-site testing and self-certification phase of the authorization process allows DCFOs to submit to wireless providers qualifying requests to disable contraband phones at that particular facility. The Commission will update its website regularly to include a list of certified CISs and, for each certified CIS, those correctional facilities where the system has been tested and self-certified for operational readiness and use in qualifying requests. T-Mobile agrees that the Commission should maintain a public list of certified CIS systems and operators that can be used by wireless providers to verify that incoming requests are genuine.[83] We note, however, that the Bureau may suspend CIS certification generally or at a particular facility if subsequent credible information calls into question a system's reliability.

38. To ensure the integrity and proper operation of CISs, we require CIS operators to retain records of all information supporting each request for disabling and the basis for terminating service to each device, for at least five years following submission of the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must also make available all records upon request from the Bureau. Commenters agree that systems should be designed to enable audits and that CIS operators should maintain logs of contraband wireless devices identified by the system and records relating to any erroneously captured devices.[84] We find that requiring CIS operators

[83] T-Mobile FNPRM Comments at 9.

[84] *See* CTIA Refresh PN Comments, Attach. A at 1; Prelude FNPRM Comments at 6.

to maintain records will support robust efforts to identify issues with CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices.

3. Qualifying Requests

39. In the *Further Notice*, the Commission invited comment on what information should be included in a qualifying request to disable contraband devices.[85] The Commission also sought comment on the appropriate format of a qualifying request to streamline the disabling process and to reduce administrative burdens. To refresh the record, the *July 2020 Refresh PN* sought further comment on the appropriate content for qualifying requests.[86]

40. Commenters agree that qualifying requests should include standardized information, including the subscriber and device identifiers and correctional facility information.[87] For instance, T-Mobile maintains that the Commission should establish baseline criteria for which information is included in all termination requests.[88] CellBlox argues that standards should be set for what constitutes a qualifying request.[89] We agree with these commenters and conclude that adopting standardized information for qualifying requests will help expedite transmission and review of the request by the wireless provider, as well as reduce the administrative burden on DCFOs. Although some parties asked the Commission to create a standardized form for qualifying requests,[90] we find that a standardized form would not provide the flexibility sufficient to account for changes in technology and would deny the DCFOs and wireless providers the flexibility to develop solutions tailored to their specific needs. By requiring that qualifying requests include specific information necessary for wireless providers to act upon the request without establishing a standardized form, we provide DCFOs and wireless providers the flexibility to structure the format of the qualifying requests while meeting the goal of facilitating efficient contraband wireless device disabling.

41. We therefore adopt minimum information that must be included in a qualifying request to disable a contraband device. Specifically, the request must include:

- A certification by the DCFO that:
    - a certified CIS[91] was used to gather the contraband subscriber and device

[85] *Further Notice*, 32 FCC Rcd at 2374, para. 100.

[86] *See July 2020 Refresh PN*, 35 FCC Rcd at 7911 (seeking to refresh the record on all aspects of the proposed Commission process).

[87] *See, e.g.*, CTIA FNPRM Comments at 6 (stating that qualifying requests should include IMSI and correctional facility); CenturyLink FNPRM Reply at 4 (agreeing with CTIA that a qualifying request should include a device's IMSI and correctional facility); *see also* CTIA FNPRM Reply at 4 (stating that requests should have a standard format); ShawnTech FNPRM Comments at 3 (supporting a standardized format for a qualifying request that should be agreed upon by the carriers); CoreCivic FNPRM Comments at 2 (noting that qualifying requests should "be based on a common data format and standardized information requirements to reduce the administrative burden on correctional facilities"); Prelude FNPRM Comments at 8 ("A sufficiently fast process for disabling contraband wireless devices requires standardized information shared between DCFOs and wireless providers."); ADOC FNPRM Comments at 2 ("Correctional facilities would benefit from a standardized data sharing and data formatting.").

[88] T-Mobile FNPRM Comments at 9.

[89] CellBlox FNPRM Comments at 3; CellBlox Refresh PN Comments at 7 (stating that stakeholders should contribute to the standard information included in qualifying requests).

[90] Verizon argues that a form with standardized fields should be completed "letter-perfect" as a condition of terminating service. *See* Verizon Refresh PN Comments at 3.

[91] As an additional measure, wireless providers will be able to verify CIS eligibility for use in the submission of qualifying requests and the correctional facilities where the system has been tested and certified for operational readiness by referencing the Commission's designated website.

information populated in the qualifying request;

- the certified CIS was used to identify contraband devices operating in a correctional facility where the CIS has been tested and self-certified for operational readiness and for use in qualifying requests, and the identification of contraband devices occurred within 30 days immediately prior to the date of the qualifying request submission;
- the DCFO has reviewed the list of contraband devices and attests that it is accurate; and
- it is a violation of an applicable state or federal criminal statute to possess or operate a contraband device in the correctional facility.

- The name and address of the correctional facility at which the contraband device(s) was identified.
- A list of contraband wireless devices with identifiers sufficient to: (1) identify the applicable wireless service provider; (2) uniquely describe each of the devices in question at the subscription level; and (3) uniquely describe each of the devices in question at the device level.

42. The DCFO must transmit a qualifying request to a wireless provider using a verifiable and secure transmission method, and a wireless provider must adopt a method, or utilize an existing method, for receiving secured and verified qualifying requests. In the *Further Notice*, we noted that a verifiable transmission mechanism is a reliable electronic means of communicating a disabling request that will provide certainty regarding the identity of both the sending and receiving parties.[92] We received one comment supporting this approach.[93] We also recognize that some wireless providers already have existing secure portals used to receive court-ordered termination requests.[94] Although we do not endorse a particular technology, the transmitting system should contain features to ensure the integrity, authentication, and provenance of the data in the qualifying request. To facilitate this process, we direct the Contraband Ombudsperson to work with wireless providers and DCFOs to coordinate the development of one or more suitable methods for securely transmitting a qualifying request. We find the Contraband Ombudsperson to be ideally situated to interface with stakeholders and assess the costs and benefits of each potential solution.

43. We find that certifications are a simple and efficient mechanism for demonstrating that a DCFO has exercised the due diligence necessary to validate the accuracy of the information being sent to wireless providers. AT&T suggests that a qualifying request should include a certification that the DCFO has "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."[95] Prelude believes that any certifications by the DCFO or his/her representative should be "assume[d] [...] in compliance," allowing the requests to be processed and approved near-instantly.[96] We agree with these commenters and find it

[92] *Further Notice*, 32 FCC Rcd at 2373-74, n.318.

[93] T-Mobile FNPRM Comments at 8-9 & n.18 (agreeing that the request should be transmitted over a verifiable transmission mechanism by authorized individuals).

[94] *See Further Notice*, 32 FCC Rcd at 2370, para. 90 (noting that Verizon indicated that secure web portals already exist to receive court-ordered termination requests). Additionally, CenturyLink potentially supports using an online web portal to process and manage qualifying requests. CenturyLink FNPRM Reply at 5.

[95] AT&T FNPRM Comments at 15. AT&T further notes that certifications incentivize thorough vetting of the list by a state official and ensures that officials not include devices in the list without supporting evidence. AT&T FNPRM Comments at 15-16.

[96] Prelude FNPRM Comments at 7.

in the public interest to require certifications as part of the standardized information for qualifying requests.[97]

44. We find that the requirement that contraband device activity be observed within the 30-day period prior to the date of the submission of a qualifying request appropriately balances various temporal interests. For example, demonstrating that a contraband device has been active in a correctional facility within the past 30 days prevents stale requests, while also affording adequate time to permit a range of CIS technologies to observe the location of contraband phone activity to help determine with a sufficient level of confidence or accuracy whether the device is in fact contraband. We also note that observation of contraband activity within the 30-day period prior to submitting the qualifying request limits the likelihood that a device could be decommissioned by the contraband user and reassigned by the wireless provider to a valid user.[98] Two commenters argue that there should be a detection period, but they offer no opinion on the Commission's proposed observation within 30-day period approach[99] or any other length of time for establishing recent contraband device activity.[100] As stated, we find that requiring the detection to be within the 30-day period prior to submitting a qualifying request is appropriate for determining whether a device has been recently active in a correctional facility.

45. A qualifying request must include a certification indicating that the DCFO has verified the list of contraband devices and attests that it is accurate. This certification represents to the wireless provider that the DCFO has used the certified CIS consistent with its certification and test plan methodology to identify contraband devices operating within the correctional facility. The certification also demonstrates that the DCFO has reviewed the list of identified contraband devices, along with other relevant data gathered by the certified CIS, to verify that none of the identified devices belong to prison staff, contractors, or passers-by, etc. Accordingly, the DCFO must include this certification as part of a qualifying request to help ensure the accuracy of the disabling process.

46. In a qualifying request, a DCFO also must certify that it is a violation of the applicable state or federal criminal statute to possess or operate a contraband device in the correctional facility and must provide the applicable federal or state criminal statutory provision. This certification ensures that, during and after the contraband activity observation period, there exists a state or federal criminal statute in the relevant jurisdiction making it illegal to possess or operate a contraband device. In addition, a qualifying request must include, at a minimum, the name and address of each correctional facility to ensure that the wireless provider can accurately identify the requesting facility.[101]

---

[97] We find that the certification requiring the DCFO to review the list of contraband devices for accuracy addresses AT&T's suggested certification.

[98] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Second Report and Order, 33 FCC Rcd 12024, 12030-31, paras. 15-16 (2018) (establishing a "minimum aging period" of 45 days before number reassignment).

[99] *Further Notice*, 32 FCC Rcd at 2374, para. 100.

[100] AT&T argues that a qualifying request should include a determination "that the device has been identified by the CIS on multiple occasions over a specified period of time" to minimize capture of passers-by. AT&T FNPRM Comments at 15-16. Corrections.com notes that a qualifying request should show evidence of "usage and destination numbers dialed over a period of time." Corrections.com FNPRM Reply at 7. While we adopt a requirement that a contraband device be observed within 30 days prior to submitting a qualifying request in order to prevent stale requests, we decline to adopt a floor requiring a minimum number of observations within that 30-day period, as doing so could create an unnecessarily rigid standard that limits the ability of CIS operators to tailor their technical parameters and analysis methodologies to the particular needs of a given correctional facility. *See* Prelude FNPRM Comments at 6 (commenting that differing accuracy needs of correctional facilities (e.g. those in cities versus those in rural areas) would mean that setting rigid minimum requirements could limit options for certain facilities).

[101] One commenter opined that a qualifying request does not need to include the physical location of a facility because that information is already included in any spectrum lease arrangement(s) between wireless providers and

(continued….)

47. A qualifying request also must include a list of the contraband devices, with identifiers sufficient to uniquely describe the devices at both the subscription- and device-levels, to provide the wireless provider with the information necessary to prevent use of contraband devices on its network and on other wireless provider networks. Although certain commenters propose requiring DCFOs to provide additional information to demonstrate that the devices at issue are contraband,[102] we decline to do so because our two-step authorization process ensures that a certified CIS can identify contraband devices with a high degree of certainty. This process should provide sufficient assurance that the devices listed in the qualifying request are contraband devices that are being used unlawfully. We decline to codify specific identifiers that must be included in a qualifying request, given the broad range of potential identifiers in use across technologies.[103] By requiring, however, that a qualifying request include at least one identifier at the subscription level, and at least one at the device level, we take steps to ensure that complete disabling can occur and limit instances of potential abuse. For example, the record is clear that a solution permitting a DCFO to transmit only a subscription-level identifier could likely result in termination of a subscription, but leave an incarcerated person with a device fully capable of having a different SIM card inserted with new subscriber information. Conversely, merely providing device identifying information for disabling without a subscription-level identifier could likely result in the transfer of subscriber-identifying information to a different, still active device within the correctional facility.[104] We acknowledge there are common mobile identifiers that are used to uniquely identify a contraband device and therefore adopt technology-neutral requirements for qualifying requests to allow the inclusion of any such identifiers, as appropriate, provided the identifiers include subscription- and device-level information as discussed.[105]

48. The minimal information approach we adopt today for a qualifying request incorporates elements of proposals submitted by several commenters.[106] Some proposals would require additional

(Continued from previous page)
the CIS providers. Prelude FNPRM Comments at 8. We recognize that not all CIS technologies rely on lease arrangements for operational authority (e.g., purely passive detection systems), and therefore find that requiring the inclusion of the requesting facility's location will help expedite review of the qualifying request by the wireless provider.

[102] For instance, CTIA's proposed service termination framework would require that a qualifying request to the Commission include factual details supporting that the identified devices have been determined to be contraband. CTIA Refresh PN Comments, Attach. A at 1. CellBlox argues that usage patterns should be included with the contraband wireless device's identification. CellBlox Refresh PN Comments at 7; CellBlox FNPRM Comments at 4. Corrections.com notes that a qualifying request should include "strong evidence that the device is a verifiable contraband device." Corrections.com FNPRM Reply at 7 (also adding that "[n]o single piece of data is enough to make the determination as to whether a phone is contraband or not").

[103] *See, e.g.*, CTIA Refresh PN Comments, Attach. A at 1-2 (noting that a qualifying request should include each device's IMSI and IMEI, among other things).

[104] *See, e.g.*, Prelude FNPRM Comments at 8; CTIA FNPRM Reply at 4-5; CTIA Refresh PN Comments, Attach. A at 2; CLA Refresh PN Comments at 4.

[105] Examples of such identifiers include International Mobile Subscriber Identity (IMSI) and international mobile equipment identifier (IMEI), used by GSM, UMTS, and LTE devices, and electronic serial number (ESN) or Mobile Equipment Identifier (MEID) (replacement for ESN), mobile identification number (MIN), also known as the Mobile Subscription Identification Number (MSIN), and mobile directory number (MDN), used by CDMA devices.

[106] For instance, CTIA argues that the following should be in any qualifying request to the Commission: "a list of contraband devices operating at a correctional facility;" "name and geographic location of the correctional institution;" factual details establishing that the devices in question are contraband; "documentation demonstrating that the equipment and process used complies with the FCC's certification and validation procedures;" each device's IMSI and IMEI, and any other information required by the FCC to "assure itself that the process used complies with the FCC's certification and validation procedures and has a valid, good faith basis;" and "contact information that wireless providers can provide to customers who question the service termination." CTIA Refresh PN Comments, Attach. A at 1-2. AT&T and T-Mobile also favor this approach. AT&T Refresh PN Comments at 4, 8; AT&T (continued….)

information such as a certification that a CIS provider possesses a spectrum lease in good standing and contact information for customers who challenge a device disabling.[107] Much of the information that certain commenters propose to require is addressed by the two-step authorization process and requirements for submitting a qualifying request we adopt today. For instance, the certification requiring that the DCFO has validated the list of contraband devices addresses commenter concerns that the DCFO has conducted the due diligence necessary to ensure that the devices at issue are, in fact, contraband.[108] Additionally, as part of the two-step authorization process, the Commission will verify that the CIS operator is a spectrum lessee in good standing, where such leases are necessary.[109] We therefore find that requiring additional information would not materially improve the accuracy of the qualifying requests. Moreover, we find that requiring additional evidentiary showings would be unduly burdensome for DCFOs and could affect their ability to send a qualifying request expeditiously, particularly during exigent circumstances.[110] However, in making this decision, we emphasize that DCFOs may provide

(Continued from previous page)
Refresh PN Reply at 6; T-Mobile Refresh PN Reply at 3. AT&T believes a qualifying request, at minimum, must include certain certifications by the DCFO, to include articulating the "law being violated by use of the phone;" a determination "that the device has been identified by the CIS on multiple occasions over a specified period of time;" that the DCFO has taken "all available steps" to determine the phone does not belong to prison staff or a contractor; a determination "that to the extent a device has been captured by the CIS on multiple occasions, there are no significant temporal gaps consistent with the device moving on and off the property (which would suggest that device is not in the possession of an inmate);" a determination that the device is "not detected in location(s) that are off-limits to inmates (i.e., the parking lot);" and has supplied "contact information and/or a process for customers and carriers who wish to dispute the finding that their device was unauthorized." AT&T FNPRM Comments at 15-16. CenturyLink thinks a request should include a device's IMSI and the "correctional facility in which the device is operating." CenturyLink FNPRM Reply at 4. T-Mobile argues for qualifying requests that "(i) are associated with certificated CIS and authorized CIS operators, (ii) contain information explaining why specific devices are contraband, (iii) are in writing and transmitted over a 'verifiable transmission mechanism,' and (iv) are issued by individuals authorized by the Commission to make such requests." T-Mobile FNPRM Comments at 8. Verizon advocates that a qualifying request should contain unique device identification information and "certify that: it uses an eligible CIS provider with a validated cell detection system; the CIS provider possesses a spectrum lease in good standing; and it contacted all licensees in the area." Verizon FNPRM Comments at 6. Corrections.com thinks a qualifying request should contain several elements, including historical timeframes during which the phone is used; usage and destination numbers dialed over a period of time; contents of attempted SMS messages; unique identifiers; and, if available, evidence that the device has or has not moved between facilities. Corrections.com FNPRM Reply at 7. In a qualifying request, Prelude would include facility location, type of CIS technology, CIS provider, contraband device data including hardware and SIM identifiers, and subscriber network. Prelude FNPRM Comments at 8. The Florida Department of Corrections states that a request should include device information, data demonstrating that a device is contraband, an interface for accepting or rejecting a request, and a specific timeframe for processing the request. FDOC FNPRM Comments at 1.

[107] *See* Verizon FNPRM Comments at 6; AT&T FNPRM Comments at 15-16; CTIA Refresh PN Comments, Attach. A at 2.

[108] *See, e.g.*, AT&T FNPRM Comments at 15-16 (noting that a qualifying request should demonstrate various steps taken by the designated official to ensure that the device at issue belongs to an inmate and not prison staff or contractors).

[109] *See* Verizon FNPRM Comments at 6. Because the determination of whether a CIS provider possesses a spectrum lease in good standing is part of the two-step authorization process, the certification that a certified CIS was used to gather the contraband subscriber and device information in the qualifying request also covers this concern.

[110] For example, we decline to mandate that a qualifying request include contact information that wireless providers can provide to customers who question the device disabling, as suggested by CTIA. *See, e.g.*, CTIA Refresh PN Comments, Attach. A at 2. Wireless providers must address qualifying requests and are therefore in the best position to resolve a questionable device disabling.

additional, targeted information—at their sole discretion—or upon mutual agreement with the wireless provider.[111]

4. Disabling Process

49. In the *Further Notice*, the Commission invited comment on the various aspects of the disabling process, with the goal of ensuring that qualifying requests are quickly transmitted, verified, and acted upon.[112] Specifically, the Commission sought comment on what steps, if any, a wireless provider should take to verify the information received, whether customer outreach should be part of the process, and the timeframe within which the steps of the disabling process must be taken.[113] The Commission also sought comment on the extent to which wireless providers should be required to investigate whether the device at issue is in fact not contraband.[114]

50. *Overview of the Disabling Process.* We find it in the public interest to adopt a rule-based disabling process designed to further long-standing efforts addressing the threat of contraband wireless devices in correctional facilities. Upon receipt of a qualifying request from a DCFO through a verifiable and secure transmission method, a wireless provider must treat the request as valid. Absent certain limited grounds for rejecting the qualifying request, a wireless provider must take all reasonable and practical steps, as described below, to disable the identified device from being used on its own or another wireless provider's network. A wireless provider must inform the DCFO whether or not the qualifying request has been granted.[115] If a device is disabled, a wireless provider may also subsequently reverse this action if it later determines that the device was identified erroneously as contraband.

51. *Disabling by Wireless Providers Upon Receiving a Qualifying Request and Timeframe for Action*. Upon receipt of a qualifying request from a DCFO, a wireless provider must treat the request as valid provided it meets the Commission-mandated information required for a qualifying request and does not contain an error in the device identifying information preventing the wireless provider from being able to disable the device. We will allow wireless providers to reject, for the relevant device, qualifying requests containing such errors; for example, a request that contains transposed digits identifying a device that is not operating on that wireless provider's network, or where the identifying information correctly identifies a contraband device but is inadvertently included in a request sent to the incorrect wireless provider.

52. Absent these circumstances warranting rejection, we require a wireless provider in receipt of a qualifying request to disable a contraband device so that it can no longer access the wireless provider's network or other provider networks.[116] In particular, absent a rejection for error, a wireless

---

[111] While a wireless provider must address the Commission-mandated criteria in a qualifying request, reviewing the additional information is optional. Furthermore, the inclusion of any such additional information in the qualifying request—whether at the DCFO's discretion or by mutual agreement—does not modify the requirement that wireless providers act on qualifying requests for disabling under the timeframe we discuss below.

[112] *Further Notice*, 32 FCC Rcd at 2375-76, para. 106.

[113] *See id.* at 2376, paras. 107-08.

[114] *See id.* at 2376, para. 107. In the *July 2020 Refresh PN,* the Commission sought additional and updated comments on these aspects to refresh the record. *See July 2020 Refresh PN*, 35 FCC Rcd at 7911.

[115] T-Mobile argues that the Commission must ensure that wireless providers are insulated from liability under section 201 of the Act, which requires wireless carriers to furnish service upon request and prohibits them from blocking calls except in limited circumstances. T-Mobile Refresh PN Comments at 6-7; T-Mobile Refresh PN Reply at 4. For the reasons set forth in this *Second Report and Order*, we have determined that compliance with the rules established herein constitutes just and reasonable practices pursuant to and consistent with sections 201 and 202 of the Communications Act. 47 U.S.C. §§ 201, 202 (prohibiting wireless providers from making "any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service").

provider must, within two business days after receipt of a qualifying request: (1) disable the device at both the subscriber level and at the device level, and (2) take all reasonable and practical steps to prevent that device from accessing other wireless provider networks (e.g., by adding the equipment identifier to the Stolen Phone Database).[117] We recognize that wireless provider actions necessary to effectuate disabling will vary depending on the deployed technology. For example, disabling at the subscriber level might require a wireless provider to disable the Subscriber Identification Module (SIM) card containing the IMSI for devices on a GSM and/or LTE network, and require disabling of the MIN/MSIN and/or Removable User Identity Module, for a device on a CDMA network.[118] For disabling at the device level, the wireless provider would disable, for example, a GSM/UMTS/LTE device through its IMEI, whereas disabling of a CDMA-based device would occur through its ESN/MEID. Wireless providers must take any necessary steps for the applicable technology to disable at both the device level and subscriber level. If the wireless provider is unable to disable the device—either because the qualifying request does not meet Commission rules or due to error in the information provided as described above—the wireless provider must reject the request within two business days of receipt of a qualifying request. We emphasize that these timeframes are maximums; we fully encourage correctional facilities to work with wireless providers to develop special procedures, where necessary, to guarantee more rapid action in exigent circumstances.

53. Commenters largely agree that unique device and subscriber identifiers, such as the IMSI, MIN, IMEI, and MEID, would provide wireless providers with the necessary information to terminate service on their network at both the device and subscriber level.[119] Some wireless providers acknowledge that they have processes and personnel already in place for addressing violations of terms of service that likely could be applied in this context to terminate service to devices identified in qualifying requests.[120] Many commenters also agree that the Stolen Phone Database is a practical means of preventing the contraband device from accessing other carrier networks.[121] The record is mixed on the appropriate timeframe for a wireless provider to respond to a qualifying request. CLA argues that the wireless provider should terminate service within one business day of receiving a request from the FCC.[122] CoreCivic defers to the Commission on time limits, but recommends that the time period be no later than 24 hours to protect public and facility safety.[123] The Florida Department of Corrections supports a

(Continued from previous page)

[116] *See* CTIA Refresh PN Comments, Attach. A at 2; Letter from Scott K. Bergmann, Senior Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Mar. 3, 2021).

[117] For instance, CellBlox suggests that the devices be disabled and entered into the Stolen Phone Database so that they are permanently disabled. CellBlox Refresh PN Comments at 7-8.

[118] Alternatively, subscriber-level disabling could require disabling of the Universal Integrated Circuit Card—a newer version of SIM card that is able to access multiple wireless technologies, including Global System for Mobile Communications (GSM), Long Term Evolution (LTE), Code-Division Multiple Access (CDMA), Universal Mobile Telecommunications System (UMTS), and High Speed Packet Access networks.

[119] CTIA Refresh PN Comments, Attach. A at 2; CellBlox Refresh PN Comments at 7; CTIA FNPRM Comments at 6; CTIA FNPRM Reply at 4-5; CenturyLink FNPRM Reply at 4; CellBlox FNPRM Comments at 4; Prelude FNPRM Comments at 8; Corrections.com FNPRM Reply at 7; GTL FNPRM Comments at 12-13. We note that these various identifiers are examples of device- and subscriber-specific information that could be used to identify a contraband device. Because certain subscriber-specific identifiers can be moved to different devices—e.g., through insertion of a SIM card (containing the IMSI and, if applicable, the MIN) into a new device—the evaluation of whether a device is contraband could be based on any relevant combination of these identifiers, through confirmation of repetitive use in a correctional facility.

[120] *See* AT&T FNPRM Comments 5-8; Verizon FNPRM Comments at 8-9.

[121] OmniProphis Refresh PN Comments at 4-5; CellBlox Refresh PN Comments at 7-8; CTIA Refresh PN Comments at 2; T-Mobile Refresh PN Comments at 8; Verizon FNPRM Comments at 9; Corrections.com FNPRM Reply at 9; GTL FNPRM Comments at 12-13.

[122] CLA Refresh PN Reply at 4.

process requiring action by the wireless providers within one hour of receiving a qualifying request, unless there is a documentable life safety issue justifying immediate termination.[124] Wireless providers do not specify an amount of time that would be sufficient to act on qualifying requests; while some wireless providers state that they can adapt systems they already have in place to terminate service relatively quickly, such systems may not fully achieve the disabling at both the device and subscriber level that we require herein.[125]

54. With the disabling timeframe we adopt today, we seek to balance public safety interests and wireless provider concerns. First, the two-day period for responding to qualifying requests strikes an appropriate balance between the significant public interest benefits of ensuring that contraband wireless devices, given the known dangers associated with their use, are rapidly disabled, and ensuring that wireless providers can perform the steps necessary to disable the device at both the subscriber and device levels. Second, we find that a two-day period is sufficient for a wireless provider to take reasonable and practical steps to prevent an identified contraband wireless device from being used on its own network or another wireless provider's network by, for example, adding the device's equipment identifier into the Stolen Phone Database.[126]

55. With regard to outreach to wireless providers' customers, we neither require nor prohibit a wireless provider from notifying a customer whose phone is being disabled. Under this approach, a wireless provider may immediately disable a contraband phone without any customer outreach, or a wireless provider may choose to contact the customer of record through any available means (e.g., text, phone, e-mail).[127] Prelude believes that, if CIS technology is correctly deployed and regularly tested, no outreach to customers is needed and that such outreach would cause delay.[128] Given the steps we take today in the interest of public safety, we find, on balance, that it is appropriate to give a wireless provider the discretion to decide whether to contact a customer. Although we provide wireless providers with the flexibility to engage in customer outreach, the provider nevertheless must comply with the two-day period for disabling upon receiving a qualifying request.

56. *Notification to the DCFO*. Within two business days of receiving a qualifying request, a wireless provider must notify a DCFO whether the request has been granted.[129] We establish this timeframe to ensure that a wireless provider responds to a DCFO within a reasonable timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected. If a qualifying request is rejected due to lack of compliance with Commission requirements or in a case of an error, the DCFO and wireless provider

(Continued from previous page)

[123] CoreCivic FNPRM Comments at 2.

[124] FDOC FNPRM Comments at 1.

[125] AT&T FNPRM Comments at 5 (stating that "the process of actually terminating service is an extremely quick one"); *see also* Verizon FNPRM Comments at 8-9.

[126] OmniProphis Refresh PN Comments at 4-5 (stating that the Stolen Phones Database is working); CellBlox Refresh PN Comments 7-8 (noting that once determined to be contraband, the devices should be disabled and entered into the Stolen Phone Database so they are permanently denied service).

[127] While this practice is not prohibited, we caution wireless providers that incarcerated people may use this approach to evade device disabling.

[128] Prelude FNPRM Comments at 10. Additionally, Cell Command asserts that carriers "will need to verify the accuracy of the information transmitted and potentially make a determination on whether to involve the customer before a decision is made on disabling." Cell Command FNPRM Comments at 12.

[129] Only one commenter opined on the notification process, but in a different context. Specifically, CTIA submits that wireless providers should not have to notify CIS providers or designated officials of whether they have fulfilled or rejected the request, arguing that a rule requiring wireless providers to comply with qualified requests, as directed by the Commission, would obviate the need for specific notification. CTIA FNPRM Comments at 7.

should attempt to resolve any outstanding issues involved with the rejection.[130] If neither party can resolve the matter, the DCFO can contest the rejection with the Contraband Ombudsperson. Upon receipt of a contested rejection, the Contraband Ombudsperson will conduct outreach and maintain a dialogue with all stakeholders until the issue is resolved.

57. *Reversals*. A wireless provider may subsequently reverse a disabling action if it determines that the device was identified erroneously as contraband. Some commenters would prefer that the Commission be directly involved in reversing the disabling of erroneously identified contraband devices.[131] In lieu of that approach, we believe the wireless provider is in the best position to undertake post-termination error-correction steps. For instance, if after device disabling, the affected customer demonstrates to the wireless provider that he or she is not an incarcerated person and is in possession of the incorrectly disabled device in accordance with the applicable statute, the wireless provider may immediately restore service to the customer, without Commission intervention. If the wireless provider chooses to reverse a disabling, however, it must promptly inform the DCFO of the mistakenly identified device.

58. We also recognize that wireless providers that choose to consider potential reversals of a disabling action may find it useful for the DCFO to be involved in reviewing the validity of a device previously identified as contraband.[132] We therefore provide the option for wireless providers that determine that a device may have been erroneously identified as contraband to request that a DCFO confirm the information provided in a qualifying request pursuant to which the device was disabled. If the wireless provider seeks to trigger the DCFO's involvement, it must provide the DCFO with: (1) the date of the qualifying request, (2) the identifying information provided for the device, and (3) any evidence supporting the wireless provider's belief that the device was erroneously identified—e.g., the customer has presented the device in store stating that it was wrongfully disabled. Upon receipt of such a request, the DCFO should review the qualifying request to determine whether the device in question was erroneously identified and either: (1) confirm the validity of the identifying information contained in the qualifying request, or (2) acknowledge the error and direct the carrier to restore service to the device. In the event the DCFO directs the wireless provider to reverse the disabling, the wireless provider must, within two business days, restore service to the device and reverse any actions taken to prevent the device from accessing other wireless provider networks (e.g., by removing the phone from the Stolen Phone Database). In the event the DCFO does not respond to a request from a wireless provider for review of a qualifying request within two business days, the wireless provider may proceed with reversing the disabling action.

59. To ensure accountability in the disabling process, we require the DCFO to provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed.[133] We direct the Bureau to issue a

[130] We also note AT&T's comment that "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" but will be unable to share it because of consumer privacy concerns, absent a court order process. AT&T FNPRM Comments 11. To the extent that a wireless provider's notification of the rejection to the DCFO may require sharing customer proprietary network information, we find that such sharing would not be a violation of wireless providers' confidentiality obligations under section 222 of the Act. *See* 47 U.S.C. § 222(c)(1) (restrictions on disclosure of individually identifiable customer proprietary network information do not apply where such disclosure is "required by law").

[131] For instance, CTIA advocates for the Commission to develop "a process for correcting any instances in which a consumer's service is erroneously identified as contraband and terminated." CTIA Refresh PN Comments, Attach. A at 2. CTIA also supports asks from T-Mobile and Verizon that the Commission ensure "that there is an effective process without carrier liability for restoring service if a device is mistakenly identified as contraband," among other things. CTIA Refresh PN Reply at 10-11.

[132] *See* Letter from Scott K. Bergmann, Senior Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 3 (filed May 25, 2021).

public notice providing additional guidance regarding the appropriate method for providing such notice to the Contraband Ombudsperson. The Commission will consider such notices in its review of whether to re-certify a given CIS system as part of the required three-year re-certification requirement and may require, as part of any determination, demonstration that the CIS has remedied any system issues that contributed to the erroneous identifications. In its re-certification decision, the Commission will also consider a DCFO's efforts to review a qualifying request at the request of a wireless provider and respond accordingly within two business days.

60. *911 Calls*. The process we adopt today will facilitate the disabling of a contraband phone's ability to be used on any wireless provider network. Notwithstanding today's action, however, section 9.10 of the Commission's rules mandates that wireless providers must transmit all wireless 911 calls, without respect to their call validation process that would otherwise confirm the call is being made from a service-initialized phone prior to transmitting.[134] This requirement, to transmit 911 calls from even non-service-initiated phones, was adopted based on the Commission's determination that ubiquitous 911 service is in the public interest.[135] We note, however, that under these existing rules, a Public Safety Answering Point (PSAP), or a wireless provider acting pursuant to state or local law-enforcement procedures, may block fraudulent 911 calls from non-service-initialized phones pursuant to applicable state and local law enforcement procedures.[136] Similarly, PSAPs have the discretion not to accept 911 calls transmitted from a CIS provider at a correctional facility.[137]

61. *Reporting Requirements*. We decline to impose reporting requirements on stakeholders at this juncture. The two-step certification process we adopt for authorizing CISs will provide the Commission with a substantial amount of information on the general operating design of CISs as well as the specific deployment plans for particular correctional facilities. Further, we establish record retention requirements related to qualifying requests. We believe that the costs and burdens of any additional reporting requirements would therefore outweigh any marginal benefits. We will rely on informal communications among stakeholders and with the Contraband Ombudsperson, as well as marketplace information, for any additional oversight. We may revisit this decision, however, after the Commission and stakeholders have more experience in implementing the disabling process we adopt today.

62. *No Reimbursement for Wireless Providers*. In adopting a disabling process, we reject calls to reimburse wireless providers for device disabling. We reject T-Mobile's arguments that establishing a process for terminating service "will create costs for CMRS wireless providers, including those associated with developing and implementing new processes, as well as hiring new personnel,"[138] and that precedent supports the recovery of costs for complying with public safety service requirements and law enforcement requests.[139] Given our approach, we anticipate that wireless providers will incur

(Continued from previous page)

[133] This notice requirement applies both where the wireless provider independently reverses a disabling and provides notice to the DCFO and where the wireless provider involves the DCFO in determining whether a device was erroneously identified.

[134] *See* 47 CFR § 9.10(b).

[135] One commenter, ShawnTech, would not support a disabling process that would prevent 911 calls. ShawnTech FNPRM Comments at 3. A non-service-initialized phone is a handset for which there is no valid service contract with a provider of the services. *See* 47 CFR § 9.10(o).

[136] *See FCC Clarifies that 911 Call-Forwarding Rule Does Not Preclude Wireless Carriers From Blocking Fraudulent 911 Calls From Non-Service Initialized Phones Pursuant to State and Local Law*, Public Notice, 17 FCC Rcd 21877 (2002); *see also 911 Call-Forwarding Requirements for Non-Service Initialized Phones*, Notice of Proposed Rulemaking, 30 FCC Rcd 3449, 3451-52, para. 5 (2015).

[137] *See* 47 CFR § 9.10(r).

[138] T-Mobile FNPRM Comments at 10-11; T-Mobile FNPRM Reply at 15.

minimal costs in disabling devices included in a qualifying request or in determining error. Additionally, we note that several wireless providers already have internal procedures for disabling contraband wireless devices pursuant to court orders, which could be modified to accommodate a rule-based disabling process,[140] and that court orders for disabling contraband phones do not always include a mechanism for cost recovery. We therefore also decline to adopt requirements for reimbursement of costs associated with receiving secured and verified qualifying requests.

B. Notification to Managed Access System Operators of Wireless Provider Technical Changes

63. To ensure the ongoing effectiveness of MAS, we adopt rules requiring advance notice from wireless providers to MAS operators of certain technical changes to the wireless providers' networks. Carrier network changes can impact proper operation and effectiveness of the system; the addition of new frequency bands or the deployment of new air interface technologies, for example, could create spectrum gaps in the MAS that could be exploited by users of contraband wireless devices.[141] In the *Further Notice*, the Commission sought comment on whether to adopt rules requiring wireless providers to provide advance notice to MAS operators of carrier network changes likely to have an impact on the MAS.[142] Although the Commission acknowledged that lack of notice to MAS operators of certain types of network changes requiring adjustments to the MAS could compromise the system's effectiveness, it also recognized that an overly broad notification requirement could result in undue burdens or costs to wireless providers.[143] The Commission therefore sought comment on the appropriate scope, content, form, and timing of any notice requirement to ensure the necessary coordination among wireless providers and MAS operators.[144]

64. *90-Day Advance Notice Requirement*. We adopt rules requiring CMRS licensees[145] leasing spectrum to MAS[146] operators, including mobile MAS operators, to provide 90 days' advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, while permitting modified notice arrangements through mutual agreement: (1) adding a new frequency band to service offerings; (2) deploying a new air interface technology or changing an existing air interface technology; and/or (3) adding, relocating, or removing a cell site. Requiring advance notice ensures that MAS operators have adequate time to make any changes necessary to maintain a system's effectiveness. Absent a notification requirement, the record indicates that MAS operators typically discover CMRS licensees' network changes only after the MAS is impacted, during which time incarcerated people may be able to bypass the MAS and directly access the wireless provider's

(Continued from previous page)

[139] T-Mobile FNPRM Comments at 11 (citing to court-ordered wiretaps and subpoenas as examples of permissible cost recovery).

[140] *See, e.g.*, *Further Notice*, 32 FCC Rcd at 2370, para. 90 (noting that Verizon has a secure portal for receiving court-ordered termination requests). *See generally* AT&T FNPRM Comments at 12 (noting that "[a]ll of the key stakeholders in this proceeding are extremely familiar with the process of obtaining and responding to a court order").

[141] *Further Notice*, 32 FCC Rcd at 2378-79, paras. 117-20.

[142] *Id.* at 2378-79, paras. 117-21.

[143] *Id.* at 2379, paras. 119-20.

[144] *Id.* at 2379, paras. 119-21.

[145] The notification requirement we adopt today applies to CMRS licensees subject to part 20 of the Commission's rules that have entered into lease agreements for operation of CISs at a correctional facility. In Section B of this *Second Report and Order*, however, we also refer to such licensees as "wireless providers."

[146] For purposes of this *Second Report and Order*, we define Managed Access Systems as CISs whose operations require: (1) one or more lease agreements with CMRS operators; and (2) real time awareness of wireless provider spectrum use in the vicinity of the correctional facility where they are deployed.

network.[147] Moreover, CMRS licensees typically plan these technical changes months before they are implemented and often provide notice of these changes to the public and third parties. We therefore find that the limited burden imposed by this requirement is outweighed by its significant public interest benefits.

65. A limited notification requirement is necessary to deploy and use MAS effectively.[148] MAS require advance knowledge of wireless provider network changes to adjust their systems to work properly in a rapidly evolving wireless provider radiofrequency environment.[149] These systems use commercial wireless spectrum to capture calls and prevent contraband phones from being used inside a correctional facility. For such systems to be effective, the MAS coverage footprint must be at or very near 100 percent. When a system is less than 100 percent effective, areas of the correctional facility are not covered, and incarcerated people can continue to make illegal calls.[150] As the Correctional Leaders Association explains, incarcerated people have unlimited time to find those areas where the system is not effective and use the phone in those areas.[151]

66. MAS operators control the footprint of the system's coverage within the facility through a variety of technical practices and designs, but these systems coexist with commercial networks in the areas immediately surrounding the facility and must therefore also account for external wireless provider technical changes that are likely to impact the MAS system. Marcus Spectrum Solutions explains that "an effective CIS [ ] needs fine tuning as the cellular network near the prison changes and as the air interface changes *even in minor ways*."[152] CTIA recognizes "[i]t is not possible . . . to eliminate the need for some CIS upgrades in response to network changes,"[153] which emphasizes the need for an advance notice requirement. As such, the effectiveness of a MAS largely depends on coordination with wireless providers, which regularly adjust their networks to deploy new wireless technology. Marcus Spectrum Solutions explains that changes such as modifications to the air interface technologies and the routine activation of new base stations near a prison may adversely impact MAS effectiveness.[154] When wireless providers fail to provide notice to MAS operators, MAS are vulnerable to "releases," which gives contraband devices within the facility the ability to access the commercial wireless network during the time it takes to reconfigure and/or remodify the MAS system.[155] MAS operators therefore require advance knowledge of the network technical changes so that the systems can be adjusted to ensure that they remain operational and effective when the changes become effective.[156]

---

[147] *See* CellBlox FNPRM Comments at 4-5; CellBlox Refresh PN Comments at 9.

[148] *See* CellBlox Refresh PN Comments at 10, 11; CellBlox FNPRM Comments at 5; Letter from Cherie R. Kiser, Counsel, GTL, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 2 (filed June 9, 2016); Letter from Michael J. Marcus, Marcus Spectrum Solutions (MSS), to Ajit Pai, Chairman, FCC, GN Docket No. 13-111 (filed Mar. 6, 2017) (MSS Mar. 6, 2017 *Ex Parte*); MSS NPRM Comments at 24; CLA Refresh PN Reply at 1-2.

[149] *See* CLA Refresh PN Reply at 1-2.

[150] *See* Prelude FNPRM Comments at 3.

[151] *See* CLA Refresh PN Reply at 1 (citing Prelude FNPRM Comments at 3).

[152] MSS Mar. 6, 2017 *Ex Parte* (emphasis in original).

[153] CTIA Refresh PN Comments at 13.

[154] MSS Mar. 6, 2017 *Ex Parte*.

[155] CellBlox FNPRM Comments at 4-5.

[156] CellBlox Refresh PN Comments at 11 (explaining that advance notice ensures that CIS providers are "aware of these changes and become more proactive in the changing of their own RF environment"); GTL FNPRM Reply at 2 (asserting that "lack of cooperation of even one wireless provider can seriously degrade the effectiveness of efforts to combat contraband wireless devices").

67. Although we recognize that CMRS licensees increasingly coordinate with MAS operators to facilitate MAS deployments,[157] current efforts have been not been sufficient to meet the needs of MAS operators reacting to external network changes.[158] Contrary to claims by Verizon and AT&T that commenters have not identified any particular problems with deployment that merit either a mandatory or voluntary solution,[159] several entities have described issues with the current coordination process, have explained the need for CMRS licensees to provide advance notice of technical changes, and have suggested that a notification requirement is appropriate to address these shortcomings.[160] CellBlox, for example, acknowledges that wireless providers have improved communications efforts over the years, but it explains that the lack of standard procedures followed by all wireless providers "mak[es] the collaboration effort cumbersome at times."[161]

68. We therefore find that it is in the public interest to require CMRS licensees leasing spectrum for operation of MAS in a correctional facility to provide 90 days' advance notice to lessees of certain technical changes, which balances our objectives of providing MAS operators sufficient advance notice of significant changes likely to impact the MAS to make technical adjustments, while not unduly burdening wireless providers.

69. *First*, the rule we adopt requires advance notice only for limited categories of major network changes occurring within 15 miles of a correctional facility with an authorized MAS. We find that a notification requirement is appropriate for such changes that could impact MAS operations nationwide and involve significant technical changes that occur only a limited number of times per year. ShawnTech supports a standard notification requirement for network changes involving new frequency bands and air interface technology,[162] and Marcus Spectrum Solutions notes that even the routine activation of new base stations near a prison may adversely impact CIS effectiveness.[163] We reject the argument that a notification requirement is unnecessary because CIS operators can conduct regular radiofrequency scans to detect network changes.[164] Although current MAS operators typically use scanning technology to detect CMRS licensee network changes,[165] this technology leaves MAS vulnerable during the time it takes the provider to detect the change and then reconfigure and/or modify the system to address the wireless provider network change.[166] In practice, notification requirements for

[157] *See* AT&T NPRM Reply at 1, n. 3; AT&T FNPRM Comments at 1-2, 4; AT&T Refresh PN Comments at 3-4; CTIA NPRM Reply at 11-12; CTIA Refresh PN Comments at 11, 13; CTIA Refresh PN Reply at 6-7; OmniProphis Refresh PN Comments at 5; Screened Images FNPRM Comments at 10; Letter from Daniel R. Hackett, Chief Financial Officer, ShawnTech, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 3 (filed Aug. 7, 2015); T-Mobile Refresh PN Comments at 9; Verizon NPRM Reply at 5-6; Verizon Refresh PN Comments at 4-6.

[158] CellAntenna NPRM Comments at 3; Letter from Marjorie K. Conner, Counsel to CellAntenna, to Roger S. Noel, Chief, Mobility Division, FCC, GN Docket No. 13-111 (filed Oct. 9, 2014) (CellAntenna Oct. 9, 2014 *Ex Parte*); CellBlox FNPRM Comments at 4-5; CellBlox Refresh PN Comments at 10; MSS NPRM Comments at 26; OmniProphis Refresh PN Comments at 5, 10; ShawnTech Refresh PN Comments at 2.

[159] *See* AT&T NPRM Reply at 1, n.3; Verizon NPRM Reply at 5.

[160] CellAntenna NPRM Comments at 2-3; CellAntenna Oct. 9, 2014 *Ex Parte*; CellBlox Refresh PN Comments at 10-11; GTL NPRM Reply at 2, 5-7; GTL FNPRM Comments at 1, 11; GTL FNPRM Reply at 2; MSS Mar. 6, 2017 *Ex Parte*; TDOC FNPRM Comments at 5.

[161] CellBlox Refresh PN Comments at 10; *see also* ShawnTech Refresh PN Comments at 2 (stating its belief that a formal notification requirement "would improve the process by simplifying efforts and creating transparency").

[162] ShawnTech Refresh PN Comments at 2.

[163] MSS Mar. 6, 2017 *Ex Parte*.

[164] Screened Images FNPRM Comments at 9; T-Mobile FNPRM Comments at 13-14; T-Mobile Refresh PN Comments at 9-10; Letter from Eric Hagerson, Principal Federal Regulatory Affairs Manager, T-Mobile, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Mar. 17, 2017) (T-Mobile Mar. 17, 2017 *Ex Parte*).

[165] CellBlox FNPRM Comments at 4.

these changes would be relatively infrequent and impose minimal burden on CMRS licensees, and we therefore find it appropriate to adopt a uniform notification requirement for these limited categories of network changes.

70. *Second*, we find that wireless providers must provide at least 90 days advance notice before making major network changes. The minimum advance notice is required to give MAS operators sufficient time to make necessary adjustments to maintain the effectiveness of their systems. ShawnTech agrees that notifications must be provided "with enough time to allow MAS vendors to make any necessary changes to hardware, lease changes, and their equipment before new spectrum is enabled."[167] We believe that a 90-day notice period provides adequate lead time to allow MAS operators to make those changes.

71. We further find that requiring CMRS licensees to provide 90 days advance notice of these major network changes will not be unduly burdensome or unduly limit CMRS licensees' flexibility to deploy a new technology. CMRS licensees already provide advance notice of such changes to a range of other entities and therefore have notification distribution processes in place to facilitate compliance, resulting in minimal incremental costs to comply.[168] Furthermore, we disagree with T-Mobile's claims that a 90-day advance notice requirement would limit flexibility and delay deployment of new technologies.[169] As CTIA acknowledges, CMRS licensees typically plan technical changes months in advance, and several wireless providers advertise and announce major network changes, including upgrades to air interface technology, to the public.[170] We therefore find that requiring notice 90 days in advance of making network changes would neither condense nor significantly alter the timeframe in which wireless providers plan and deploy new technology. We find that, on balance, the benefits to MAS operators in adopting a limited, standardized notification policy for major network changes outweigh the minimal costs imposed on CMRS licensees.[171]

72. *Finally*, while we disagree with commenters that argue that the Commission should allow notification requirements to be established entirely via contractual arrangements between the parties rather than a Commission rule,[172] we find that private negotiations and agreements may be suitable to modify the terms of notification where our requirements may be overly inclusive.[173] For example, there

(Continued from previous page)
[166] *Id.*

[167] ShawnTech Refresh PN Comments at 2-3.

[168] *See* CellBlox FNPRM Comments at 5 (noting that CMRS licensees already plan, submit for approval, and notify many parties using internal control practices).

[169] *See* T-Mobile Mar. 17, 2017 *Ex Parte* at 1-2; T-Mobile FNPRM Comments at 14; T-Mobile FNPRM Reply at 2; T-Mobile Refresh PN Reply at 5-6.

[170] CTIA FNPRM Reply at 6 (acknowledging that the "addition of new frequencies available for CMRS use are made public, providing CIS operators with ample time to modify their systems as necessary"); T-Mobile FNPRM Comments at 14 (explaining that "CMRS air interfaces, frequency block assignments, and spectrum licenses are public knowledge, and it is entirely reasonable to expect CIS providers to use this public information when designing their systems"). CellBlox agrees that a 90-day advance notice requirement is appropriate and recommends a process in which the wireless provider is required to provide notice "not less than 90 days in advance of the planned change." *See* CellBlox FNPRM Comments at 5 (suggesting that CMRS licensees provide notice "not less than 90 days in advance of the planned change"); CellBlox Refresh PN Comments at 9-10 (recommending that, once a planned network change is internally approved, CMRS licensees provide 90 days advance notice "so that their systems can be reconfigured or modified in a similar 'planned' manner").

[171] *See* GTL FNPRM Reply at 2 (explaining that the "lack of cooperation of even one wireless provider can seriously degrade the effectiveness of efforts to combat contraband wireless devices").

[172] *See* CTIA NPRM Reply at 13, 15; Verizon FNPRM Comments at 3, 10-11.

may be cell sites within 15 miles of a correctional facility that have signals that nevertheless do not reach the correctional facilities, and therefore even the major network changes for which we require notice would not have any practical impact on nearby MAS. We therefore find it in the public interest to adopt a rule permitting CMRS licensee lessors and MAS operator lessees to adjust the terms of our notice requirement through mutual agreement. We also recognize that there are a range of wireless provider network changes other than the three categories we address in our rule that occur frequently and are highly localized and may affect nearby MAS (e.g., power increases and decreases, antenna height or direction adjustments). We find that MAS operators and CMRS licensees are best positioned to take into account the local RF environment and each entity's specific business needs and to supplement, as appropriate, our notice requirement with additional notice of other categories of network changes, including those that are site-specific and regularly occurring, for which advanced notice would prove beneficial.[174] To ensure that issues regarding notification to solutions providers of more frequent, localized wireless provider network changes are appropriately considered, we find it in the public interest to require CMRS licensees and MAS operators to negotiate in good faith to reach an agreement for notification for those types of network adjustments not covered by the notice requirement we adopt today.

73. We also note that advanced notifications—both those required herein and any modified notifications to which the parties may agree—may contain information that wireless providers deem commercially sensitive and for which wireless providers might seek confidential treatment if such information was provided to the Commission. Because the process we adopt today requires CMRS licensees to provide direct notice to MAS providers of such changes without a Commission submission, we find it appropriate to require CMRS licensees and MAS operators to negotiate in good faith regarding the parties' treatment of confidential information contained in notifications required by rule and/or negotiated between the parties.

74. *Emergency Network Changes*. We find it in the public interest to adopt an exception to the 90-day advance notice requirement for network technical changes within 15 miles of the facility that are required due to emergency/disaster preparedness. The record supports the need for a notification exception to ensure that wireless providers are not restricted in their ability to respond quickly during

(Continued from previous page)

[173] For example, a correctional facility located in a dense urban area may be within 15 miles of several small cell sites that may not have the same (if any) impact on a MAS network as would a higher-power macro cell site that is within close proximity of the facility. We envision that MAS operators and CMRS licensees could negotiate mutually agreed upon terms of notification where our requirements may be overly inclusive.

[174] *See* CTIA NPRM Reply at 11, 13, 15 (submitting "the Commission can best facilitate this continued communication by preserving parties' flexibility to tailor these discussions to individual relationships" and urging the Commission to "not intrude on the business arrangements between wireless providers and the managed access providers"); CTIA Refresh PN Comments at 11; CTIA Refresh PN Reply at 7 (arguing that "[i]mposing rigid notice requirements cannot account for the specific circumstances of the wireless network and the systems provider involved in the way that the current cooperative relationships can"); GTL NPRM Reply at 2 ("The Commission, however, must ensure that its rules do not limit the ability of a correctional facility to utilize the solution that best meets its needs. Each correctional facility is unique and attempting to adopt a one-size-fits all approach will undermine the Commission's effort[s]"); Screened Images FNPRM Comments at 10 (maintaining that mandated notification requirements are not necessary); T-Mobile Refresh PN Comments at 10 (recommending "wireless carriers and solutions providers should be permitted to work cooperatively to ensure the flow of information regarding network changes"); T-Mobile Refresh PN Reply at 6-7 (agreeing with CTIA that "the Commission should allow [the current coordination process] to continue to develop through collaborative—and not prescriptive—engagement"); TDOC FNPRM Comments at 5 (maintaining that, at a minimum, the Commission should "facilitate good faith collaboration and cooperation between wireless carriers and the correctional community"); Verizon FNPRM Comments at 3 (asserting "[t]he Commission should leave the details of operational issues, such as licensees notifying [CIS] vendors of network changes . . . to contractual arrangements between the parties"); Verizon Refresh PN Comments at 4 (arguing "[t]he Commission should thus avoid prescriptive requirements and generally allow wireless companies and MAS vendors to coordinate implementation and operation of their respective facilities in good faith").

times of public or national emergency. CellBlox agrees that notification should be provided "as soon as practical after the occurrence" to maintain the effectiveness of the MAS, which ensures that contraband wireless devices can continue to be managed and prevented from accessing the commercial wireless provider network.[175] No commenter opposed adoption of such a requirement.[176] We find it appropriate to require CMRS licensees to provide notice of these technical changes immediately after the exigency to ensure that operators continue to be notified of network changes that could impact the effectiveness of the MAS to make necessary adjustments.

IV. SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

75. In addition to MAS and other types of CIS technology, an extensive record has been developed through the Commission's 2013 *Notice of Proposed Rulemaking*, the 2017 *Further Notice*, and the *July 2020 Refresh PN* on a variety of other technological solutions to combatting contraband phone use in correctional facilities. In light of today's adoption of a rule-based contraband phone disabling process in the *Second Report and Order*, in this *Second Further Notice of Proposed Rulemaking*, we seek further comment on the relative effectiveness, viability, and cost of additional solutions previously identified in the record, particularly those referenced in Congress's Explanatory Statement to the 2021 Consolidated Appropriations Act.[177]

76. In the *Further Notice*, the Commission invited comment on wireless provider-disabling of devices identified by CISs, as well as other technological solutions to address the problem of contraband wireless devices in correctional facilities.[178] Specifically, the Commission sought comment on the use of "quiet zones," geofencing, network-based solutions, and beacon systems.[179] The 2021 Explanatory Statement urged the Commission to consider all legally permissible options for combatting contraband cellphone use, including the creation, or use, of "quiet or no service zones," geolocation-based denial, and beacon technologies to geographically appropriate correctional facilities.[180] In this *Second Further Notice of Proposed Rulemaking*, we seek comment specifically on whether there have been technological, economic, policy, and/or legal developments sufficient to overcome the variety of challenges presented to the widespread deployment of these technologies and whether and how the Commission can further facilitate these technologies through regulatory next steps.

A. Quiet Zones

77. We seek further comment on the approach suggested by certain commenters whereby the Commission would establish "quiet zones" in and around correctional facilities in which wireless communications are not authorized such that contraband wireless devices in correctional facilities would not receive service from a wireless provider.[181] In response to the *Further Notice* and *July 2020 Refresh PN*, commenters, including wireless carriers and solutions providers, argue quiet zones are infeasible to engineer without disrupting service to legitimate users[182] and are inferior to MAS because they do not

[175] CellBlox Refresh PN Comments at 11.

[176] *See* CellBlox FNPRM Comments at 6 (explaining that, "in certain instances[,] CMRS licensees must make emergency network changes in reaction to unplanned events"); T-Mobile FNPRM Reply at 15-16 (asserting "it is not practical to provide notification for many network changes as they are routinely implemented in response to real time environmental changes").

[177] *See* 2021 Explanatory Statement at H8440.

[178] *Further Notice*, 32 FCC Rcd at 2380-83, paras. 122-31.

[179] *Id.*

[180] 2021 Explanatory Statement at H8440.

[181] *Further Notice*, 32 FCC Rcd at 2380-81, paras. 123-27.

[182] CTIA Refresh PN Comments at 18; T-Mobile Refresh PN Comments at 15; AT&T Refresh PN Reply at 9; CLA Refresh PN Comments at 6; CTIA FNPRM Comments at 10-11; CTIA FNPRM Reply at 10; T-Mobile FNPRM (continued….)

allow authorized continued use (e.g., by correctional officers) of wireless devices from within the facility.[183] Commenters also express concern that quiet zones would be extremely costly to deploy and would require wireless providers to either re-design their radio access networks or substantially power down their transmitters.[184] Verizon further argues that requiring quiet zones would implicate section 316 of the Act by modifying wireless providers' licensed geographic area without an adjudication.[185] The American Correctional Association states that quiet zones are an incomplete solution because they merely terminate service to a device, but do not disable the device's camera and memory functions.[186]

78. We seek comment on whether there have been technological advancements in the carriers' network engineering that might make it more feasible to precisely define quiet zones around the borders of correctional facilities. To what extent does the increased reliance on small cell network deployments impact the feasibility of engineering quiet zones? Do these or similar solutions already exist, and if so, who is using them and where/in what context? While some members of the corrections community state that quiet zones may be a viable solution, we note that such an approach does not address two primary concerns of correctional facilities: (1) allowing continued use by authorized wireless devices (e.g., correctional officers, delivery personnel) from within the facility; and (2) complete disabling of the device. We seek comment on whether, absent the emergence of solutions to such concerns, commenters would still deem quiet zones a viable solution.

79. We also seek comment on the cost of creating quiet zones, particularly as relative to deploying MAS or advanced detection. What are the various types of costs necessary for a wireless provider to establish quiet zones, while maintaining desired communications services, including 5G, outside the correctional facility—e.g., network adjustments and system integration, hardware, software, engineering, ongoing maintenance to ensure the correctional facility continues to be denied service —and what are the estimated costs associated with each category? Would costs differ when comparing the creation of a quiet zone surrounding a rural correctional facility versus an urban one and, if so, how? Absent a quiet zone, wireless providers with networks that provide coverage in the vicinity of a correctional facility generate revenue from subscriber customers operating contraband devices. The record reflects wireless providers' contention that the costs of solutions to combat contraband devices are a "public responsibility" that "should not be shifted to one industry sector."[187] If the Commission were to mandate quiet zones, who should bear the cost of implementing such a solution? Should carriers be required to defray some of the costs of CIS if quiet zones are not mandated? Are there alternatives to a Commission mandate that might encourage implementation?

B. Geolocation-Based Denial and Carrier Network-Based Solutions

80. We seek comment on geolocation-based denial, also known as geofencing, whereby mobile device software and/or hardware is used to shut down contraband wireless devices that violate a perimeter surrounding a correctional facility.[188] Relatedly, we seek further comment on a "network-based

(Continued from previous page)
Comments at 16; T-Mobile FNPRM Reply at 5; Verizon FNPRM Comments at 12; Corrections.com FNPRM Reply at 10-11; *see also* ShawnTech FNPRM Comments at 4-5 (stating that the feasibility of implementing quiet zones is dependent on the physical characteristics of each site in question, which might preclude standardization).

[183] CTIA Refresh PN Comments at 18; ShawnTech Refresh PN Comments at 3; CTIA FNPRM Comments at 10; *but see* CLA Refresh PN Comments, Exh. B at 3 (noting the California Department of Corrections believes quiet zones would be a desirable approach if they can be implemented without depriving the general public of cellular service).

[184] Verizon FNPRM Comments at 12; CenturyLink FNPRM Reply at 8.

[185] Verizon FNPRM Comments at 12.

[186] ACA FNPRM Comments at 4.

[187] CTIA Refresh PN Comments at 13, 17-18; *see also* T-Mobile Refresh PN Comments at 10-12.

[188] *Further Notice*, 32 FCC Rcd at 2380-81, paras. 123-27.

solution," whereby wireless providers would be required to identify and disable contraband wireless devices in correctional facilities using their own network elements, including base stations and handsets/devices.[189]

81. In response to the *Further Notice* and *July 2020 Refresh PN*, many commenters point out that geolocation-based denial that relies on GPS or other location services is easily defeated if incarcerated people disable location services on the device,[190] and that network-based geofencing (i.e., use of cell site triangulation) is only a theoretical concept today, with several technical concerns regarding its viability as a solution.[191] Regarding carrier network-based solutions, some solutions providers and the corrections community support the use of carrier network-based solutions to identify and disable contraband cell phones.[192] Wireless providers oppose the approach, arguing that it is technically infeasible to use network elements to precisely identify the location of devices, particularly in rural areas with fewer base station deployments and in deep-indoor environments of a correctional institution.[193] Wireless providers further state that they do not, as a practice, track their customers' locations, and that doing so would violate the prohibition in section 222 of the Act on the use of customer proprietary network information without prior customer authorization.[194] Finally, wireless providers argue that prison officials and law enforcement, not carriers, should be responsible for determining whether a device, even one identified as present within a correctional facility, is contraband.[195]

82. We seek comment on whether there have been technological advancements in the carriers' network engineering that might make it more feasible to implement network-based geofencing around the borders of correctional facilities. To what extent does the increased reliance on small cell network deployments impact the feasibility of engineering network-based geofencing? What real-world data is there with respect to the viability of network-based geofencing? Do these or similar solutions already exist, and if so, who is using them and where/in what context? We seek comment on the specific engineering steps that wireless providers would need to take to implement such a solution, including the necessary testing and maintenance necessary to ensure its accuracy and ongoing viability. To what degree of accuracy could wireless providers define geofencing around the precise perimeter of the correctional facility? Can network-based geofencing allow for continued authorized use (e.g., by correctional officers) from within the facility? What information would wireless carriers need in order to account for such continued authorized use, and how would such information be shared? We also seek comment on the cost of implementing geofencing, particularly as relative to MAS and advanced detection. What are the various types of costs necessary to implement geofencing—e.g., hardware,

[189] *Id.* at 2381-82, paras. 128-29.

[190] Verizon Refresh PN Comments at 7-8; T-Mobile Refresh PN Comments at 16; Verizon FNPRM Comments at 13.

[191] CTIA Refresh PN Comments at 17; Verizon FNPRM Comments at 13; CTIA FNPRM Reply at 10.

[192] CLA Refresh PN Comments at 5; ShawnTech FNPRM Comments at 5; GTL FNPRM Comments at 7, 12-13; Prelude FNPRM Comments at 5, 10.

[193] T-Mobile FNPRM Comments at 17; T-Mobile FNPRM Reply at 5-6; *see also* Corrections.com FNPRM Reply at 12.

[194] Verizon Refresh PN Comments at 8; T-Mobile Refresh PN Comments at 16; CTIA FNPRM Comments at 11-12; CTIA FNPRM Reply at 10; T-Mobile FNPRM Comments at 17; T-Mobile FNPRM Reply at 5-6; *see also* Corrections.com FNPRM Reply at 12; *but see* CLA Refresh PN Comments at 5 (arguing this approach does not implicate privacy concerns because wireless providers would only query the location of cellular devices connecting to specific base stations in the area of the correctional facility and would only store the location data for devices determined to be contraband).

[195] CTIA Refresh PN Comments at 17; T-Mobile FNPRM Comments at 18; *see also* Corrections.com FNPRM Reply at 12.

software, network integration, engineering, ongoing maintenance—and what are the costs associated with each category?

83. We also seek comment on carrier network-based solutions that would allow wireless providers to independently identify and disable contraband wireless devices located within correctional facilities. Should the Commission adopt a rule requiring wireless providers to use their own network elements to identify phones operating within a correctional facility? Should such a rule define the parameters and necessary indicia that wireless providers must observe prior to terminating service to a device identified via geofencing? For example, how long should the carrier observe the device operating within the correctional facility prior to determining the device is contraband? Are there other criteria that might indicate a device is contraband (e.g., time and duration of calls)? What regulatory steps could the Commission take to reduce liability and privacy concerns related to a carrier network-based solution? Would a Commission rule requiring carriers to deny service to unauthorized devices identified via network-based solutions resolve any liability concerns? Alternatively, are there steps wireless providers could take to reduce such concerns, for example by modifying the terms of their customer contracts? We also seek comment on the cost of implementing carrier network-based solutions, particularly as relative to MAS and advanced detection. What are the various types of costs necessary to implement network-based solutions—e.g., hardware, software, network integration, engineering, ongoing maintenance—and what are the costs associated with each category?

C. Beacon Technology

84. We seek further comment on the potential efficacy of technologies that are intended to disable contraband wireless devices in correctional facilities using the interaction of a beacon system set up in the correctional facility with software embedded in the wireless devices.[196] In response to the *Further Notice* and *July 2020 Refresh PN*, many commenters oppose beacon technology as an infeasible solution, arguing that it would require device manufacturers to install proprietary software and hardware on all mobile devices, which would take years to implement and even longer to impact use of contraband devices.[197] Some commenters further argue that mandating a proprietary technology such as beacons would violate the Commission's long-standing policy to remain technology neutral.[198] Others point out that beacon technology would be ineffective with respect to legacy devices and would likely create a black market inside correctional facilities for devices without beacon technology.[199] Some commenters argue that mandating all new devices be manufactured with beacon technology could lead to unintended cybersecurity threats, since bad actors could install beacons in other locations and use it to prevent legitimate use.[200] Cell Command, a producer of beacon technology, argues that beacons are a reliable and

[196] *Further Notice*, 32 FCC Rcd at 2382-83, paras. 130-31.

[197] T-Mobile Refresh PN Comments at 10; CLA Refresh PN Comments at 6; CTIA FNPRM Comments at 9-10; Verizon FNPRM Comments at 12; Corrections.com FNPRM Reply at 13; CenturyLink FNPRM Reply at 7-8; Inpixion FNPRM Reply at 6.

[198] CTIA FNPRM Comments at 9-10; CTIA FNPRM Reply at 9; T-Mobile FNPRM Comments at 18; T-Mobile FNPRM Reply at 7; Corrections.com FNPRM Reply at 13; Inpixion FNPRM Reply at 9; *but see* Cell Command FNPRM Reply at 4-5 (arguing that beacon technology is a technology neutral solution, since correctional facilities would remain free to use whatever CIS they choose or none at all and stating that it only requests that the Commission adopt a voluntary program under which the wireless industry would install beacon technology software on wireless devices); ACA FNPRM Comments at 4-5 (arguing that the policy against mandating one technology is "totally inappropriate in the public safety setting").

[199] T-Mobile FNPRM Comments at 19; T-Mobile FNPRM Reply at 7; Corrections.com FNPRM Reply at 13; Inpixion FNPRM Reply at 6.

[200] CTIA FNPRM Comments at 10; CTIA FNPRM Reply at 9; T-Mobile FNPRM Reply at 7; Inpixion FNPRM Reply at 6.

comprehensive solution to combatting contraband devices and would be cheaper than alternative solutions, since Cell Command intends to license its systems to manufacturers.[201]

85. We seek comment on whether there have been technological advancements that might increase the viability of beacon technology as a comprehensive solution to combatting contraband phone use in correctional facilities. Particularly in light of the exigent public safety concerns associated with contraband phone use, we acknowledge commenters' concerns related to the timeline for implementing beacon technology on all new mobile devices and the ability to circumvent beacons via legacy devices that were manufactured without the requisite hardware and/or software. Have there been any developments in beacon technology that make it possible to install beacon software on mobile devices remotely (e.g., through a software update)? Do these or similar technologies already exist, and if so, who is using them and where/in what context? What authority does the Commission have to require the installation of such software on devices and how is such an approach consistent with technological neutrality? How does this technology ensure that authorized users (e.g., correctional officers) are still able to use their devices? What is the cost and implementation timing for beacon technology, specifically as compared to MAS or advanced detection, and who would bear this cost? What are the various types of costs associated with this type of technology, including hardware, software, network integration, engineering, ongoing maintenance, etc.?

D. MAS Evolved and Future CIS Use Cases

86. We seek further comment on potential regulatory steps that might be necessary to ensure that MAS maintains effectiveness as wireless technology continues to evolve nationwide from 2G to widespread 3G/4G and ultimately 5G deployments. In the *July 2020 Refresh PN*, the Bureau noted that MAS solutions depend largely on forcing contraband devices from 3G/4G to 2G services, which carriers are rapidly phasing out, and current network security issues can prevent these systems from capturing calls made from 5G phones.[202] The Bureau noted that stakeholders have already begun exploring solutions to this issue, as highlighted by the 2019 Task Force Status Report from CTIA and the Association of State Correctional Administrators describing the next generation of managed access system solutions as "MAS Evolved." In order to facilitate MAS Evolved deployments, the 2019 Task Force Report indicated the need for wireless providers to establish roaming agreements allowing a MAS Evolved system to block calls by preventing authentication on the network, and enabling newer generation services on MAS networks where calls are captured without forcing the devices down to 2G. Thus far, the Commission has relied on stakeholder negotiations to govern roaming agreements, as well as implementation of best practices in this developing area. The Bureau sought comment in the *July 2020 Refresh PN* on how a MAS Evolved approach could be more effective, less complex, easier to manage, and less costly to implement when compared to a more traditional MAS deployment.[203]

87. Commenters largely agree that MAS Evolved will be even more effective than existing MAS deployments, as it allows for seamless automated interoperation without human intervention or resultant delay.[204] AT&T states that MAS Evolved technology has built-in information sharing that permits near-real time updates to the system as carriers adjust or evolve their networks, thereby making the systems more responsive to changes in radio environment.[205] Commenters believe that MAS Evolved will be easier and less expensive to deploy than current systems, can be "future proof" for newer generations of technology, and can be fine-tuned in order to reduce coverage holes and improve the ability to locate contraband devices.[206] CTIA states that deployments are expected in multiple states in

[201] Cell Command FNPRM Comments at 3-6; 16-18.

[202] *July 2020 Refresh PN*, 35 FCC Rcd at 7912.

[203] *Id.* at 7913.

[204] CTIA Refresh PN Comments at 4-5; CellBlox Refresh PN Comments at 12; CLA Refresh PN Comments at 4.

[205] AT&T Refresh PN Comments at 6.

the near term and the wireless industry is actively advancing development and deployment of MAS Evolved.[207] Both Verizon and AT&T state that they have reached initial roaming agreements with MAS Evolved vendors and continue to cooperate in good faith with solutions providers to facilitate further deployments.[208] OmniProphis states that it has roaming agreements in place with Verizon, AT&T, and T-Mobile covering all 21 facilities where OmniProphis has MAS deployments but expresses concern about whether roaming agreements with major wireless providers will also cover regional and international carriers that roam on the major wireless providers' networks.[209] Despite this initial progress, solutions providers and members of the corrections community argue that roaming agreements can be costly and burdensome to obtain and that the Commission should adopt rules requiring carriers to enter into roaming agreements with solutions providers.[210]

88. We seek further comment on steps the Commission could take to facilitate MAS deployments. Should the Commission mandate roaming agreements between wireless carriers and solutions providers in the corrections context given the vital public safety concerns? If so, using what parameters and under what timeframe? What are the key lessons that wireless carriers and solutions providers have learned from initial roaming agreement negotiations? Have agreements become more standardized? How can negotiations be expedited? Are there particular "sticking points" that prolong negotiations? How could roaming agreements account for international devices roaming on the wireless carriers' networks? Are roaming agreements able to account for regional and international carriers that may also be roaming on the wireless providers' networks? How can agreements provide MAS operators the keys necessary to acquire identifying information from international devices? If full roaming partners, can solutions providers leverage their small cell deployments to create a virtual fence and enhance the ability to identify and block contraband phones? Are there specific challenges that arise from entering into such full roaming partner agreements? To achieve the full benefits of MAS-Evolved, what regulatory steps, if any, should the Commission take to ensure that technical issues arising from solutions providers becoming roaming partners are fully addressed in executed roaming partner agreements? Are network adjustments needed to ensure that 911 calls are passed to public safety answering points under a MAS Evolved model? Would additional technical or other information be necessary? In addition to the execution of roaming agreements, are there other approaches that could be developed by the wireless providers and/or the vendors to add features or services and help defray the cost of MAS deployments and operations? Should the Commission revise the previously streamlined leasing rules in the correctional facility context to facilitate further CIS (including MAS) deployments nationwide?

89. We also seek comment on what additional regulatory steps within the Commission's authority might be necessary to accommodate future CIS use cases to address the problem of contraband wireless device use. Are there any emerging technologies that could be accessed by incarcerated people that might expand the uses and types of contraband wireless devices, such as technologies that might facilitate operation outside of carrier-based subscriber services? If so, what is the capacity of existing CIS technologies to evolve to detect devices operating via such applications? Could we adapt the rules-based disabling process we adopt in the *Second Report and Order* to facilitate disabling of contraband wireless devices that will rely on deployment of emerging technologies? Could evolving technologies and developments in wireless provider network security present difficulties in solution providers' capability to deploy current CIS technology and still provide adequate subscriber-identifying and device-identifying information to achieve contraband device disabling? If so, what regulatory steps might be necessary to

(Continued from previous page)

[206] CTIA Refresh PN Comments at 5-6; AT&T Refresh PN Comments at 6.

[207] CTIA Refresh PN Comments at 4-6.

[208] Verizon Refresh PN Comments at 5-6 (stating it has reached roaming agreements with two primary vendors that cover ten institutions in three states and is engaging with a third vendor); AT&T Refresh PN Comments at 5-7.

[209] OmniProphis Refresh PN Comments at 9.

[210] ShawnTech Refresh PN Comments at 4; OmniProphis Refresh PN Comments at 9.

ensure that, in the face of technological and network changes, wireless providers can continue to be able to receive information from DCFOs sufficient to effectuate the disabling of contraband wireless devices at both the subscription- and device-levels pursuant to the process we adopt today?

V. PROCEDURAL MATTERS

90. *Paperwork Reduction Analysis*. This *Second Report and Order* contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law No. 104-13. It will be submitted to the Office of Management and Budget for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new information collection requirements contained in this proceeding. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 47 U.S.C. § 3506(c)(4), we asked for specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees in the *Further Notice*,[211] and we received no comment.

91. In the present document, we have assessed the effects of rules that would facilitate the development of multiple technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide, and find that the adopted rule changes impose new or additional reporting or recordkeeping and/or other compliance obligations for small entities as well as other applicants and licensees.

92. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this *Second Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

93. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[212] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[213] Accordingly, we have prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in the *Second Report and Order* on small entities. The FRFA is set forth in Appendix B. We have also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the possible impact of the rule changes contained in the *Second Further Notice of Proposed Rulemaking* on small entities. The IRFA is set forth in Appendix C.

VI. ORDERING CLAUSES

94. Accordingly, IT IS ORDERED that, pursuant to sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. § 151, 152, 154(i), 154(j), 301, 302, 303, 307, 308, 309, 310, and 332, this *Second Report and Order and Second Further Notice of Proposed Rulemaking* is HEREBY ADOPTED.

95. IT IS FURTHER ORDERED that the amendments of part 20 of the Commission's rules, as set forth in Appendix A, ARE ADOPTED, effective thirty (30) days after publication in the Federal Register. The revisions to section 20.23(b)-(d) of the Commission's rules, which contain new or modified information collection requirements that require review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act, will not become effective until the effective date for

[211] *Further Notice*, 32 FCC Rcd at 2384, para. 136.

[212] *See* 5 U.S.C. §§ 601–612. The RFA has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[213] *Id.* § 605(b).

those information collections is announced by the Commission in a document published in the Federal Register after the Commission receives OMB approval.

96. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Second Report and Order* and *Second Further Notice of Proposed Rulemaking*, including the Final Regulatory Flexibility Analysis and Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

97. IT IS FURTHER ORDERED that the Commission SHALL SEND a copy of this *Second Report and Order and Second Further Notice of Proposed Rulemaking* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends 47 CFR part 20 as follows:

PART 20 – COMMERCIAL MOBILE SERVICES

1. The authority citation for part 20 continues to read as follows:

AUTHORITY: [To be inserted prior to summary being published in the Federal Register].

2. Amend § 20.3 by adding the following definitions in alphabetical order:

§ 20.3 Definitions.

* * * * *

CIS Operator. An operator of a CIS at a correctional facility, whether a CIS solutions provider, or a DCFO or responsible party that deploys its own CIS at a correctional facility.

* * * * *

Contraband Interdiction System. A Contraband Interdiction System (CIS) is any system comprised of one or more stations that is used only at a permanent correctional facility that is authorized to operate such systems pursuant to this part and that is designed exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of the facility and/or to obtain identifying information from such contraband wireless devices.

Designated Correctional Facility Official. A Designated Correctional Facility Official (DCFO) is an official of the state, local, or Federal government responsible for administration and oversight of the relevant correctional facility where a contraband wireless device is located.

(1) In government-run correctional facilities, this definition requires the DCFO to be, at a minimum, the official with responsibility for oversight of the relevant facility (e.g., the warden) or higher ranking official.

(2) In privately-run correctional facilities, this definition requires the DCFO to be a government official with responsibility for oversight of the facility's performance through contract.

* * * * *

Managed Access System. A Managed Access System (MAS) is a Contraband Interdiction System whose operations require:

(1) One or more lease agreements with CMRS operators; and

(2) Real-time awareness of wireless provider spectrum use in the vicinity of the correctional facility where it is deployed.

* * * * *

3. Amend § 20.23 by replacing paragraph (b) and adding paragraphs (c) and (d) to read as follows:

§ 20.23 Contraband wireless devices in correctional facilities.

*****

(b) *Contraband Interdiction System (CIS) authorization process.* The provisions in this section apply to any person seeking certification of a CIS authorized for use in the submission of qualifying disabling requests, whether operating a system that requires a license and is regulated as CMRS or private mobile radio service (PMRS), or operating a passive system that does not require a license. The Wireless Telecommunications Bureau (Bureau) will establish, via public notice, the form and procedure for: CIS operators to file CIS certification applications, self-certifications, and periodic re-certification; CIS

operators to serve on wireless providers notice of testing and copies of self-certification; and wireless providers to file objections to self-certifications, including required service on CIS operators and DCFOs.

(1) *Application requirements*. To obtain CIS certification, an applicant must submit an application to the Bureau for review and approval that:

(i) Demonstrates that all radio transmitters used as part of the CIS have appropriate equipment authorizations pursuant to Commission rules in part 2 of this chapter;

(ii) Demonstrates that the CIS is designed and will be configured to locate devices solely within a correctional facility;

(iii) Describes the methodology to be used in analyzing data collected by the CIS and demonstrates that such methodology is adequately robust to ensure that the particular wireless device is in fact located within a correctional facility and includes specific data analysis benchmarks designed to ensure successful detection, such as rate of detection of contraband versus non-contraband devices and relevant sample size (e.g. number of devices observed and length of observation period);

(iv) Demonstrates that the CIS will secure and protect all information or data collected as part of its intended use;

(v) Demonstrates that the CIS will not interfere with emergency 911 calls;

(vi) Describes whether the CIS requires a spectrum or network access agreement (e.g., a spectrum leasing arrangement or roaming agreement) to be authorized to operate; and

(vii) Includes a proposed test plan for subsequent site-based testing of each CIS, that must include detailed descriptions and technical specifications to facilitate Commission review of whether the system satisfies its legal requirements and technically functions as anticipated.

(2) *Marketing and sales*. CIS that are certified for use in qualifying requests for disabling of contraband devices may be marketed or sold only to correctional facilities or entities that will provide contraband interdiction services to such facilities.

(3) *Site-based testing and self-certification requirements*.

(i) *Site-based testing.* A CIS operator seeking to use the CIS to submit qualifying requests for disabling must test a certified CIS at each location where it intends to operate. Thereafter, the CIS operator must file with the Bureau a self-certification that complies with paragraph (b)(3)(ii) of this section, confirming that the testing at that specific correctional facility is complete and successful. The CIS operator must serve notice of the testing on all relevant wireless providers prior to testing and provide such wireless providers a reasonable opportunity to participate in the tests. Relevant wireless providers include any wireless provider holding a spectrum license that:

(A) Authorizes operation on the frequencies on which the CIS seeks to detect contraband use; and

(B) Authorizes service in the geographic area (e.g., census tract, county, Partial Economic Area (PEA), Economic Area (EA), Cellular Market Area (CMA), Regional Economic Area Grouping (REAG)) within which the correctional facility is located.

(ii) *Self-certification*. Following the testing, and to be eligible for use in conjunction with qualifying requests for disabling, a CIS operator must file a self-certification with the Bureau that:

(A) Identifies the correctional facility where it seeks to deploy;

(B) Attests that applicable Federal or state criminal statutes prohibit the possession or operation of contraband devices within the correctional facility (and includes the applicable Federal or state criminal statutory provision);

(C) Describes the results of on-site tests of the certified CIS conducted at the correctional facility;

(D) Attests that the on-site testing was performed consistent with the approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device;

(E) Identifies whether any relevant wireless providers participated in the testing, and provides proof that the relevant wireless providers were given notice regarding the testing and a reasonable opportunity to participate;

(F) Includes proof of any spectrum and/or network access agreement (e.g., a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate and/or for the system to function effectively;

(G) Includes proof that the self-certification was served via electronic means on all relevant wireless providers; and

(H) Includes an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.

(I) The self-certification must be filed in accordance with part 1, subpart F, of this chapter.

(4) *Submitting objections*. Wireless providers may submit objections to the Bureau within five business days from the certification filing date. Any such objections must be served on the DCFO and the CIS operator.

(5) *Recertification*. At least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO for contraband device disabling must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

(6) *Suspension of CIS eligibility*. The Bureau may suspend CIS certification generally or at a particular facility if subsequent credible information calls into question a system's reliability.

(7) *Records maintenance*. To ensure the integrity and proper operation of CISs, a CIS operator must retain records of all information supporting each request for disabling and the basis for disabling each device, including copies of all documents submitted in the qualifying request, for at least five years following the date of submission of the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must make available all records upon request from the Bureau.

(c) *Disabling contraband wireless devices.* A DCFO may request that a CMRS licensee disable a contraband wireless device that has been detected in a correctional facility by a CIS that has been certified in accordance with paragraph (b) of this section. Absent objections from a wireless provider, as described under paragraph (b)(4) of this section, the DCFO may submit a qualifying request to a wireless provider beginning on the sixth business day after the later of the self-certification filing or actual service, as described under paragraph (b)(3)(ii) of this section.

(1) *DCFO list*. The Commission will maintain a publicly available list of DCFOs that are authorized to transmit qualifying disabling requests. Authorized DCFOs that seek to be recognized on the Commission's DCFO list must send a letter to the Commission's Contraband

Ombudsperson, signed by the relevant state attorney general or the relevant Bureau of Prisons Regional Director and providing:

(i) The individual's name;

(ii) The individual's official government position; and

(iii) A list of correctional facilities over which the individual has oversight and management authority.

(2) *Qualifying request*. A qualifying request must be made in writing, contain the certifications in paragraph (c)(2)(i) of this section and the device and correctional facility identifying information in paragraph (c)(2)(ii) of this section, and be signed by the appropriate DCFO. The DCFO must transmit a qualifying request to a CMRS licensee using a secure communication means that will provide certainty regarding the identity of both the sending and receiving parties. A CMRS licensee must adopt a method, or use an existing method, for receiving secured and verified qualifying requests.

(i) *Certifications*. A qualifying request must include the following certifications by the DCFO:

(A) A CIS that has been certified in accordance with paragraph (b) of this section was used to gather the contraband subscriber and device information populated in the qualifying request;

(B) The certified CIS was used to identify contraband wireless devices operating in a correctional facility where the CIS has been tested and self-certified for operational readiness and for use in qualifying requests, and the identification of contraband wireless devices occurred within 30 days immediately prior to the date of the qualifying request submission;

(C) The DCFO has reviewed the list of contraband wireless devices and attests that it is accurate; and

(D) It is a violation of applicable state or Federal criminal statutes to possess or operate a contraband device in the correctional facility.

(ii) *Device and correctional facility identifying information*. The qualifying request must identify the contraband wireless device to be disabled and the correctional facility by providing the following information:

(A) Identifiers sufficient to:

(1) Identify the applicable wireless service provider;

(2) Uniquely describe each of the contraband wireless devices in question at the subscription level; and

(3) Uniquely describe each of the contraband wireless devices in question at the device-level;

(B) Name of the correctional facility at which the contraband wireless device(s) were identified; and

(C) Street address of the correctional facility at which the contraband wireless device(s) were identified.

(3) *Licensee actions upon receipt of a qualifying request*. Upon receiving a request from a DCFO to disable a contraband wireless device, a licensee providing CMRS service must verify that the request contains the required information for a qualifying request, as defined in paragraph (c)(2) of this section.

(i) *Disabling upon receipt of a qualifying request and timing.* If the qualifying request contains the required information, and does not contain an error in the device identifying information preventing the licensee from being able to disable the device, a licensee must, within two business days of receipt of the qualifying request, disable the contraband wireless device from using the wireless provider's network at both the device and subscriber level and take reasonable and practical steps to prevent the contraband wireless device from being used on another wireless provider's network.

(ii) *Rejection of a qualifying request and timing.* A licensee may reject a qualifying request within two business days of receipt of a qualifying request if it does not include the information required for a qualifying request or, with respect to a relevant device, the request contains an error in the device-identifying information preventing the licensee from being able to disable the device.

(iii) *Customer outreach*. A licensee may immediately disable a contraband wireless device without any customer outreach, or a licensee may contact the customer of record through any available means to notify them that the device will be disabled, but any such notice does not modify the licensee's obligation to comply with paragraphs (c)(3)(i) and (ii) of this section.

(iv) *Notification to the Designated Correctional Facility Official*. Within two business days of receiving a qualifying request from a DCFO, a licensee must inform the DCFO whether the request has been granted or rejected.

(4) *Reversals*. A licensee may reverse a disabled wireless device if it determines that the wireless device was identified erroneously as contraband. The licensee must promptly inform the DCFO of the erroneously identified wireless device.

(i) *DCFO involvement*. Prior to reversing a disabling action, a wireless provider that determines that a device may have been erroneously identified as contraband may request that the DCFO review and confirm the information provided in a qualifying request pursuant to which the device was previously disabled. To trigger DCFO involvement, the wireless provider must provide the DCFO with:

(A) The date of the qualifying request;

(B) The identifying information provided for the device; and

(C) Any evidence supporting the wireless provider's belief that the device was erroneously identified.

(ii) *DCFO response*. Upon receipt of a request from a wireless provider, the DCFO should review the qualifying request and determine whether the device in question was erroneously identified and either confirm the validity of the identifying information contained in the qualifying request or acknowledge the error and direct the carrier to restore service to the device.

(iii) *Restoration of service*. In the event the DCFO directs the wireless provider to reverse the disabling, the wireless provider must, within two business days, restore service to the device and reverse any actions taken to prevent the device from accessing other wireless provider networks.

(iv) *Wireless provider action in absence of timely DCFO response*. In the event the DCFO does not respond to a request from a wireless provider for review of a qualifying request within two business days, the wireless provider may proceed with reversing the disabling action.

(v) *Notice of reversals*. The DCFO must provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed.

(d) *Notification to Managed Access System (MAS) operators of wireless provider technical changes*.

(1) *Notification requirements*. CMRS licensees leasing spectrum to MAS operators must provide 90 days' advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, unless parties modify notification arrangements through mutual agreement:

(i) Adding a new frequency band to service offerings;

(ii) Deploying a new air interface technology or changing an existing air interface technology; and/or

(iii) Adding, relocating, or removing a site.

(2) *Good faith negotiations*. CMRS licensee lessors and MAS operator lessees must negotiate in good faith to reach an agreement for notification for other types of network adjustments not covered by the notice requirement set forth in paragraph (d)(1) of this section and for the parties' treatment of confidential information contained in notifications required pursuant to this rule section and/or negotiated between the parties.

(3) *Emergency network changes exception*. CMRS licensees leasing spectrum to managed access systems (MAS) operators are not required to provide 90 days' advance notice to MAS operators of network technical changes occurring within 15 miles of the correctional facility that are required due to emergency and disaster preparedness. CMRS licensees must provide notice of these technical changes immediately after the exigency.

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Further Notice of Proposed Rulemaking* (*Further Notice*) released in March 2017 in this proceeding.[2] The Commission sought written public comment on the proposals in the *Notice*, including comment on the IRFA. No comments were filed addressing the IRFA. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Final Rules

2. The Second Report and Order (*Second Report and Order*) adopted by the Commission today continues the Commission's efforts to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. Federal, state, and local correctional administrators recognize the need to address the contraband problem in correctional facilities. In 2010, Congress passed the Contraband Cell Phone Act, which prohibited the possession of cell phones in federal prisons by unauthorized persons. Similarly, a number of states have enacted legislation that designated wireless devices in correctional facilities as contraband, and a substantial majority of states impose criminal penalties for possessing or operating contraband wireless devices within correctional facilities. In conjunction with legislation, the federal government and states have been conducting trials and investing in technologies that will enable them to combat contraband wireless device use in correctional facilities.

3. The *Second Report and Order* establishes rules requiring wireless providers to disable contraband wireless devices in qualifying correctional facilities using an authorized Contraband Interdiction System (CIS) pursuant to the submission of qualifying requests from designated correctional facility officers (DCFOs) and adopts a framework to facilitate the disabling process. The *Second Report and Order* describes the qualifications for DCFOs, details the requirements for the submission and processing of qualifying requests, and establishes the requirements for wireless providers to notify CIS operators of major technical changes to ensure that CIS effectiveness is maintained. In addition, with the rules adopted in the *Second Report and Order*, the Commission furthers its goal of promoting the public interest by ensuring that parties making the disabling request have the necessary authority and accountability and that CIS use at a correctional facility is authorized. Further, these rules will provide law enforcement with the tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threat posed by the illegal use of such devices in correctional facilities.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

4. There were no comments filed that specifically addressed the proposed rules and policies presented in the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[4]

---

[1] *See* 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996, (SBREFA) Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017) (*Order and Further Notice*). When not referring to the *Order*, the FRFA will reference only the *Further Notice.*

[3] *See* 5 U.S.C. § 604.

6. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

7. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[5] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[6] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[7] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[8]

8. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[9] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 30.7 million businesses.[11]

9. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[12] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[13] Nationwide, for tax year 2018, there

(Continued from previous page)

[4] *Id.* § 604 (a)(3).

[5] *Id.* § 604(a)(4).

[6] *Id.* § 601(6).

[7] *Id.* § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[8] 15 U.S.C. § 632.

[9] *See* 5 U.S.C. § 601(3)-(6).

[10] *See* SBA, Office of Advocacy, "What's New With Small Business?", https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/23172859/Whats-New-With-Small-Business-2019.pdf (Sept 2019).

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), "Who must file,"

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[14]

10. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[15] U.S. Census Bureau data from the 2017 Census of Governments[16] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[17] Of this number there were 36,931 general purpose governments (county[18], municipal and town or township[19]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[20] with enrollment populations of less than 50,000.[21] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[22]

11. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and

[14] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for Region 1-Northeast Area (76,886), Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[15] 5 U.S.C. § 601(5).

[16] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[17] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* Table 2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[18] *See id.* at Table 5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[19] *See id. at* Table 6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[20] *See id.* at Table 10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* Table 4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[21] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[22] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations Tables 5, 6, and 10.

infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[23] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[24] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[25] Of this total, 3,083 operated with fewer than 1,000 employees.[26] Thus, under this size standard, the majority of firms in this industry can be considered small.

12. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[27] The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[28] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.[29] Of that number, 3,083 operated with fewer than 1,000 employees.[30] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[31] Of this total, an estimated 317 have 1,500 or fewer employees.[32] Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

13. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses

---

[23] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[24] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[25] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[26] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[27] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[28] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[29] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[30] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[31] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*). https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[32] *Id*.

and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[33] Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees.[34] U.S. Census Bureau data from 2012 show that 1,341 firms provided resale services during that year.[35] Of that number, all operated with fewer than 1,000 employees.[36] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[37] Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees.[38] Consequently, the Commission estimates that the majority of local resellers are small entities.

14. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[39] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[40] Under that size standard, such a business is small if it has 1,500 or fewer employees.[41] 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[42] Of that number, 1,341 operated with fewer than 1,000 employees.[43] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision

[33] *See* U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[34] *See* 13 CFR § 121.201, NAICS Code 517911.

[35] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[36] *Id*. Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA's size standard.

[37] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[38] *See id*.

[39] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[40] *See* 13 CFR § 121.201, NAICS Code 517911.

[41] *Id.*

[42] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false..

[43] *Id.* Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA's size standard.

of toll resale services.[44] Of this total, an estimated 857 have 1,500 or fewer employees.[45] Consequently, the Commission estimates that the majority of toll resellers are small entities.

15. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable size standard under SBA rules is for Wired Telecommunications Carriers.[46] The applicable SBA size standard consists of all such companies having 1,500 or fewer employees.[47] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[48] Of that number, 3,083 operated with fewer than 1,000 employees.[49] Thus, under this category and the associated small business size standard, the majority of Other Toll Carriers can be considered small. According to internally developed Commission data, 284 companies reported that their primary telecommunications service activity was the provision of other toll carriage.[50] Of these, an estimated 279 have 1,500 or fewer employees.[51] Consequently, the Commission estimates that most Other Toll Carriers are small entities.

16. *800 and 800-Like Service Subscribers*. Neither the Commission nor the SBA has developed a small business size standard specifically for 800 and 800-like service ("toll free") subscribers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[52] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[53] Under that size standard, such a business is small if it has 1,500 or fewer employees.[54] 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[55] Of that number, 1,341 operated with fewer than 1,000 employees.[56]

---

[44] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[45] *See id.*

[46] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[47] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[48] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[49] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[50] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[51] *Id*.

[52] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search

[53] *See* 13 CFR § 121.201, NAICS Code 517911.

[54] *Id.*

[55] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911,

(continued….)

Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[57] Of this total, an estimated 857 have 1,500 or fewer employees.[58] Consequently, the Commission estimates that the majority of 800 and 800-Like Service Providers are small.

17. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[59] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[60] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[61] Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more.[62] Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

18. *Broadband Personal Communications Service.* The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[63] For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[64] These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA.[65] No small

(Continued from previous page)
https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[56] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of establishments that meet the SBA size standard.

[57] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[58] *See id.*

[59] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite)",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517312&search=2017+NAICS+Search&search=2017.

[60] *See* 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

[61] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012.

[62] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[63] *See Amendment of Parts 20 and 24 of the Commission's Rules – Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap; Amendment of the Commission's Cellular/PCS Cross-Ownership Rule*; WT Docket No. 96-59, GN Docket No. 90-314, Report and Order, 11 FCC Rcd 7824, 7850-52, paras. 57-60 (1996) (*PCS Report and Order*); *see also* 47 CFR § 24.720(b).

[64] *See PCS Report and Order*, 11 FCC Rcd at 7852, para. 60.

[65] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks.[66] On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22.[67] Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

19. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status.[68] Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses.[69] On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71.[70] Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses.[71] On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block Broadband PCS licenses in Auction No. 78.[72] Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.[73]

20. *Advanced Wireless Services (AWS) - (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3))*. For the AWS-1 bands,[74] the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and

[66] *See D*, *E and F Block Auction Closes*, Public Notice, DA-97-81 (Jan. 15, 1997), 1997 WL 20711.

[67] *See C*, *D*, *E*, *and F Block Broadband PCS Auction Closes*, Public Notice, 14 FCC Rcd 6688 (WTB 1999). Before Auction No. 22, the Commission established a very small standard for the C Block to match the standard used for F Block. *Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licensees*, WT Docket No. 97-82, Fourth Report and Order, 13 FCC Rcd 15743, 15768, para. 46 (1998).

[68] *See C and F Block Broadband PCS Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 2339 (2001).

[69] *See Broadband PCS Spectrum Auction Closes; Winning Bidders Announced for Auction No. 58*, Public Notice, 20 FCC Rcd 3703 (2005).

[70] *See Auction of Broadband PCS Spectrum Licenses Closes; Winning Bidders Announced for Auction No. 71*, Public Notice, 22 FCC Rcd 9247 (2007).

[71] *Id*.

[72] *See Auction of AWS-1 and Broadband PCS Licenses Closes; Winning Bidders Announced for Auction 78*, Public Notice, 23 FCC Rcd 12749 (WTB 2008).

[73] *Id.*

[74] The service is defined in section 90.1301 *et seq*. of the Commission's Rules, 47 CFR § 90.1301 *et seq*.

other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.[75]

21. *Specialized Mobile Radio Licenses.* The Commission awards "small entity" bidding credits in auctions for Specialized Mobile Radio (SMR) geographic area licenses in the 800 MHz and 900 MHz bands to firms that had revenues of no more than $15 million in each of the three previous calendar years.[76] The Commission awards "very small entity" bidding credits to firms that had revenues of no more than $3 million in each of the three previous calendar years.[77] The SBA has approved these small business size standards for the 900 MHz Service.[78] The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz bands. The 900 MHz SMR auction began on December 5, 1995 and closed on April 15, 1996. Sixty bidders claiming that they qualified as small businesses under the $15 million size standard won 263 geographic area licenses in the 900 MHz SMR band. The 800 MHz SMR auction for the upper 200 channels began on October 28, 1997 and was completed on December 8, 1997. Ten bidders claiming that they qualified as small businesses under the $15 million size standard won 38 geographic area licenses for the upper 200 channels in the 800 MHz SMR band.[79] A second auction for the 800 MHz band conducted in 2002 and included 23 BEA licenses. One bidder claiming small business status won five licenses.[80]

22. The auction of the 1,053 800 MHz SMR geographic area licenses for the General Category channels was conducted in 2000. Eleven bidders won 108 geographic area licenses for the General Category channels in the 800 MHz SMR band and qualified as small businesses under the $15 million size standard.[81] In an auction completed in 2000, a total of 2,800 Economic Area licenses in the lower 80 channels of the 800 MHz SMR service were awarded.[82] Of the 22 winning bidders, 19 claimed small business status and won 129 licenses. Thus, combining all four auctions, 41 winning bidders for geographic licenses in the 800 MHz SMR band claimed status as small businesses.

23. In addition, there are numerous incumbent site-by-site SMR licenses and licensees with extended implementation authorizations in the 800 and 900 MHz bands. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. In addition, we do not know how many of these firms have 1,500 or fewer employees, which is the SBA-determined size standard for Wireless Telecommunications

---

[75] *See Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Report and Order, 18 FCC Rcd 25162, Appx. B (2003), *modified by Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Order on Reconsideration, 20 FCC Rcd 14058, Appx. C (2005); *Service Rules for Advanced Wireless Services in the 1915–1920 MHz*, *1995–2000 MHz*, *2020–2025 MHz and 2175–2180 MHz Bands; Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, 19 FCC Rcd 19263, Appx. B (2005); *Service Rules for Advanced Wireless Services in the 2155–2175 MHz Band*, Notice of Proposed Rulemaking, 22 FCC Rcd 17035, Appx. (2007).

[76] 47 CFR § 90.814(b)(1).

[77] *Id*.

[78] *See* Letter from Aida Alvarez, Administrator, SBA, to Thomas Sugrue, Chief, Wireless Telecommunications Bureau, Federal Communications Commission (filed Aug. 10, 1999) (*Alvarez Letter 1999*).

[79] *See Correction to Public Notice DA 96-586 "FCC Announces Winning Bidders in the Auction of 1020 Licenses to Provide 900 MHz SMR in Major Trading Areas*," Public Notice, 18 FCC Rcd 18367 (WTB 1996).

[80] *See Multi-Radio Service Auction Closes*, Public Notice, 17 FCC Rcd 1446 (WTB 2002).

[81] *See 800 MHz Specialized Mobile Radio (SMR) Service General Category (851–854 MHz) and Upper Band (861–865 MHz) Auction Closes; Winning Bidders Announced*, Public Notice, 15 FCC Rcd 17162 (2000).

[82] *See 800 MHz SMR Service Lower 80 Channels Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 1736 (2000).

Carriers (except Satellite).[83] We assume, for purposes of this analysis, that all of the remaining extended implementation authorizations are held by small entities, as defined by the SBA.

24. *Lower 700 MHz Band Licenses*. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits.[84] The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[85] A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[86] Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[87] The SBA approved these small size standards.[88] An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses.[89] A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses.[90] Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses.[91] On July 26, 2005, the Commission completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

25. In 2007, the Commission reexamined its rules governing the 700 MHz band in the *700 MHz Second Report and Order*.[92] An auction of 700 MHz licenses commenced January 24, 2008, and closed on March 18, 2008, which included: 176 Economic Area licenses in the A-Block, 734 Cellular

---

[83] *See generally* 13 CFR § 121.201, NAICS Code 517312.

[84] *See Reallocation and Service Rules for the 698–746 MHz Spectrum Band (Television Channels 52–59)*, Report and Order, 17 FCC Rcd 1022 (2002) (*Channels 52–59 Report and Order*).

[85] *See id*. at 1087-88, para. 172.

[86] *See id*.

[87] *See id*. at 1088, para. 173.

[88] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[89] *See Lower 700 MHz Band Auction Closes*, Public Notice, 17 FCC Rcd 17272 (WTB 2002).

[90] *See id*.

[91] *See id*.

[92] *Service Rules for the 698–746*, *747–762 and 777–792 MHz Band; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones; Biennial Regulatory Review—Amendment of Parts 1*, *22*, *24*, *27*, *and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services; Former Nextel Communications*, *Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules; Implementing a Nationwide*, *Broadband*, *Interoperable Public Safety Network in the 700 MHz Band; Development of Operational*, *Technical and Spectrum Requirements for Meeting Federal*, *State and Local Public Safety Communications Requirements Through the Year 2010; Declaratory Ruling on Reporting Requirement under Commission's Part 1 Anti-Collusion Rule*, WT Docket Nos. 07-166, 06-169, 06-150, 03-264, and 96-86, PS Docket No. 06-229, CC Docket No. 94-102, Second Report and Order, 22 FCC Rcd 15289, 15359 n.434 (2007) (*700 MHz Second Report and Order*).

Market Area licenses in the B-Block, and 176 EA licenses in the E-Block.[93] Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty-three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

26. *Upper 700 MHz Band Licenses*. In the *700 MHz Second Report and Order*, the Commission revised its rules regarding Upper 700 MHz licenses.[94] On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block.[95] The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

27. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[96] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules.[97] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[98] Of this total, 299 firms had annual receipts of less than $25 million.[99] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

28. *All Other Telecommunications*. The **"**All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[100] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[101] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[102] The SBA has developed a small business size standard for "All Other Telecommunications", which consists of all such firms with annual receipts of $35 million or less.[103] For

---

[93] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[94] *700 MHz Second Report and Order*, 22 FCC Rcd 15289.

[95] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[96] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

[97] *See* 13 CFR § 121.201, NAICS Code 517410.

[98] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012.

[99] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[100] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517919&search=2017+NAICS+Search&search=2017.

[101] *Id.*

[102] *Id*.

this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[104] Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49, 999,999.[105] Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

29. *Other Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[106] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[107] The SBA has established a size standard for this industry as all such firms having 750 or fewer employees.[108] U.S. Census Bureau data for 2012 shows that 383 establishments operated in that year.[109] Of that number, 379 operated with fewer than 500 employees and 4 had 500 to 999 employees.[110] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

30. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[111] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[112] The SBA has established a small business size standard for this industry of 1,250 employees or less.[113] U.S. Census Bureau data for 2012 show that 841 establishments operated in this industry in that year.[114] Of that number, 828 establishments operated with fewer than 1,000

(Continued from previous page)

[103] *See* 13 CFR § 121.201, NAICS Code 517919.

[104] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[105] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[106] *See* U.S. Census Bureau, *2017 NAICS Definition, "334290 Other Communications Equipment Manufacturing*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334290&search=2017+NAICS+Search&search=2017.

[107] *Id.*

[108] *See* 13 CFR 121.201, NAICS Code 334290.

[109] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size*: *2012*, NAICS Code 334290, https://data.census.gov/cedsci/table?text=EC1231SG2&n=334290&tid=ECNSIZE2012.EC1231SG2&hidePreview=false&vintage=2012.

[110] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[111] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=334220&search=2017.

[112] *Id*.

[113] *See* 13 CFR § 121.201, NAICS Code 334220.

[114] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012*,

(continued….)

employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments operated with 2,500 or more employees.[115] Based on this data, we conclude that a majority of manufacturers in this industry are small.

31. *Engineering Services*. This industry comprises establishments primarily engaged in applying physical laws and principles of engineering in the design, development, and utilization of machines, materials, instruments, structures, process, and systems.[116] The assignments undertaken by these establishments may involve any of the following activities: provision of advice, preparation of feasibility studies, preparation of preliminary and final plans and designs, provision of technical services during the construction or installation phase, inspection and evaluation of engineering projects, and related services.[117] This category includes civil, environmental, construction and mechanical engineering services, and engineers' offices.[118]

32. The SBA has different small business size standards for different types of engineering services in this industry. For engineering firms except military and aerospace equipment and military weapons engineering, contracts and subcontracts for engineering services awarded under the National Energy Policy Act of 1992 and marine engineering and naval architecture are deemed small under the SBA standard if they have $16.5 million or less in annual receipts.[119] The SBA deems military and aerospace equipment and military weapons engineering, contracts and subcontracts for engineering services awarded under the National Energy Policy Act of 1992 and marine engineering and naval architecture firms small if they have annual receipts of $41.5 million or less.[120]

33. The U.S. Census Bureau includes engineering services under the SBA size standard of $16.5 million and $38 million under the same NAICS code.[121] According to 2012 U.S. Census Bureau data, there were 37,184 engineering services firms that operated for the entire year.[122] Of the 37,184 firms, 35,096 had less than $10 million in annual receipts, and 2,088 had $10 million or more in annual receipts.[123] Accordingly, the Commission estimates that a majority of engineering service firms are small.

34. *Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing.* This U.S. industry comprises establishments primarily engaged in manufacturing search, detection, navigation, guidance, aeronautical, and nautical systems and

(Continued from previous page)
NAICS Code 334220,
https://data.census.gov/cedsci/table?text=EC1231SG2&n=334220&tid=ECNSIZE2012.EC1231SG2&hidePreview=false.

[115] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[116] *See* U.S. Census Bureau, *2017 NAICS Definition, "541330 Engineering Services*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=541330&search=2017+NAICS+Search&search=2017.

[117] *Id.*

[118] *Id.*

[119] *See* 13 CFR § 121.201, NAICS Code 541330.

[120] *Id.*

[121] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1254SSSZ4, *Professional, Scientific, and Technical Services: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the U.S.: 2012,* NAICS Code 541330,
https://data.census.gov/cedsci/table?y=2012&n=541330&tid=ECNSIZE2012.EC1254SSSZ4&hidePreview=false.

[122] *Id.*

[123] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

instruments. Examples of products made by these establishments are aircraft instruments (except engine), flight recorders, navigational instruments and systems, radar systems and equipment, and sonar systems and equipment.[124] The SBA has established a size standard for this industry of 1,250 or fewer employees.[125] U.S. Census Bureau data for 2012 show that 588 establishments operated in this industry for the entire year.[126] Of that number, 557 establishments operated with fewer than 1,000 employees, 21 establishments operated with between 1,000 and 2,499 employees and 10 establishments operated with 2,500 or more employees.[127] Based on this data, we conclude that a majority of manufacturers in this industry are small.

35. *Security Guards and Patrol Services*. This industry comprises establishments primarily engaged in providing guard and patrol services such as bodyguard, guard dog, and parking security services.[128] The SBA deems security guards and patrol services firms as small if they have $22 million or less in annual receipts.[129] According to U.S. Census Bureau data for 2012, there were 4,873 firms that operated for the entire year.[130] Of the 4,873 firms, 4,649 had less than $10 million in annual receipts while 224 had more than $10 million in annual receipts.[131] Accordingly, the Commission estimates that a majority of firms in this category are small.

36. *All Other Support Services*. This industry comprises establishments primarily engaged in providing day-to-day business and other organizational support services (except office administrative services, facilities support services, employment services, business support services, travel arrangement and reservation services, security and investigation services, services to buildings and other structures, packaging and labeling services, and convention and trade show organizing services).[132] The SBA deems all other support services firms to be small if they have $12 million or less in annual receipts.[133] According to U.S. Census Bureau data for 2012, there were 9,742 firms in this industry in operation for the full year.[134] Of the 9,742 firms, 9,518 had less than $10 million while 224 had greater than $10

---

[124] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*334511 Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334511&search=2017+NAICS+Search&search=2017.

[125] *See* 13 CFR § 121.201, NAICS Code 334511.

[126] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012*, NAICS Code 334511, https://data.census.gov/cedsci/table?y=2012&n=334511&tid=ECNSIZE2012.EC1231SG2&hidePreview=false.

[127] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[128] *See* U.S. Census Bureau, *2017 NAICS Definition, "561612 Security Guards and Patrol Services",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561612&search=2017+NAICS+Search&search=2017.

[129] *See* 13 CFR § 121.201, NAICS Code 561612.

[130] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size: Summary Statistics by Receipts Size of Firms for the U.S.: 2012*, NAICS Code 561612, https://data.census.gov/cedsci/table?y=2012&n=561612&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false.

[131] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[132] *See* U.S. Census Bureau, *2017 NAICS Definition, "561990 All Other Support Services*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561990&search=2017+NAICS+Search&search=2017.

[133] *See* 13 CFR § 121.201, NAICS Code 561990.

million in annual receipts.[135] Accordingly, the Commission estimates that a majority of firms in this category are small.

37. *Correctional Institutions (State and Federal Facilities)*. This industry comprises government establishments primarily engaged in managing and operating correctional institutions.[136] The facility is generally designed for the confinement, correction, and rehabilitation of adult and/or juvenile offenders sentenced by a court. The Department of Justice's Bureau of Justice Statistics (BJS) collects and publishes census information on adult correctional facilities operating under state or federal authority as well as private and local facilities operating under contract to house inmates for federal or state correctional authorities.[137] The types of facilities included in the census data from BJS are prisons and prison farms; prison hospitals; centers for medical treatment and psychiatric confinement; boot camps; centers for reception; diagnosis; classification; alcohol and drug treatment; community correctional facilities; facilities for parole violators and other persons returned to custody; institutions for youthful offenders; and institutions for geriatric inmates.[138]

38. While neither the SBA nor the Commission has developed a size standard for this category, the size standard for a small facility in the BJS census data is one that has an average daily population (ADP) of less than 500 inmates. The latest BJS census data available shows that as December 30, 2005 there were a total of 1821 correctional facilities operating under state or local federal authority.[139] Of that number more than half of the facilities or a total 946 facilities had an average daily population of less than 500 inmates.[140] Based on this data a majority of "Governmental Correctional Institutions" potentially affected by the rules adopted can be considered small.

39. *Facilities Support Services*. This industry comprises establishments primarily engaged in providing operating staff to perform a combination of support services within a client's facilities.[141] Establishments in this industry typically provide a combination of services, such as janitorial, maintenance, trash disposal, guard and security, mail routing, reception, laundry, and related services to support operations within facilities. These establishments provide operating staff to carry out these support activities but are not involved with or responsible for the core business or activities of the client. Establishments providing facilities (except computer and/or data processing) operation support services and establishments providing private jail services or operating correctional facilities (i.e., jails) on a

(Continued from previous page)

[134] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size: Summary Statistics by Receipts Size of Firms for the U.S.: 2012*, NAICS Code 561990, https://data.census.gov/cedsci/table?y=2012&n=561990&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false

[135] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[136] *See* U.S. Census Bureau, *2017 NAICS Definition, "922140 Correctional Institutions*," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=922140&search=2017+NAICS+Search&search=2017.

[137] *See* U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, Census of State and Federal Correctional Facilities, 2005 at 1. (Oct 2008), https://www.bjs.gov/content/pub/pdf/csfcf05.pdf.

[138] *Id.*

[139] *Id.* Appendix table 3. "Number of correctional facilities under state or federal authority, by size, June 30, 2000, and December 30, 2005." This data excludes city, county, and regional jails and private facilities that did not house primarily state or federal incarcerated people. It also excluded facilities for the military, U.S. Immigration and Customs Enforcement (ICE), Bureau of Indian Affairs (BIA), U.S. Marshals Service (USMS), and correctional hospital wards not operated by correctional authorities.

[140] *Id.*

[141] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*561210 Facilities Support Services",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561210&search=2017+NAICS+Search&search=2017.

contract or fee basis are included in this industry. The SBA small business size standard for this category classifies all such entities having $41.5 million or less in annual receipts as small.[142] According to U.S. Census Bureau data for 2012, there were 1,669 firms in this category that operated for the entire year.[143] Of this number 1,549 firms had annual receipts of less than $25 million, and 60 firms had annual receipts between $25,000,000 and $49,999,999.[144] Based on this information, the majority of firms in this category can be considered small under the SBA small business size standard.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

40. The *Second Report and Order* adopts new or additional reporting or recordkeeping and compliance obligations for small entities as well as other applicants and licensees. Small entities may have to hire attorneys, engineers, consultants, or other professionals in order to meet the reporting, recordkeeping or compliance obligations in the *Second Report and Order,* however, the Commission cannot quantify the cost of compliance with the requirements. To minimize burdens, we have adopted processes and procedures where possible to allow direct interaction between the DCFOs and the wireless providers and avoided interjecting the Commission and additional regulations into the process. In our approach, we sought to provide small and other entities flexible options such as giving DCFOs and wireless providers the flexibility to structure the format of the qualifying requests in a way that meets the unique needs of the parties rather than adopting a standardized form. We also adopted minimum requirements for information to be included in a qualifying request to disable a contraband device and allowed for self-certification to meet the certification requirements. Below we discuss reporting, recordkeeping, and/or compliance requirements adopted in the *Second Report and Order*.

41. Designated Correctional Facility Official Requirements. The *Second Report and Order* requires that a DCFO satisfy certain requirements in order to submit qualifying requests to wireless providers. Specifically, qualifying disabling requests must be submitted by a DCFO, which we define as an official of the state, local, or federal government with responsibility for oversight of the relevant facility. In government-run correctional facilities, this definition requires the DCFO to be, at a minimum, the official with responsibility for oversight of the relevant facility (e.g., the warden) or higher ranking official; in privately-run correctional facilities, the DCFO must be a government official with responsibility for oversight of the facility's performance through a contract.

42. The *Second Report and Order* also adopts a process for certification of DCFOs that will provide certainty to wireless providers that disabling requests are duly authorized by the relevant federal, state, or local government entities. The Commission will maintain a publicly available list of DCFOs that are authorized to transmit qualifying disabling requests. Authorized individuals that wish to be recognized on the Commission's DCFO list must send a letter to the Commission's Contraband Ombudsperson, signed by the relevant state attorney general, providing the individual's name, official government position, and a list of correctional facilities over which the individual has oversight and management authority.

43. Authorization of CISs. The *Second Report and Order* establishes a two-phase authorization process for CIS applicants seeking to deploy CISs that will provide the requisite

---

[142] *See* 13 CFR § 121.201, NAICS Code 561210.

[143] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size: Summary Statistics by Receipts Size of Firms for the U.S.: 2012*, NAICS Code 561210, https://data.census.gov/cedsci/table?y=2012&n=561210&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false.

[144] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

information necessary for DCFOs to submit qualifying requests to disable contraband devices at qualifying correctional facilities. In phase one, CIS applicants will submit applications to the Wireless Telecommunications Bureau (the Bureau) describing their legal and technical qualifications of the systems. The Bureau will review the applications and approve—at a system level—those CISs that meet the requirements. In phase two, CIS applicants will perform on-site testing of approved CISs at individual qualifying correctional facilities. After both phases are complete, DCFOs will be authorized to submit qualifying requests to disable contraband devices using approved CISs at each approved correctional facility.

44. *CIS Certification Process*. The *Second Report and Order* adopts a CIS certification process for detection systems to be used in qualifying requests. To obtain CIS certification, a CIS applicant must submit an application to the Bureau for review and approval. The application must demonstrate, at a minimum that: (1) all radio transmitters used as part of the CIS have appropriate equipment authorization pursuant to Commission rules; (2) the CIS is designed and will be configured to locate devices solely within a correctional facility; (3) the methodology to be used in analyzing data collected by the CIS is sufficiently robust to ensure that the particular wireless device is in fact located within a correctional facility, including specific data analysis benchmarks designed to ensure successful detection, such as rate of detection of contraband versus non-contraband devices, relevant sample size (e.g. number of devices observed and length of observation period); (4) the CIS will secure and protect all information or data collected as part of its intended use; and (5) the CIS will not interfere with emergency 911 calls. The application must also include a description of whether the CIS requires a spectrum or network access agreement (e.g., a spectrum leasing arrangement and/or roaming agreement) to be authorized to operate. Finally, the application must include a proposed test plan for subsequent site-based testing of each CIS, which must include detailed descriptions and technical specifications to facilitate Commission review of whether the system satisfies its legal requirements and technically functions as anticipated.

45. *Site-Based Testing and Self-Certification Requirement*. In the second phase of the CIS authorization process, a CIS operator—which could be a CIS solutions provider, or a DCFO or other responsible party that deploys its own CIS at a correctional facility[145]—seeking to use the CIS to submit qualifying requests for disabling contraband devices must test a certified CIS at each location and, thereafter, must file a self-certification to the Bureau confirming that the testing at that specific correctional facility is complete and successful. The CIS operator must also serve notice of the testing on each of the wireless providers holding a spectrum license that includes the county within which the correctional facility is located and provide a reasonable opportunity to participate in the tests. Following the testing, and to be eligible for use in conjunction with qualifying requests for disabling, the CIS operator must submit a self-certification that: (1) identifies the correctional facility where it seeks to deploy; (2) attests that applicable federal or state criminal statutes prohibit possession or operation of contraband devices within the correctional facility (and includes the applicable federal or state criminal statutory provision); (3) describes the results of on-site tests of the certified CIS conducted at the correctional facility; (4) attests that the on-site testing was performed consistent with the approved test plans for the certified CIS and that the CIS deployment minimizes the risk of disabling a non-contraband device; (5) identifies whether any wireless providers participated in the testing, and provides proof that the wireless providers were given notice regarding the testing and a reasonable opportunity to participate; and (6) includes proof of any spectrum and/or network access agreement (e.g., a spectrum leasing arrangement and/or roaming agreement) required to be authorized to operate and/or for the system to function effectively. The self-certification submitted by a CIS operator must be accompanied by an attestation from the DCFO verifying that all information contained in the self-certification is true and accurate.

[145] *See* Appendix A, Final Rules (adding definition to section 20.3 of the Commission's rules, 47 CFR § 20.3).

46. CIS operators must submit self-certifications in accordance with filing procedures established by the Bureau and those certifications must also be served via electronic means on all wireless providers licensed in the geographic area occupied by the correctional facility. Wireless providers have five business days from the certification filing date to submit objections to the Bureau and to serve any such objections on the DCFO and the CIS operator. Absent objections, the DCFO may submit qualifying requests to wireless providers beginning on the sixth business day after the certification filing. If an objection is submitted, the DCFO may not submit qualifying requests until the Bureau addresses the objection.

47. *Records Maintenance*. To ensure the integrity and proper operation of CIS, we require CIS operators to retain records of all information supporting each request for disabling and the basis for disabling each device, for at least five years following the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must also make available all records upon request from the Bureau.

48. *Recertification*. In order to ensure the ongoing accuracy and reliability of a given CIS at a particular facility, at least every three years after the initial self-certification, CIS operators seeking to maintain the ability to submit qualifying requests through a DCFO to disable contraband devices must retest their systems and recertify them for continued CIS accuracy. Recertifications must comply with the same rules and filing instructions that apply to the initial self-certification.

49. *Qualifying Requests*. We required that qualifying requests to disable a contraband device include the following material: (1) a certification that (a) a certified CIS was used to gather the contraband subscriber and device information populated in the qualifying request; (b) the certified CIS was used to identify contraband devices operating in a correctional facility where the CIS has been tested and self-certified for operational readiness and for use in qualifying requests, and the identification of contraband devices occurred within 30 days immediately prior to the date of the qualifying request submission; (c) the DCFO has reviewed the list of contraband devices and attests that it is accurate; and (d) it is a violation of applicable state or federal criminal statutes to possess or operate a contraband device in the correctional facility; (2) the name and address of each requesting correctional facility; and (3) a list of contraband devices with identifiers sufficient to uniquely describe the devices in question at both the subscription and device level.

50. *Disabling Process and Timeframe for Disabling a Contraband Device*. The *Second Report and Order* adopts the following process for disabling contraband devices. Upon receipt of a qualifying request from a DCFO through a verifiable and secure transmission method, a wireless provider must treat the request as valid. The wireless provider may only reject a request if the request fails to meet the Commission-mandated information for a qualifying request or if there are errors with respect to the device identifying information that leave the wireless provider unable to disable the device. Unless a wireless provider finds these grounds to reject the qualifying request, it must, within two business days after receipt of a qualifying request: (1) disable the device at both the subscriber level and at the device level; and (2) take reasonable and practical steps to prevent an identified device from being accessing another wireless provider's network (e.g., by adding the equipment identifier to the Stolen Phone Database). A wireless provider must inform the DCFO whether or not the request has been granted within two business days of receiving the qualifying request.

51. *Reversals.* A wireless provider may subsequently reverse a device disabling if it determines that the device was identified erroneously as contraband. If the wireless provider chooses to reverse a disabling, however, it must promptly inform the DCFO of the mistakenly identified device. The *Second Report and Order* also provides wireless providers with the option to trigger the involvement of the DCFO in the reviewing the validity of a device previously identified and disabled as contraband. If the wireless provider seeks to trigger the DCFO's involvement, it must provide the DCFO with: (1) the date of the qualifying request, (2) the identifying information provided for the device, and (3) any evidence supporting the wireless provider's belief that the device was erroneously identified. The *Second Report and Order* states that, upon receipt of such a request, the DCFO should review the qualifying

request to determine whether the device in question was erroneously identified and either: (1) confirm the validity of the identifying information contained in the qualifying request, or (2) acknowledge the error and direct the carrier to restore service to the device. In the event the DCFO directs the wireless provider to reverse the disabling, the wireless provider must, within two business days, restore service to the device and reverse any actions taken to prevent the device from accessing other wireless provider networks (e.g., by removing the phone from the Stolen Phone Database). In the event the DCFO does not respond to a request from a wireless provider for review of a qualifying request within two business days, the wireless provider may proceed with reversing the disabling action. The *Second Report and Order* requires the DCFO to provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices on a quarterly basis at the end of any quarter during which a device disabling was reversed, and directs the Wireless Telecommunications Bureau to issue a public notice providing additional guidance regarding the appropriate method for providing such notice.

52. Transmission of the Qualifying Request. DCFOs must transmit a qualifying request to a wireless provider using a verifiable and secure transmission method, and a wireless provider must adopt a method, or utilize an existing method, for receiving secured and verified qualifying requests. The *Second Report and Order* directs the Contraband Ombudsperson to work with wireless providers to develop suitable methods for securely transmitting a qualifying request.

53. Notification to CIS Operators of Wireless Provider Technical Changes. Commercial Mobile Radio Service (CMRS) licensees leasing spectrum to managed access systems (MAS) must provide 90 days advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, while permitting modified notice arrangements through mutual agreement: (1) adding a new frequency band to service offerings; (2) deploying a new air interface technology or changing an existing air interface technology; and/or (3) adding, relocating, or removing a site. This limited notification requirement is necessary to deploy MAS effectively. The *Second Report and Order* adopts an exception to the 90-day advance notice requirement for network technical changes within 15 miles of the facility that are required due to emergency/disaster preparedness, but it requires CMRS licensees to provide notice of these technical changes immediately after the exigency. The *Second Report and Order* also requires CMRS licensee lessors and MAS operator lessees to negotiate in good faith to reach an agreement for notification for other, more localized types of network adjustments not covered bv the major network change notice requirement. The *Second Report and Order* further requires CMRS licensees and MAS operators to negotiate in good faith regarding the parties' treatment of confidential information contained in notifications required by rule and/or negotiated between the parties.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

54. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities."[146]

55. The *Second Report and Order* establishes rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopts a framework to facilitate the disabling process. We have taken steps to minimize the economic impact on small and other impacted entities with the rules we adopt by providing flexibility, minimum requirements, and permitting and encouraging negotiations and collaboration between the parties subject to our requirements rather than adopting additional rules.

[146] 5 U.S.C. § 604(a)(6).

56. *Rule-Based Disabling Process*. We adopted a rule-based disabling process, which will provide an efficient, effective means for stakeholders to address the issue of contraband device use and includes the same safeguards against erroneous disabling and potential carrier liability as would a more burdensome and time-consuming court order process. We considered but rejected a court-ordered termination process, which we concluded would be unnecessarily burdensome, time-consuming, especially for small entities, and may impose unnecessary legal costs.

57. *Designated Correctional Facility Official Requirements*. We adopted requirements for qualifying DCFOs that will ensure parties making disabling requests have the necessary authority and accountability to safeguard the integrity of the contraband device identification and disabling process. Specifically, we require that qualifying disabling requests be submitted by a government official with responsibility for administration of the correctional facility. We also adopted a process for certification of DCFOs that will provide certainty to small and other wireless providers that disabling requests are duly authorized by the relevant federal, state, or local government entities.

58. In adopting this requirement, we considered whether the Commission, instead of DCFOs, should transmit the qualifying requests directly to wireless providers. We concluded that injecting the Commission in the process at the request transmission stage could cause unnecessary delay, particularly during an exigent circumstance where immediate disabling is justified due to the threat to public or facility safety. We also concluded that it is in the public interest to define an eligible DCFO as an official of the state, local, or federal government entity responsible for administration and oversight of the relevant correctional facility because these individuals have the authority and incentive to ensure the accuracy of devices identified as contraband. The Commission will maintain a publicly available list of DCFOs that are authorized to transmit a qualifying request, which will reduce the burden on small entities who would otherwise be required to conduct independent investigations to verify the qualifications of the DCFO transmitting the request.

59. *CIS Certification Process*. The required information for compliance with the certification requirement including technical specifications and proposed test plans, should be readily available to a prepared applicant and is consistent with the type of showing the Commission typically requires prospective operators to provide and should therefore minimize the burden on small entities to comply with this requirement. The Commission took steps to adopt a process that includes minimal requirements to ensure that CISs are designed to minimize the risk of disabling a non-contraband device, while refraining from imposing additional burdens, such as requiring that CIS operators fully deploy or test the systems prior to obtaining CIS certification which should likewise lessen the economic impact for small entities.

60. *Site-Based Testing and Self-Certification Requirement*. The on-site testing and self-certification requirements we adopted will help ensure that qualifying requests identify contraband devices accurately and in accordance with relevant legal authorities, and will ensure that the systems detecting contraband wireless devices are designed to support operational readiness and minimize the risk of disabling a non-contraband device. This approach avoids potential conflict of law issues that small and other wireless providers might otherwise face in complying with the rule-based disabling process we adopted. In addition, while we considered arguments from some commenters that CIS operators should be authorized to identify contraband wireless devices for disabling so long as there is at least a correctional facility policy prohibiting the use of contraband wireless devices, we determined that a more stringent policy requiring a state or federal prohibition is appropriate in this context.

61. *Records Maintenance*. To ensure the integrity and proper operation of CIS, we require CIS operators to retain records of all information supporting each request for disabling and the basis for disabling each device, for at least five years following the relevant disabling request. CIS operators of systems that have been tested and approved for use in qualifying requests must also make available all records upon request from the Bureau. Requiring CIS operators to maintain records will support robust efforts to identify issues with CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices.

62. *Qualifying Requests*. We reduced the burden on small entities by adopting minimum information that must be included in a qualifying request from DCFOs to disable a contraband device. Further, adopting standardized information for qualifying requests will help expedite transmission and review of the request by the wireless provider, as well as reduce the administrative burden on DCFOs. We considered creating a standardized form for qualifying requests, but we find that a standardized form would not provide the flexibility sufficient to account for changes in technology and would deny the DCFOs and wireless providers the flexibility to develop solutions tailored to their specific needs. By requiring that qualifying requests include specific information necessary for wireless providers to consider the request without establishing a specific form, we provide DCFOs and wireless providers the flexibility to structure the format of the qualifying requests in a way that meets the unique needs of the parties. This approach should provide small entities and others with the flexibility to tailor solutions to the unique needs of particular facilities and specific wireless providers as the industry may find beneficial.

63. *Transmission of the Qualifying Request*. Our requirement for DCFOs to transmit a qualifying request to a wireless provider using a verifiable and secured transmission method and for wireless providers to adopt or utilize an existing method for receiving secured and verified qualifying requests does not endorse or require a particular technology, but instead directs that the transmitting system should contain features to ensure the integrity, authentication, and provenance of the data in the qualifying request. We recognize that some wireless providers already have existing secure portals used to receive court-ordered termination requests that may be useable to comply with our requirement which could minimize the cost of compliance for such providers, particularly those that are small entities. Thus, to facilitate this process, we have directed the Contraband Ombudsperson to work with wireless providers to develop suitable methods for securely transmitting a qualifying request. We find the Contraband Ombudsperson to be ideally situated to interface with stakeholders, including small entities, and assess the costs and benefits of each potential solution for small entities and other parties.

64. *Timeframe for Disabling a Contraband Device*. The record was mixed regarding the appropriate timeframe for a wireless provider to respond to a qualifying request to disable a contraband phone. Alternatives raised for our consideration included: termination of service within one business day of receiving a request from the FCC, within 24 hours of receiving a qualifying request and within one hour of receiving a qualifying request, unless there is a documentable life safety issue justifying immediate termination. Our adoption of a two-day period for responding to qualifying requests strikes an appropriate balance between the significant public interest benefits of ensuring that contraband devices are rapidly disabled and ensuring that small and other wireless providers have sufficient time to carry out the disabling process. Similarly, a two-day period is sufficient for a wireless provider to take reasonable and practical steps to prevent an identified device from accessing another wireless provider's network.

65. *Customer Outreach*. We gave small entities and other wireless providers the discretion to decide whether or not to notify a customer whose phone is being disabled under our rules. In doing so we minimize the impact and do not impose any additional costs on small entities and other wireless providers affected by the new rules.

66. *Reversals*. We considered whether the Commission should develop its own process for addressing erroneously identified contraband, but declined to do so because we believe that wireless providers are in the best position to undertake post-termination error-correction processes. As a result, small entities and other wireless providers are not subject additional procedural requirements and their associated administrative costs.

67. *Reporting Requirements*. We declined to impose reporting requirements by stakeholders at this juncture. Instead, we rely on informal communications among stakeholders and with the Contraband Ombudsperson, as well as marketplace information, for any additional oversight. We do not wish to impose reporting requirements that would be unduly burdensome on small and other entities utilizing resources that could otherwise be used to combat contraband devices in correctional facilities.

68. *No reimbursement for wireless providers*. In adopting a disabling process in the *Second Report and Order*, we rejected calls to reimburse wireless providers for device disabling, which would

create additional costs for small entities that would have been required to contribute to reimbursement costs.

69. *Notification to CIS Operators of Wireless Provider Technical Changes*. The 90-day notification requirement in the *Second Report and Order* applicable to CMRS licensees leasing spectrum to MAS[147] operators is necessary to ensure that MAS operators have adequate time to make changes to ensure that the system's effectiveness is maintained. We considered the current coordination process and determined the limited burden on small entities and other CMRS licensees imposed by this requirement is outweighed by its significant public interest benefits. Absent a notification requirement, the record indicates that MAS operators typically discover CMRS licensees' network changes only after the MAS is impacted, during which time incarcerated people may be able to bypass the MAS and directly access the wireless provider's network. The record also indicates that CMRS licensees typically plan these types of technical changes months before they are implemented and often provide notice of these changes to the public and third parties.

70. We took steps to lessen any burdens by permitting CMRS licensee lessors and MAS operator lessees to adjust the terms of the notification requirement by private agreement. We also provide an exception to the 90-day advance notice requirement for network technical changes within 15 miles of the facility that are required due to emergency/disaster preparedness, which ensures that wireless providers are not restricted in their ability to respond quickly during times of public or national emergencies. We note that because CMRS licensees already provide advance notice of such changes to other entities, small CMRS licensees may therefore already have notification distribution processes in place to facilitate compliance, resulting in minimal incremental costs to comply.

G. Report to Congress

71. The Commission will send a copy of the *Second Report and Order*, including this FRFA, in a report to Congress pursuant to the Congressional Review Act.[148] In addition, the Commission will send a copy of the *Second Report and* Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Second Report and Order*, and FRFA (or summaries thereof) will also be published in the Federal Register.[149]

[147] Managed Access Systems are CISs whose operations require: (1) one or more a lease agreements with CMRS operators; and (2) real time awareness of wireless provider spectrum use in the vicinity of the correctional facility where they are deployed.

[148] *See* 5 U.S.C. § 801(a)(1)(A).

[149] *See* 5 U.S.C. § 604(b).

APPENDIX C

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in this *Second Further Notice of Proposed Rulemaking* (*Second Further Notice*). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *Second Further Notice*. The Commission will send a copy of the *Second Further Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *Second Further Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. In today's *Second Further Notice* the Commission seeks comment on methods to provide additional tools and develop additional rules to alleviate the use of contraband wireless devices in correctional facilities. For decades, incarcerated people have smuggled wireless devices, including cell phones, into correctional facilities. Federal, state, and local correctional administrators recognize the need to address the contraband problem in correctional facilities. In 2010, Congress passed the Contraband Cell Phone Act, which prohibited the possession of cell phones in federal prisons by unauthorized persons. Similarly, a number of states have enacted legislation that designated wireless devices in correctional facilities as contraband, and a substantial majority of states impose criminal penalties for possessing or operating contraband wireless devices within correctional facilities. In conjunction with legislation, the federal government and states have been conducting trials and investing in technologies that will enable them to combat contraband wireless device use in correctional facilities.

3. As a result of the Commission's efforts in the 2013 *Notice of Proposed Rulemaking*, the 2017 *Further Notice*, and the *July 2020 Refresh PN*, we have developed an extensive record on a variety of technological solutions to combat contraband phone use in prisons.[4] In light of the extensive steps the Commission takes in the *Second Report and Order* to adopt a rule-based disabling process, in this *Second Further Notice*, the Commission seeks further comment on the relative effectiveness, viability, and cost of additional solutions previously identified in the record in these proceedings, particularly those referenced in Congress's Explanatory Statement to the 2021 Consolidated Appropriations Act.[5]

4. In the *Further Notice*, the Commission invited comment on other technological solutions, besides wireless provider-disabling of devices identified by Contraband Interdiction Systems (CISs), to address the problem of contraband wireless devices in correctional facilities.[6] Specifically, the

---

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See* 5 U.S.C. § 603(a).

[3] *See id*.

[4] *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Notice of Proposed Rulemaking, 28 FCC Rcd 6603 (2013) (*Notice of Proposed Rulemaking*); *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336 (2017) (*Further Notice*)*; Wireless Telecommunications Bureau Seeks to Refresh the Record on Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Public Notice, 35 FCC Rcd 7910 (2020) (*July 2020 Refresh PN*).

[5] *See* Explanatory Statement to 2021 Consolidated Appropriations Act, Book IV, 166 Cong. Rec. H8311, H8440 (daily ed. Dec. 21, 2020) (2021 Explanatory Statement).

Commission sought comment on the use of "quiet zones," geofencing, network-based solutions, and beacon systems.[7] In the 2021 Explanatory Statement, Congress urged the Commission to consider all legally permissible options for combatting contraband cellphone use, including the creation, or use, of ''quiet or no service zones,'' geolocation-based denial, and beacon technologies to geographically appropriate correctional facilities.[8] Through our discussion and inquiries in the *Second Further Notice*, the Commission specifically seeks comment on whether there have been technological, economic, policy, and/or legal developments sufficient to overcome the variety of challenges presented to the widespread deployment of these technologies and whether and how the Commission can further facilitate these technologies through a regulatory framework.

B. Legal Basis

5. The proposed action is authorized pursuant to sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposals discussed herein, if adopted.[9] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[10] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[11] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[12]

7. Small Businesses, Small Organizations, Small Governmental Jurisdictions. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[13] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[14] These types of

(Continued from previous page)

[6] *Further Notice*, 32 FCC Rcd at 2380-83, paras. 122-31.

[7] *Id*.

[8] *See* 2021 Explanatory Statement at H8440.

[9] 5 U.S.C. § 603(b)(3).

[10] *Id.* § 601(6).

[11] *Id.* § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[12] 15 U.S.C. § 632.

[13] *See* 5 U.S.C. § 601(3)-(6).

[14] *See* SBA, Office of Advocacy, "What's New With Small Business?", https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/23172859/Whats-New-With-Small-Business-2019.pdf (Sept 2019).

small businesses represent 99.9% of all businesses in the United States, which translates to 30.7 million businesses.[15]

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[16] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[17] Nationwide, for tax year 2018, there were approximately 571,709 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[18]

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[19] U.S. Census Bureau data from the 2017 Census of Governments[20] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[21] Of this number there were 36,931 general purpose governments (county[22], municipal and town or township[23]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[24] with enrollment

[15] *Id*.

[16] 5 U.S.C. § 601(4).

[17] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), "Who must file,"

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[18] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for Region 1-Northeast Area (76,886), Region 2-Mid-Atlantic and Great Lakes Areas (221,121), and Region 3-Gulf Coast and Pacific Coast Areas (273,702) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[19] 5 U.S.C. § 601(5).

[20] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[21] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* Table 2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[22] *See id.* at Table 5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[23] *See id. at* Table 6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

populations of less than 50,000.[25] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[26]

10. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[27] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[28] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[29] Of this total, 3,083 operated with fewer than 1,000 employees.[30] Thus, under this size standard, the majority of firms in this industry can be considered small.

11. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[31] The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[32] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.[33] Of that number, 3,083 operated with fewer than 1,000

(Continued from previous page)

[24] *See id.* at Table 10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* Table 4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[25] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[26] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations Tables 5, 6, and 10.

[27] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[28] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[29] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[30] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[31] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[32] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[33] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110,

(continued….)

employees.[34] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[35] Of this total, an estimated 317 have 1,500 or fewer employees.[36] Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

12. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[37] Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees.[38] U.S. Census Bureau data from 2012 show that 1,341 firms provided resale services during that year.[39] Of that number, all operated with fewer than 1,000 employees.[40] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[41] Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees.[42] Consequently, the Commission estimates that the majority of local resellers are small entities.

13. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[43] The SBA has developed a small business size standard for the category of

(Continued from previous page)
https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[34] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[35] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*). https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[36] *Id*.

[37] *See* U.S. Census Bureau, *2017 NAICS Definition, "517911 Telecommunications Resellers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[38] *See* 13 CFR § 121.201, NAICS Code 517911.

[39] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[40] *Id*. Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA's size standard.

[41] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[42] *See id*.

Telecommunications Resellers.[44] Under that size standard, such a business is small if it has 1,500 or fewer employees.[45] 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[46] Of that number, 1,341 operated with fewer than 1,000 employees.[47] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[48] Of this total, an estimated 857 have 1,500 or fewer employees.[49] Consequently, the Commission estimates that the majority of toll resellers are small entities.

14. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. The closest applicable size standard under SBA rules is for Wired Telecommunications Carriers.[50] The applicable SBA size standard consists of all such companies having 1,500 or fewer employees.[51] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[52] Of that number, 3,083 operated with fewer than 1,000 employees.[53] Thus, under this category and the associated small business size standard, the majority of Other Toll Carriers can be considered small. According to internally developed Commission data, 284 companies reported that their primary telecommunications service activity was the provision of other toll carriage.[54] Of these, an estimated 279 have 1,500 or fewer employees.[55] Consequently, the Commission estimates that most Other Toll Carriers are small entities.

(Continued from previous page)

[43] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[44] *See* 13 CFR § 121.201, NAICS Code 517911.

[45] *Id.*

[46] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false..

[47] *Id.* Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA's size standard.

[48] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[49] *See id.*

[50] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[51] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[52] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[53] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[54] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[55] *Id.*

15. *800 and 800-Like Service Subscribers*. Neither the Commission nor the SBA has developed a small business size standard specifically for 800 and 800-like service ("toll free") subscribers. The appropriate size standard under SBA rules is for the category Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[56] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[57] Under that size standard, such a business is small if it has 1,500 or fewer employees.[58] 2012 U.S. Census Bureau data show that 1,341 firms provided resale services during that year.[59] Of that number, 1,341 operated with fewer than 1,000 employees.[60] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[61] Of this total, an estimated 857 have 1,500 or fewer employees.[62] Consequently, the Commission estimates that the majority of 800 and 800-Like Service Providers are small.

16. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[63] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[64] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[65] Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more.[66] Thus under this category and the

---

[56] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search

[57] *See* 13 CFR § 121.201, NAICS Code 517911.

[58] *Id.*

[59] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517911, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517911&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[60] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of establishments that meet the SBA size standard.

[61] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[62] *See id.*

[63] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite)",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517312&search=2017+NAICS+Search&search=2017.

[64] *See* 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

[65] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012.

[66] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

17. *Broadband Personal Communications Service.* The broadband personal communications services (PCS) spectrum is divided into six frequency blocks designated A through F, and the Commission has held auctions for each block. The Commission initially defined a "small business" for C- and F-Block licenses as an entity that has average gross revenues of $40 million or less in the three previous calendar years.[67] For F-Block licenses, an additional small business size standard for "very small business" was added and is defined as an entity that, together with its affiliates, has average gross revenues of not more than $15 million for the preceding three calendar years.[68] These small business size standards, in the context of broadband PCS auctions, have been approved by the SBA.[69] No small businesses within the SBA-approved small business size standards bid successfully for licenses in Blocks A and B. There were 90 winning bidders that claimed small business status in the first two C-Block auctions. A total of 93 bidders that claimed small business status won approximately 40 percent of the 1,479 licenses in the first auction for the D, E, and F Blocks.[70] On April 15, 1999, the Commission completed the reauction of 347 C-, D-, E-, and F-Block licenses in Auction No. 22.[71] Of the 57 winning bidders in that auction, 48 claimed small business status and won 277 licenses.

18. On January 26, 2001, the Commission completed the auction of 422 C and F Block Broadband PCS licenses in Auction No. 35. Of the 35 winning bidders in that auction, 29 claimed small business status.[72] Subsequent events concerning Auction 35, including judicial and agency determinations, resulted in a total of 163 C and F Block licenses being available for grant. On February 15, 2005, the Commission completed an auction of 242 C-, D-, E-, and F-Block licenses in Auction No. 58. Of the 24 winning bidders in that auction, 16 claimed small business status and won 156 licenses.[73] On May 21, 2007, the Commission completed an auction of 33 licenses in the A, C, and F Blocks in Auction No. 71.[74] Of the 12 winning bidders in that auction, five claimed small business status and won 18 licenses.[75] On August 20, 2008, the Commission completed the auction of 20 C-, D-, E-, and F-Block

---

[67] *See Amendment of Parts 20 and 24 of the Commission's Rules – Broadband PCS Competitive Bidding and the Commercial Mobile Radio Service Spectrum Cap; Amendment of the Commission's Cellular/PCS Cross-Ownership Rule*; WT Docket No. 96-59, GN Docket No. 90-314, Report and Order, 11 FCC Rcd 7824, 7850-52, paras. 57-60 (1996) (*PCS Report and Order*); *see also* 47 CFR § 24.720(b).

[68] *See PCS Report and Order*, 11 FCC Rcd at 7852, para. 60.

[69] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[70] *See D*, *E and F Block Auction Closes*, Public Notice, DA-97-81 (Jan. 15, 1997), 1997 WL 20711.

[71] *See C*, *D*, *E*, *and F Block Broadband PCS Auction Closes*, Public Notice, 14 FCC Rcd 6688 (WTB 1999). Before Auction No. 22, the Commission established a very small standard for the C Block to match the standard used for F Block. *Amendment of the Commission's Rules Regarding Installment Payment Financing for Personal Communications Services (PCS) Licensees*, WT Docket No. 97-82, Fourth Report and Order, 13 FCC Rcd 15743, 15768, para. 46 (1998).

[72] *See C and F Block Broadband PCS Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 2339 (2001).

[73] *See Broadband PCS Spectrum Auction Closes; Winning Bidders Announced for Auction No. 58*, Public Notice, 20 FCC Rcd 3703 (2005).

[74] *See Auction of Broadband PCS Spectrum Licenses Closes; Winning Bidders Announced for Auction No. 71*, Public Notice, 22 FCC Rcd 9247 (2007).

[75] *Id*.

Broadband PCS licenses in Auction No. 78.[76] Of the eight winning bidders for Broadband PCS licenses in that auction, six claimed small business status and won 14 licenses.[77]

19. *Advanced Wireless Services* (*AWS) - (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3)*). For the AWS-1 bands,[78] the Commission has defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. For AWS-2 and AWS-3, although we do not know for certain which entities are likely to apply for these frequencies, we note that the AWS-1 bands are comparable to those used for cellular service and personal communications service. The Commission has not yet adopted size standards for the AWS-2 or AWS-3 bands but proposes to treat both AWS-2 and AWS-3 similarly to broadband PCS service and AWS-1 service due to the comparable capital requirements and other factors, such as issues involved in relocating incumbents and developing markets, technologies, and services.[79]

20. *Specialized Mobile Radio Licenses.* The Commission awards "small entity" bidding credits in auctions for Specialized Mobile Radio (SMR) geographic area licenses in the 800 MHz and 900 MHz bands to firms that had revenues of no more than $15 million in each of the three previous calendar years.[80] The Commission awards "very small entity" bidding credits to firms that had revenues of no more than $3 million in each of the three previous calendar years.[81] The SBA has approved these small business size standards for the 900 MHz Service.[82] The Commission has held auctions for geographic area licenses in the 800 MHz and 900 MHz bands. The 900 MHz SMR auction began on December 5, 1995 and closed on April 15, 1996. Sixty bidders claiming that they qualified as small businesses under the $15 million size standard won 263 geographic area licenses in the 900 MHz SMR band. The 800 MHz SMR auction for the upper 200 channels began on October 28, 1997 and was completed on December 8, 1997. Ten bidders claiming that they qualified as small businesses under the $15 million size standard won 38 geographic area licenses for the upper 200 channels in the 800 MHz SMR band.[83] A second auction for the 800 MHz band conducted in 2002 and included 23 BEA licenses. One bidder claiming small business status won five licenses.[84]

---

[76] *See Auction of AWS-1 and Broadband PCS Licenses Closes; Winning Bidders Announced for Auction 78*, Public Notice, 23 FCC Rcd 12749 (WTB 2008).

[77] *Id.*

[78] The service is defined in section 90.1301 *et seq*. of the Commission's Rules, 47 CFR § 90.1301 *et seq*.

[79] *See Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Report and Order, 18 FCC Rcd 25162, Appx. B (2003), *modified by Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Order on Reconsideration, 20 FCC Rcd 14058, Appx. C (2005); *Service Rules for Advanced Wireless Services in the 1915–1920 MHz*, *1995–2000 MHz*, *2020–2025 MHz and 2175–2180 MHz Bands; Service Rules for Advanced Wireless Services in the 1.7 GHz and 2.1 GHz Bands*, Notice of Proposed Rulemaking, 19 FCC Rcd 19263, Appx. B (2005); *Service Rules for Advanced Wireless Services in the 2155–2175 MHz Band*, Notice of Proposed Rulemaking, 22 FCC Rcd 17035, Appx. (2007).

[80] 47 CFR § 90.814(b)(1).

[81] *Id*.

[82] *See* Letter from Aida Alvarez, Administrator, SBA, to Thomas Sugrue, Chief, Wireless Telecommunications Bureau, Federal Communications Commission (filed Aug. 10, 1999) (*Alvarez Letter 1999*).

[83] *See Correction to Public Notice DA 96-586 "FCC Announces Winning Bidders in the Auction of 1020 Licenses to Provide 900 MHz SMR in Major Trading Areas*,*"* Public Notice, 18 FCC Rcd 18367 (WTB 1996).

[84] *See Multi-Radio Service Auction Closes*, Public Notice, 17 FCC Rcd 1446 (WTB 2002).

21. The auction of the 1,053 800 MHz SMR geographic area licenses for the General Category channels was conducted in 2000. Eleven bidders won 108 geographic area licenses for the General Category channels in the 800 MHz SMR band and qualified as small businesses under the $15 million size standard.[85] In an auction completed in 2000, a total of 2,800 Economic Area licenses in the lower 80 channels of the 800 MHz SMR service were awarded.[86] Of the 22 winning bidders, 19 claimed small business status and won 129 licenses. Thus, combining all four auctions, 41 winning bidders for geographic licenses in the 800 MHz SMR band claimed status as small businesses.

22. In addition, there are numerous incumbent site-by-site SMR licenses and licensees with extended implementation authorizations in the 800 and 900 MHz bands. We do not know how many firms provide 800 MHz or 900 MHz geographic area SMR service pursuant to extended implementation authorizations, nor how many of these providers have annual revenues of no more than $15 million. One firm has over $15 million in revenues. In addition, we do not know how many of these firms have 1,500 or fewer employees, which is the SBA-determined size standard for Wireless Telecommunications Carriers (except Satellite).[87] We assume, for purposes of this analysis, that all of the remaining extended implementation authorizations are held by small entities, as defined by the SBA.

23. *Lower 700 MHz Band Licenses*. The Commission previously adopted criteria for defining three groups of small businesses for purposes of determining their eligibility for special provisions such as bidding credits.[88] The Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years.[89] A "very small business" is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years.[90] Additionally, the lower 700 MHz Service had a third category of small business status for Metropolitan/Rural Service Area (MSA/RSA) licenses—"entrepreneur"—which is defined as an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $3 million for the preceding three years.[91] The SBA approved these small size standards.[92] An auction of 740 licenses (one license in each of the 734 MSAs/RSAs and one license in each of the six Economic Area Groupings (EAGs)) commenced on August 27, 2002, and closed on September 18, 2002. Of the 740 licenses available for auction, 484 licenses were won by 102 winning bidders. Seventy-two of the winning bidders claimed small business, very small business or entrepreneur status and won a total of 329 licenses.[93] A second auction commenced on May 28, 2003, closed on June 13, 2003, and included 256 licenses: 5 EAG licenses and 476 Cellular Market Area licenses.[94] Seventeen winning bidders claimed small or very small business status and won 60 licenses, and nine winning bidders claimed entrepreneur status and won 154 licenses.[95] On July 26, 2005, the Commission

---

[85] *See 800 MHz Specialized Mobile Radio (SMR) Service General Category (851–854 MHz) and Upper Band (861–865 MHz) Auction Closes; Winning Bidders Announced*, Public Notice, 15 FCC Rcd 17162 (2000).

[86] *See 800 MHz SMR Service Lower 80 Channels Auction Closes; Winning Bidders Announced*, Public Notice, 16 FCC Rcd 1736 (2000).

[87] *See generally* 13 CFR § 121.201, NAICS Code 517312.

[88] *See Reallocation and Service Rules for the 698–746 MHz Spectrum Band (Television Channels 52–59)*, Report and Order, 17 FCC Rcd 1022 (2002) (*Channels 52–59 Report and Order*).

[89] *See id*. at 1087-88, para. 172.

[90] *See id*.

[91] *See id*. at 1088, para. 173.

[92] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (filed Dec. 2, 1998) (*Alvarez Letter 1998*).

[93] *See Lower 700 MHz Band Auction Closes*, Public Notice, 17 FCC Rcd 17272 (WTB 2002).

[94] *See id*.

completed an auction of 5 licenses in the Lower 700 MHz band (Auction No. 60). There were three winning bidders for five licenses. All three winning bidders claimed small business status.

24. In 2007, the Commission reexamined its rules governing the 700 MHz band in the *700 MHz Second Report and Order*.[96] An auction of 700 MHz licenses commenced January 24, 2008, and closed on March 18, 2008, which included: 176 Economic Area licenses in the A-Block, 734 Cellular Market Area licenses in the B-Block, and 176 EA licenses in the E-Block.[97] Twenty winning bidders, claiming small business status (those with attributable average annual gross revenues that exceed $15 million and do not exceed $40 million for the preceding three years) won 49 licenses. Thirty-three winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) won 325 licenses.

25. *Upper 700 MHz Band Licenses*. In the *700 MHz Second Report and Order*, the Commission revised its rules regarding Upper 700 MHz licenses.[98] On January 24, 2008, the Commission commenced Auction 73 in which several licenses in the Upper 700 MHz band were available for licensing: 12 Regional Economic Area Grouping licenses in the C Block, and one nationwide license in the D Block.[99] The auction concluded on March 18, 2008, with 3 winning bidders claiming very small business status (those with attributable average annual gross revenues that do not exceed $15 million for the preceding three years) and winning five licenses.

26. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[100] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules.[101] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[102] Of this total, 299 firms had annual

(Continued from previous page)

[95] *See id*.

[96] *Service Rules for the 698–746, 747–762 and 777–792 MHz Band; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; Section 68.4(a) of the Commission's Rules Governing Hearing Aid-Compatible Telephones; Biennial Regulatory Review—Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services; Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission's Rules; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010; Declaratory Ruling on Reporting Requirement under Commission's Part 1 Anti-Collusion Rule*, WT Docket Nos. 07-166, 06-169, 06-150, 03-264, and 96-86, PS Docket No. 06-229, CC Docket No. 94-102, Second Report and Order, 22 FCC Rcd 15289, 15359 n.434 (2007) (*700 MHz Second Report and Order*).

[97] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[98] *700 MHz Second Report and Order*, 22 FCC Rcd 15289.

[99] *See Auction of 700 MHz Band Licenses Closes*, Public Notice, 23 FCC Rcd 4572 (WTB 2008).

[100] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

[101] *See* 13 CFR § 121.201, NAICS Code 517410.

[102] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012.

receipts of less than $25 million.[103] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

27. *All Other Telecommunications.* The "All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[104] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[105] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[106] The SBA has developed a small business size standard for "All Other Telecommunications", which consists of all such firms with annual receipts of $35 million or less.[107] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[108] Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49, 999,999.[109] Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

28. *Other Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[110] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[111] The SBA has established a size standard for this industry as all such firms having 750 or fewer employees.[112] U.S. Census Bureau data for 2012 shows that 383 establishments operated in that year.[113] Of that number,

---

[103] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[104] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517919&search=2017+NAICS+Search&search=2017.

[105] *Id.*

[106] *Id*.

[107] *See* 13 CFR § 121.201, NAICS Code 517919.

[108] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[109] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[110] *See* U.S. Census Bureau, *2017 NAICS Definition, "334290 Other Communications Equipment Manufacturing*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334290&search=2017+NAICS+Search&search=2017.

[111] *Id.*

[112] *See* 13 CFR 121.201, NAICS Code 334290.

[113] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size*: *2012*, NAICS Code 334290, https://data.census.gov/cedsci/table?text=EC1231SG2&n=334290&tid=ECNSIZE2012.EC1231SG2&hidePreview=false&vintage=2012.

379 operated with fewer than 500 employees and 4 had 500 to 999 employees.[114] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

29. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[115] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[116] The SBA has established a small business size standard for this industry of 1,250 employees or less.[117] U.S. Census Bureau data for 2012 show that 841 establishments operated in this industry in that year.[118] Of that number, 828 establishments operated with fewer than 1,000 employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments operated with 2,500 or more employees.[119] Based on this data, we conclude that a majority of manufacturers in this industry are small.

30. *Engineering Services*. This industry comprises establishments primarily engaged in applying physical laws and principles of engineering in the design, development, and utilization of machines, materials, instruments, structures, process, and systems.[120] The assignments undertaken by these establishments may involve any of the following activities: provision of advice, preparation of feasibility studies, preparation of preliminary and final plans and designs, provision of technical services during the construction or installation phase, inspection and evaluation of engineering projects, and related services.[121] This category includes civil, environmental, construction and mechanical engineering services, and engineers' offices.[122]

31. The SBA has different small business size standards for different types of engineering services in this industry. For engineering firms except military and aerospace equipment and military weapons engineering, contracts and subcontracts for engineering services awarded under the National Energy Policy Act of 1992 and marine engineering and naval architecture are deemed small under the SBA standard if they have $16.5 million or less in annual receipts.[123] The SBA deems military and aerospace equipment and military weapons engineering, contracts and subcontracts for engineering

---

[114] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[115] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=334220&search=2017.

[116] *Id*.

[117] *See* 13 CFR § 121.201, NAICS Code 334220.

[118] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012*, NAICS Code 334220, https://data.census.gov/cedsci/table?text=EC1231SG2&n=334220&tid=ECNSIZE2012.EC1231SG2&hidePreview=false.

[119] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[120] *See* U.S. Census Bureau, *2017 NAICS Definition, "541330 Engineering Services*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=541330&search=2017+NAICS+Search&search=2017.

[121] *Id.*

[122] *Id.*

[123] *See* 13 CFR § 121.201, NAICS Code 541330.

services awarded under the National Energy Policy Act of 1992 and marine engineering and naval architecture firms small if they have annual receipts of $41.5 million or less.[124]

32. The U.S. Census Bureau includes engineering services under the SBA size standard of $16.5 million and $38 million under the same NAICS code.[125] According to 2012 U.S. Census Bureau data, there were 37,184 engineering services firms that operated for the entire year.[126] Of the 37,184 firms, 35,096 had less than $10 million in annual receipts, and 2,088 had $10 million or more in annual receipts.[127] Accordingly, the Commission estimates that a majority of engineering service firms are small.

33. *Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing.* This U.S. industry comprises establishments primarily engaged in manufacturing search, detection, navigation, guidance, aeronautical, and nautical systems and instruments. Examples of products made by these establishments are aircraft instruments (except engine), flight recorders, navigational instruments and systems, radar systems and equipment, and sonar systems and equipment.[128] The SBA has established a size standard for this industry of 1,250 or fewer employees.[129] U.S. Census Bureau data for 2012 show that 588 establishments operated in this industry for the entire year.[130] Of that number, 557 establishments operated with fewer than 1,000 employees, 21 establishments operated with between 1,000 and 2,499 employees and 10 establishments operated with 2,500 or more employees.[131] Based on this data, we conclude that a majority of manufacturers in this industry are small.

34. *Security Guards and Patrol Services*. This industry comprises establishments primarily engaged in providing guard and patrol services such as bodyguard, guard dog, and parking security services.[132] The SBA deems security guards and patrol services firms as small if they have $22 million or less in annual receipts.[133] According to U.S. Census Bureau data for 2012, there were 4,873 firms that operated for the entire year.[134] Of the 4,873 firms, 4,649 had less than $10 million in annual receipts

---

[124] *Id.*

[125] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1254SSSZ4, *Professional, Scientific, and Technical Services: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the U.S.: 2012,* NAICS Code 541330, https://data.census.gov/cedsci/table?y=2012&n=541330&tid=ECNSIZE2012.EC1254SSSZ4&hidePreview=false.

[126] *Id.*

[127] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[128] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*334511 Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334511&search=2017+NAICS+Search&search=2017.

[129] *See* 13 CFR § 121.201, NAICS Code 334511.

[130] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1231SG2, *Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012*, NAICS Code 334511, https://data.census.gov/cedsci/table?y=2012&n=334511&tid=ECNSIZE2012.EC1231SG2&hidePreview=false.

[131] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[132] *See* U.S. Census Bureau, *2017 NAICS Definition, "561612 Security Guards and Patrol Services",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561612&search=2017+NAICS+Search&search=2017.

[133] *See* 13 CFR § 121.201, NAICS Code 561612.

[134] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size:*

(continued….)

while 224 had more than $10 million in annual receipts.[135] Accordingly, the Commission estimates that a majority of firms in this category are small.

35. *All Other Support Services*. This industry comprises establishments primarily engaged in providing day-to-day business and other organizational support services (except office administrative services, facilities support services, employment services, business support services, travel arrangement and reservation services, security and investigation services, services to buildings and other structures, packaging and labeling services, and convention and trade show organizing services).[136] The SBA deems all other support services firms to be small if they have $12 million or less in annual receipts.[137] According to U.S. Census Bureau data for 2012, there were 9,742 firms in this industry in operation for the full year.[138] Of the 9,742 firms, 9,518 had less than $10 million while 224 had greater than $10 million in annual receipts.[139] Accordingly, the Commission estimates that a majority of firms in this category are small.

36. *Correctional Institutions (State and Federal Facilities)*. This industry comprises government establishments primarily engaged in managing and operating correctional institutions.[140] The facility is generally designed for the confinement, correction, and rehabilitation of adult and/or juvenile offenders sentenced by a court. The Department of Justice's Bureau of Justice Statistics (BJS) collects and publishes census information on adult correctional facilities operating under state or federal authority as well as private and local facilities operating under contract to house inmates for federal or state correctional authorities.[141] The types of facilities included in the census data from BJS are prisons and prison farms; prison hospitals; centers for medical treatment and psychiatric confinement; boot camps; centers for reception; diagnosis; classification; alcohol and drug treatment; community correctional facilities; facilities for parole violators and other persons returned to custody; institutions for youthful offenders; and institutions for geriatric inmates.[142]

37. While neither the SBA nor the Commission has developed a size standard for this category, the size standard for a small facility in the BJS census data is one that has an average daily population (ADP) of less than 500 inmates. The latest BJS census data available shows that as December 30, 2005 there were a total of 1821 correctional facilities operating under state or local federal authority.[143] Of that number more than half of the facilities or a total 946 facilities had an average daily

(Continued from previous page)
Summary Statistics by Receipts Size of Firms for the U.S.: 2012, NAICS Code 561612, https://data.census.gov/cedsci/table?y=2012&n=561612&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false.

[135] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[136] *See* U.S. Census Bureau, *2017 NAICS Definition, "561990 All Other Support Services"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561990&search=2017+NAICS+Search&search=2017.

[137] *See* 13 CFR § 121.201, NAICS Code 561990.

[138] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size: Summary Statistics by Receipts Size of Firms for the U.S.: 2012*, NAICS Code 561990, https://data.census.gov/cedsci/table?y=2012&n=561990&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false

[139] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[140] *See* U.S. Census Bureau, *2017 NAICS Definition, "922140 Correctional Institutions*," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=922140&search=2017+NAICS+Search&search=2017.

[141] *See* U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, Census of State and Federal Correctional Facilities, 2005 at 1. (Oct 2008), https://www.bjs.gov/content/pub/pdf/csfcf05.pdf.

[142] *Id.*

population of less than 500 inmates.[144] Based on this data a majority of "Governmental Correctional Institutions" potentially affected by the rules adopted can be considered small.

38. *Facilities Support Services*. This industry comprises establishments primarily engaged in providing operating staff to perform a combination of support services within a client's facilities.[145] Establishments in this industry typically provide a combination of services, such as janitorial, maintenance, trash disposal, guard and security, mail routing, reception, laundry, and related services to support operations within facilities. These establishments provide operating staff to carry out these support activities but are not involved with or responsible for the core business or activities of the client. Establishments providing facilities (except computer and/or data processing) operation support services and establishments providing private jail services or operating correctional facilities (i.e., jails) on a contract or fee basis are included in this industry. The SBA small business size standard for this category classifies all such entities having $41.5 million or less in annual receipts as small.[146] According to U.S. Census Bureau data for 2012, there were 1,669 firms in this category that operated for the entire year.[147] Of this number 1,549 firms had annual receipts of less than $25 million, and 60 firms had annual receipts between $25,000,000 and $49,999,999.[148] Based on this information, the majority of firms in this category can be considered small under the SBA small business size standard.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

39. In the *Second Further Notice*, the Commission seeks comment on whether there have been technological, economic, policy, and/or legal developments sufficient to overcome the variety of challenges presented to the widespread deployment of these technologies and whether and how the Commission can further facilitate these technologies through regulatory next steps. In doing so, the Commission contemplates various approaches to combatting the use of contraband wireless devices in correctional facilities that would each have their own projected reporting, recordkeeping, and other compliance requirements. We cannot quantify the cost of compliance with any regulatory next steps and do not know whether small entities will have to hire professionals to comply with any rules that we ultimately adopt. Below we discuss the projected reporting, recordkeeping, and other compliance requirements associated with the various approaches in the *Second Further Notice* to combat contraband wireless device use in correctional facilities.

(Continued from previous page)

[143] *Id.* Appendix table 3. "Number of correctional facilities under state or federal authority, by size, June 30, 2000, and December 30, 2005." This data excludes city, county, and regional jails and private facilities that did not house primarily state or federal inmates. It also excluded facilities for the military, U.S. Immigration and Customs Enforcement (ICE), Bureau of Indian Affairs (BIA), U.S. Marshals Service (USMS), and correctional hospital wards not operated by correctional authorities.

[144] *Id.*

[145] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*561210 Facilities Support Services",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=561210&search=2017+NAICS+Search&search=2017.

[146] *See* 13 CFR § 121.201, NAICS Code 561210.

[147] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1256SSSZ4, *Administrative and Support and Waste Management and Remediation Services: Subject Series - Establishment and Firm Size: Summary Statistics by Receipts Size of Firms for the U.S.: 2012*, NAICS Code 561210, https://data.census.gov/cedsci/table?y=2012&n=561210&tid=ECNSIZE2012.EC1256SSSZ4&hidePreview=false.

[148] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

40. The Commission contemplates as a potential solution the creation of "quiet zones" in and around correctional facilities where wireless communications are not authorized such that contraband wireless devices in correctional facilities would not be able to receive service from a wireless provider. Quiet zones would require wireless carriers and solution providers to have appropriate engineering capabilities to precisely define quiet zones around the borders of correctional facilities. To understand the cost implications for small and other entities, we seek comment on the potential costs that could be associated with the implementation of quiet zones, including the cost of hardware, software, network integration, engineering, and ongoing maintenance. The Commission also seeks comment on who should bear the cost of implementing quiet zones, and the potential alternatives to a Commission mandate that might encourage implementation.

41. The *Second Further Notice* seeks comments on the options of geolocation-based denial, also known as geofencing, and a "network-based solution." The geolocation-based denial would allow for mobile device software and/or hardware to be used to shut down contraband wireless devices that violate a perimeter surrounding a correctional facility. A geolocation-based solution would require adequate engineering to locate and disable wireless contraband. Relatedly, a "network-based solution" would require CMRS licensees to independently identify and disable contraband wireless devices in correctional facilities using their own network elements. Therefore, the Commission seeks comment on whether there have been technological advancements in carriers' network engineering that might make it more feasible for entities to implement and comply with network-based geofencing. If network-based geofencing is selected as the solution for contraband wireless devices in correctional facilities, then the engineering required could have associated costs, including the testing and maintenance necessary to ensure accuracy and ongoing viability. The Commission's request for comment on additional costs that could be associated with the implementation of network-based geofencing, including software and network integration, should provide insight and allow us to evaluate costs for small and other entities that will be impacted by any future rules we adopt regarding these two potential solutions.

42. Today's *Second Further Notice* also contemplates the option of using beacon technology to combat the issue of contraband wireless device use in correctional facilities. The Commission seeks comment on the potential advancements in beacon technology that would allow beacon software to be installed on mobile devices remotely (e.g., through a software update). If the Commission is found to have the authority to require entities to install the software on devices, then this approach could require related compliance requirements. Relatedly, the Commission seeks comment on how beacon technology could ensure that authorized users (e.g., correctional officers) are still able to use their devices. This requirement could impose recordkeeping and compliance requirements for entities such as wireless providers and mobile device manufacturers that must implement beacon technology via hardware and/or software changes to mobile devices for all users. We raise inquiries and seek information on the cost and implementation timing for beacon technology, specifically as compared to MAS or advanced detection, and who should bear these costs. In addition, we request information on the various types of costs for entities associated with this type of technology, including hardware, software, network integration, engineering, ongoing maintenance, etc., which is germane to our analysis of any regulatory next steps and could impact the nature and type of recordkeeping, reporting, and compliance obligations that may result in this proceeding.

43. The Commission also seeks further comment on potential regulatory steps that might be necessary to ensure that MAS maintains effectiveness as wireless technology evolves from 2G to widespread 3G/4G and ultimately 5G deployments. We note that the commenters on the *July 2020 Refresh PN* largely agree that MAS Evolved will be even more effective than existing MAS systems. In today's *Second Further Notice*, we seek further comment on steps the Commission could take to facilitate MAS deployments. Depending on the comments, it is possible that the Commission could mandate roaming agreements between wireless carriers and solutions providers in the corrections context given the vital public safety concerns, which would impact small entities. It is also possible that the Commission could implement other approaches that could be developed by the wireless providers and/or the vendors to add features or services and help defray the cost of MAS deployments and operations. Lastly, the

Commission could revise the previously streamlined leasing rules in the correctional facility context to facilitate further CIS deployments nationwide. Each of these potential rule changes could require additional recordkeeping and reporting from entities that seek to deploy MAS Evolved solutions.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

44. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof for small entities."[149]

45. The *Second Further Notice* considers a number of potential solutions to address the issue of contraband wireless devices in correctional facilities that might create additional compliance costs for small and other entities. Specifically, the Commission invites comment on quiet zones, geolocation-based denial and carrier network-based solutions, beacon technology, and MAS Evolved deployments. To understand the economic impact for small and other entities, for each of the alternatives, the Commission requests comments regarding potential technological advancements that might increase the viability of the solution. Commenters are also asked to provide their input on a range of necessary costs—e.g., hardware, software, network integration, engineering, ongoing maintenance—and the costs associated with deployment of each solution, particularly in relation to MAS or advanced detection. For quiet zones, geolocation-based denial (geofencing), carrier network-based solutions, and beacon technology, the Commission requests comment on whether these or similar solutions currently exist in the marketplace, and if so, who is using them and where and in what context are the solutions being used. For the MAS Evolved solution, the Commission invites comment on potential approaches that could be developed by the wireless providers and/or vendors to add features or services and help defray the cost of MAS deployments and operations. Through these comments, the Commission seeks to develop final rules that combat the exigent public safety concerns of contraband phone use in correctional facilities, while also minimizing economic and other compliance burdens on small and other entities to the greatest extent possible.

46. In order to clarify and simplify compliance and reporting requirements for impacted small and other entities the *Second Further Notice* invites comment regarding the prospective needs of entities and the various approaches that can be taken to accommodate those needs. For example, for the geolocation-based denial and carrier network-based solutions, the Commission asks about: (1) the specific engineering steps that wireless providers would need to take to implement such a solution, including the necessary and maintenance necessary to ensure its accuracy and ongoing viability, (2) the degree of accuracy that wireless providers could define geofencing around the precise perimeter of a correctional facility, (3) the information that wireless carriers would need in order to account for continued authorized use, and the necessary information to be shared, and (4) the criteria that might indicate a device is contraband. Similarly, for the MAS Evolved solution, the Commission seeks comment on steps that the Commission could take to facilitate MAS deployments. The Commission, for example, specifically asks commenters: (1) whether it should mandate roaming agreements between wireless carriers and solutions providers in the corrections context; (2) how roaming agreement negotiations can be expedited; and (3) whether the Commission should revise previously streamlined leasing rules in the correctional facility context to facilitate further CIS deployments. In doing so, the Commission invites small and other entities to help inform on any necessary clarifications and/or simplification of compliance and reporting requirements that should be incorporated in the final rules.

[149] 5 U.S.C. § 603(c)(1)-(4).

Receiving input from small entities will allow the Commission to the extent feasible, to better consider options that could minimize the impact for these entities.

47. The Commission does not seek comment on any particular performance standards for the potential solutions discussed in the *Second Further Notice* to eliminate the use of contraband wireless devices in correctional facilities. Instead, the Commission allows small and other entities to provide relevant information on whether there have been technological, economic, policy, and/or legal developments sufficient to overcome the variety of challenges presented to the widespread deployment of various technologies to combat wireless contraband in correctional facilities, and whether and how the Commission can further facilitate the use of these technologies through regulatory next steps. Such information may provide insight on whether and what type of, if any, performance standards or regulatory measures need to be adopted and the costs of such standards or measures.

48. Finally, the Commission finds an overriding public interest in preventing the illicit use of contraband wireless devices by incarcerated people to perpetuate criminal enterprises and therefore does not propose any exemptions for small entities from the potential solutions discussed in the *Second Further Notice*. If small entities were to be exempted from the selected approach, it is likely that the overall effectiveness of the solution would be reduced which is not consistent with, and is contrary to, the Commission's overarching goal of eliminating the use of contraband wireless devices in correctional facilities. Small and other entities have the opportunity to provide comments on technological, economic, policy, and/or legal developments sufficient to overcome the potential challenges presented by widespread deployment of the various options discussed in the *Second Further Notice* to combat wireless contraband use in correctional facilities. Importantly, this gives small entities the ability to submit comments on economic and other challenges they may face with the potential solutions that have been discussed, and the opportunity to suggest other alternatives for the Commission to consider in any final rules that we may adopt.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

49. None.

APPENDIX D

List of Commenters

Contraband FNPRM Comments

American Correctional Association (ACA)
Arizona Department of Corrections (ADOC)
Association of State Correctional Administrators (ASCA)
AT&T Services, Inc. (AT&T)
CellBlox Acquisitions, LLC (CellBlox)
Cell Command, Inc. (formerly Try Safety First, Inc.) (Cell Command)
CoreCivic
CTIA – The Wireless Association (CTIA)
Florida Department of Corrections (FDOC)
Global Tel*Link Corporation (GTL)
Human Rights Defense Center (HRDC)
Inpixon USA
Prelude Communications (Prelude)
Screened Images, Inc. (d/b/a Corrections.com) (Corrections.com)
ShawnTech Communications, Inc. (ShawnTech)
Tennessee Department of Correction (TDOC)
T-Mobile USA, Inc. (T-Mobile)
Verizon Wireless (Verizon)

Contraband FNPRM Reply Comments

AT&T Services, Inc. (AT&T)
CellAntenna Corporation (CellAntenna)
Cell Command, Inc. (formerly Try Safety First, Inc.) (Cell Command)
CenturyLink Public Communications, Inc. (CenturyLink)
Corizon Health
CTIA – The Wireless Association (CTIA)
Global Tel*Link Corporation (GTL)
Human Rights Defense Center (HRDC)
Inpixon USA
T-Mobile USA, Inc. (T-Mobile)

July 28, 2020 PN Comments

AT&T Services, Inc. (AT&T)
Association of Public-Safety Communications Officials-International, Inc. (APCO)
CellBlox Acquisitions, LLC (CellBlox)
Correctional Leaders Association (CLA)
CTIA – The Wireless Association (CTIA)
Global Tel*Link Corporation (GTL)
National Public Safety Telecommunications Council (NPSTC)
OmniProphis Corporation (OmniProphis)
Senator James Lankford, Senator Tom Cotton, Senator John Kennedy, Senator David Perdue, Senator Thom Tillis, Senator Kelly Loeffler, Senator John Boozman (Senators' Letter)
ShawnTech Communications, Inc. (ShawnTech)

T-Mobile USA, Inc. (T-Mobile)
Verizon Wireless (Verizon)

July 28, 2020 PN Reply Comments

AT&T Services, Inc. (AT&T)
Correctional Leaders Association (CLA)
CTIA – The Wireless Association (CTIA)
T-Mobile USA, Inc. (T-Mobile)

STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111

Imagine receiving a threatening call. You are told to pay up and if you don't, someone in your family will get hurt . . . or worse. These are the kinds of calls that were made to the parents of Ryan Rust, when he was incarcerated in Alabama. As *The New York Times* described the situation last year, the demands began with small dollar amounts and escalated quickly. They were told that failure to respond would lead to torture and eventually death. The calls became so frequent and the threats so outrageous, the family feared for their safety.

But the Rust story is hardly unique. That's because these kinds of blackmail schemes are happening in prisons and jails across the country. They often start when one inmate realizes that another has someone on the outside depositing money into their commissary account to buy things like toothpaste or deodorant. Sometimes they begin when an inmate falls into debt to another, with interest rates that compound exponentially. Regardless of how they get going, the result is the same. The incarcerated person is threatened or beaten into turning over information about potential extortion targets on the outside—names, phone numbers, home addresses, places of work—and then the calls begin. They take place at all hours of day and night. Families fearing for the safety of their incarcerated kin often pay up and then find the threats rachet up along with the fear that their loved ones may pay with their lives.

To make these schemes work requires one thing: contraband cell phones. They are smuggled in by inmates, taken from employees, thrown over walls, and even flown in by drone. Combatting their availability and use is a serious challenge for corrections department officials. Because despite efforts to identify and confiscate contraband phones, with everything from cell searches to phone-sniffing dogs, these devices still make their way in, making it possible for these extortion schemes to take place.

The action we take today is designed to help them stop. It sets up a streamlined system for corrections department officials to use certified contraband interdiction systems to identify where contraband phones may be in use and request that wireless carriers have them deactivated. This builds on previous FCC efforts and responds to the explanatory statement in last year's appropriations legislation directing us to adopt rules to require wireless carriers to disable contraband devices upon proper identification.

But we're not stopping here. That's because we're also seeking comment on further updates to our rules and the potential for other systems to help us combat the proliferation of contraband phones, to the extent they are permitted under the Communications Act of 1934.

Addressing this problem is not easy. The incentive to bring these devices into prisons and jails will not simply go away with better contraband interdiction systems in place. These underlying problems need to be addressed. However, we will continue to update our policies, consistent with the law, to help stop the kind of abuse the Rust family faced and help this troubling extortion come to an end.