September 9, 2025

FCC FACT SHEET*
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities
Third Further Notice of Proposed Rulemaking – GN Docket No. 13-111

Background: The problem of contraband wireless device use in correctional facilities has been a persistent public safety issue for decades, and corrections officials continue to seek authority to leverage additional tools to combat their use. In this Third FNPRM, the Commission seeks to build a record on a proposed regulatory framework to authorize, for the first time, non-federal operation of radio frequency jamming solutions in the limited context of correctional facilities, thereby expanding the scope of technical options available to corrections officials facing this threat.

What the Third Further Notice of Proposed Rulemaking Would Do:

- Propose to deauthorize, for purposes of Commission licensing, operation of contraband wireless devices in correctional facilities, paving the way for the deployment of jamming solutions to combat contraband device use in a way that complies with section 333 of the Act's prohibition against willful or malicious interference to authorized stations.
- Propose to leverage the Commission's existing leasing process as a preferred approach to licensing jamming solutions and seek comment on restrictions that may be necessary to ensure that jamming solutions are limited to the correctional facility context, including a stricter regulatory framework from a technical perspective.
- Seek comment on the possible effects of the deployment of jamming solutions in correctional facilities on wireless emergency/911 calls and public safety communications.
- Propose a requirement that wireless providers engage in good faith lease negotiations with entities seeking to deploy a jamming solution in a correctional facility, but in the absence of a good faith agreement, as a method of last resort, the department of corrections/solutions provider would be eligible to apply for a non-exclusive overlay license.
- Seek comment, with respect to the proposed overlay licensing mechanism, on the technical requirements that should apply as well as how the proposal might impact non-contraband devices.
- Propose to require entities seeking to deploy a jamming solution in a correctional facility to comply with existing equipment authorization procedures for certification and prohibit certification for equipment used under our unlicensed rules. Seek comment on whether additional procedures or rule changes are required for the equipment authorization process or the Commission's marketing, importation, or labeling procedures.
- Ask questions about other technological solutions to combat contraband wireless device use in correctional facilities, whether the Commission should take regulatory steps to support their development and deployment, and on further facilitating and streamlining the authorization of current contraband interdiction system technology.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in GN Docket No. 13-111, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs/). Before filing, participants should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq*.

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

THIRD FURTHER NOTICE OF PROPOSED RULEMAKING*

Adopted: [] **Released: []**

Comment Date: [30 days after date of publication in the Federal Register]
Reply Comment Date: [45 days after date of publication in the Federal Register]

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 3
A. Commission Action on Contraband Wireless Devices in Correctional Facilities 5
B. Current Status of Contraband Interdiction System Deployment 12
C. Current Status of RF Jamming Solutions 13
III. THIRD FURTHER NOTICE OF PROPOSED RULEMAKING 18
A. Definition of Jamming Solution 20
B. Deauthorizing Subscriber Operation of Contraband Wireless Devices 23
1. Subscriber Authority Rule 24
2. Section 316 License Modification 30
3. Safe Harbor to Proposed Deauthorization Rule 31
C. Facilitating the Authorization of Jamming Solutions Under Section 301 35
1. Authorization of Jamming Solutions 36
a. Spectrum Leasing 36
b. Non-Exclusive Overlay Licensing 72
(i) Overlay Licensing and Operating Rules 77

* This document has been circulated for tentative consideration by the Commission at its September 30, 2025 open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chair has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's *ex parte* rules apply and presentations are subject to "permit-but-disclose" *ex parte* rules. *See, e.g.*, 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

(ii) Technical Parameters for Overlay Licenses 89
(iii) Application Process and Procedures 104
2. Authorizing Jamming Solutions on Other Spectrum 109
a. Unlicensed Operations Under Part 15 110
b. Part 25 Spectrum 119
3. Transmitters Used to Enable Jamming Solutions 120
a. Part 2 Equipment Authorization 120
b. Marketing, Labeling, and Importation of Equipment Used for Jamming Solutions 125
D. Facilitating Other Handset-Centric Technologies 130
E. Further Facilitating and Streamlining the Authorization of Current CIS Technology 135
F. Other Technological Solutions 140
G. Costs and Benefits 141
IV. PROCEDURAL MATTERS 142
V. ORDERING CLAUSES 150
APPENDIX A: PROPOSED RULES
APPENDIX B: INITIAL REGULATORY FLEXIBILITY ANALYSIS

I. INTRODUCTION

1. Correctional facilities in the United States continue to be plagued by an influx of contraband wireless devices that threaten the safety of prison officials and employees, the prison population, and members of the general public. Across the country, inmates have reportedly used these devices to orchestrate criminal activity, including murder, assault, witness intimidation, illegal drug operations, phone scams, and prison escapes. Congressional leaders, in particular Senator Tom Cotton of Arkansas and Representative David Kustoff of Tennessee, have successfully brought national attention to these real threats to public safety, introducing key legislation to facilitate deployment of new technologies to combat this problem. Despite these significant efforts, and the implementation of currently approved technologies to combat the use of these devices, corrections officials in a substantial number of states continue to seek authority to leverage additional tools in this ongoing effort.

2. The Commission's goal in this *Third Further Notice of Proposed Rulemaking* (*Third Further Notice*) is to enhance public safety by removing regulatory barriers to the deployment and viability of existing and developing technologies that combat contraband wireless device use in correctional facilities. Today, we build upon prior Commission actions by seeking comment on a proposed framework consistent with applicable Congressional statutes to authorize, for the first time, non-federal operation of radio frequency (RF) jamming solutions in correctional facilities, expanding the scope of technical options available to corrections officials facing this threat. Through this approach, we seek to foster a collaborative environment among key stakeholders, including departments of correction, solutions providers, wireless providers, public safety and 911 entities, to explore an expanded range of solutions to a shared problem that has remained exceptionally challenging and complex over time.

II. BACKGROUND

3. The use of contraband wireless devices, primarily cell phones, by inmates in correctional facilities to engage in criminal activities has been a persistent problem for decades.[1] This threat to public safety prompted action by Congress and state legislatures to restrict wireless devices in correctional facilities, establishing penalties for their unauthorized use or possession and for attempts to bring such devices into correctional facilities. For example, in 2010, Congress passed the Cell Phone Contraband

[1] *See, e.g.,* U.S. Government Accountability Office, Report to Congressional Committees, Bureau of Prisons: Improved Evaluations and Increased Coordination Could Improve Cell Phone Detection, GAO-11-893 at 23-24 (2011), https://www.gao.gov/assets/gao-11-893.pdf; U.S. Department of Commerce, National Telecommunications and Information Administration, Contraband Cell Phones in Prisons: Possible Wireless Technology Solutions at 3 (2010), https://www.ntia.gov/sites/default/files/publications/contrabandcellphonereport_december2010_0.pdf.

Act, which prohibits the possession of cell phones in federal prisons by unauthorized persons.[2] All 50 states, along with the District of Columbia and U.S. territories,[3] have enacted laws or promulgated regulations designating as contraband wireless devices in correctional facilities, thereby restricting their possession and operation.[4] A substantial majority of states impose criminal penalties, while others have opted to rely on administrative sanctions for these types of prison violations.[5]

4. Despite these measures, state corrections officials continue to highlight contraband wireless devices as a public safety crisis and advocate for additional ways to combat the evolving methods of smuggling wireless devices into correctional facilities,[6] which increasingly include delivery by drones.[7] One study of 20 state correctional administrators indicates that prison authorities recovered more than 25,000 cell phones in their facilities in 2020.[8] Beyond the record developed in this proceeding, recent news articles and reports continue to highlight the myriad creative ways that contraband wireless devices are smuggled into correctional facilities and then used in many cases to perpetrate crimes.[9]

---

[2] Cell Phone Contraband Act of 2010, Pub. L. No. 111-225 (2010) (amending 18 U.S.C. § 1791) (Cell Phone Contraband Act).

[3] In this *Third Further Notice*, any reference to "state" includes the District of Columbia and any territories and possessions of the United States.

[4] *See* Andrew W. Eichner, *A Cross-Jurisdictional Analysis of Penalties for Possession of Contraband Phones by Inmates and a Proposal to Increase the Federal Penalty*, 38 Touro L. Rev 1169 (2023), https://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=3420&context=lawreview.

[5] *See, e.g.*, Ala. Code §§ 14-11-50, 14-11-51 (violation of prohibition is a Class C felony); Ark. Code Ann § 5-54-119(c) (possession of a prohibited cellular telephone or other communication device is a Class B felony); Fla. Stat. Ann. § 944.47(1)(a)(6), (2)(a) (violation of prohibition is a third-degree felony); Ga. Code Ann. § 42-5-18(c), (d)(1) (felony for an inmate to possess a telecommunications device); S.C. Code Ann. § 24-3-980 (violation of prohibition results in a misdemeanor for first offense and felony for second or subsequent offense). *Compare*, *e.g.*, 103 Code of Mass. Reg. §§ 430.24 2-31, 430.25 (possession of cell phone or unauthorized electronic device is Category 2 offense, which may result in administrative penalties, such as disciplinary detention for up to 15 days, loss of privilege, etc.); Cal Penal Code § 4576(c) (providing that an inmate found to be possession of a wireless communication device shall be subject to credit denial or loss of up to 90 days); Minn. Dep't of Corr. Pol'y 303.010 (Jan. 5, 2021), https://policy.doc.mn.gov/DOCPolicy/ (providing the policy for punishing inmates found with contraband).

[6] *See infra* note 50.

[7] *See, e.g.*, Dix, M. O., Mecray, M., Man, J., Vetter, E., Tucker, M., Parsons, N. Craig, T., and Criminal Justice Testing and Evaluation Consortium, National Institute of Justice, *Contraband and Drones in Correctional Facilities*, RTI International (2022), https://cjttec.org/files/65532e9a1817a (finding that the evolution of drone technology enables drone operators to carry larger payloads and operate at lower levels of investment); Press Release, United States Attorney's Office, District of New Jersey, *Second Former Inmate Admits Role in Scheme to Use Drones to Smuggle Contraband into Fort Dix Federal Prison* (Jan. 10, 2022), https://www.justice.gov/usao-nj/pr/second-former-inmate-admits-role-scheme-use-drones-smuggle-contraband-fort-dix-federal; Harrison Keegan, Springfield News-Leader, *Man used drone to fly cell phones into Springfield's Fed Med, prosecutors say* (Mar. 2, 2023), https://www.news-leader.com/story/news/crime/2023/03/02/oklahoma-man-accused-of-flying-drone-dropping-cell-phones-at-fed-med/69957987007/ (man accused of using a drone to drop cell phones into a federal prison).

[8] *See* Sarah Aukamp, *Tackling Contraband Cell Phones in State Departments of Corrections* (July 1, 2024), https://www.urban.org/urban-wire/tackling-contraband-cell-phones-state-departments-corrections. The study was conducted by the Urban Institute and their partners, CAN Corporation, Correctional Leaders Association, the American Correctional Association, and criminal justice consultants John Shafer and Joe Russo.

[9] *See, e.g.*, State Grand Jury of South Carolina, *Report of the Thirty-Fourth State Grand Jury on Organized Crime and the Use of Cell Phones Within the South Carolina Department of Corrections* at 1-2 (2025), https://www.scag.gov/media/12fhnnym/filed-sgj-report-34th-paper-route-6-3-25.pdf, State Grand Jury of South Carolina, *Report of the Thirty-Fifth State Grand Jury on Organized Crime and the Use of Cell Phones Within the South Carolina Department of Corrections* at 1-2 (2025), https://www.scag.gov/media/bnxfzekj/filed-sgj-report-

(continued….)

A. Commission Action on Contraband Wireless Devices in Correctional Facilities

5. The Commission has taken numerous steps to aid departments of correction (DOCs) by facilitating and authorizing tools, specifically contraband interdiction systems (CISs), to combat contraband wireless device use. CISs are designed exclusively to prevent transmissions to or from contraband wireless devices within the boundaries of a correctional facility and/or to obtain identifying information from such devices.[10] Common types of current CISs include managed access systems (MAS),[11] MAS Evolved (E-MAS),[12] and detection systems.[13]

6. The Commission, in its 2013 *Contraband NPRM*, detailed its prior extensive efforts to engage with stakeholders and facilitate state correctional officials' abilities to address the public safety issue of contraband device use.[14] At that time, only a small number of states were testing or deploying MAS solutions, but wireless providers and MAS solutions providers relying on the Commission's

(Continued from previous page)
35th-clean-sweep-6-5-25.pdf (together, SC Jury Reports) (finding that inmates in the South Carolina DOC system engage in scams using cell phones to prey upon law-abiding citizens, often elderly, and that illegal cell phones are the "principal tool inmates use to manage all phases of their operations."); Press Release, United States Attorney's Office, Middle District of Tennessee, *More than Two Dozen Sentenced in Connection with Prison-Based Drug Ring* (Mar. 26, 2025), https://www.justice.gov/usao-mdtn/pr/more-two-dozen-sentenced-connection-prison-based-drug-ring (drug and money laundering conspiracy operated by incarcerated persons with phones smuggled into Tennessee prisons); Press Release, United States Department of Justice, *Final Defendant Sentenced in South Carolina's Largest RICO Conspiracy* (Aug. 1, 2023), https://www.justice.gov/archives/opa/pr/final-defendant-sentenced-south-carolinas-largest-rico-conspiracy (inmates ran an international drug trafficking enterprise in prison using cell phones to orchestrate murders, kidnappings, gun trafficking, and an international drug operation).

[10] *See* 47 CFR § 1.9003 (defining CIS as "a 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 to obtain identifying information from such contraband wireless devices").

[11] A MAS is a micro-cellular, private network that typically operates on spectrum already licensed to wireless providers offering commercial subscriber services in geographic areas that include a correctional facility. A MAS utilizes base stations that are optimized to capture and analyze all voice, text, and data communications to and from a wireless device within the system coverage area to determine if the communications are authorized or unauthorized by the correctional facility for purposes of accessing wireless carrier networks. When a wireless device attempts to connect to the network from within the coverage area of the MAS, the system cross-checks the identifying information of the device against a database that lists wireless devices authorized to operate in the coverage area. Authorized or "white-listed" devices are allowed to communicate (i.e., transmit and receive voice, text, and data) with the commercial wireless network, while transmissions to or from unauthorized devices are terminated.

[12] MAS Evolved systems are MAS systems that are designed to work with wireless networks that use advanced 4G and 5G technologies. A MAS Evolved system becomes a roaming partner with the carrier network it monitors and does not permit contraband devices to authenticate on that network, in the same manner a wireless provider addresses non-subscribers. These systems can be easily upgraded as wireless service providers add new technologies and frequency bands.

[13] Detection systems are used to detect devices within a correctional facility by locating, tracking, and identifying radio signals originating from a device. Some detection systems use passive, receive-only technologies that do not transmit radio signals and do not require separate Commission authorization. However, detection systems have evolved with the capability of transmitting radio signals to not only locate a wireless device, but also to obtain device identifying information. These types of advanced transmitting detection systems also operate on frequencies licensed to wireless providers and require separate Commission authorization, also typically through the filing of part 1 spectrum leasing notifications/applications reflecting wireless provider agreement.

[14] *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, 6608-09, paras. 7-9 (2013) (*Contraband NPRM*).

spectrum leasing process faced challenges and transaction costs involved in MAS deployment.[15] In seeking comment on other technological solutions besides MAS, the Commission specifically invited commenters to discuss whether there was a statutory bar that precluded the use of the technology or rendered it infeasible, "most significantly Section 333's sweeping prohibition against interference…."[16]

7. In 2017, the Commission released the *Contraband First R&O* to streamline the process of deploying CISs to thwart contraband wireless device use in correctional facilities.[17] Specifically, the Commission eliminated certain filing and regulatory requirements and provided for immediate approval of the part 1 leasing applications/notifications filed to authorize operation of these systems.[18] In addition, the *Contraband First R&O* provided for community notice of CIS deployment, required good faith lease negotiations between wireless providers and CIS solutions providers, and addressed enhanced 911 (E911) issues.[19] In the *Contraband First FNPRM*, the Commission sought additional comment on a broad range of steps it could take to help eliminate the threat to public safety caused by contraband wireless device use in correctional facilities, on additional methods and technologies that might prove successful in combating such use, and on various other proposals related to the authorization process for CISs and the deployment of these systems.[20]

8. In 2020, the Wireless Telecommunications Bureau (Bureau) issued the *Contraband Refresh PN* to refresh the record on the proposals and questions raised in the *Contraband First FNPRM*.[21] In particular, the Bureau sought comment on a process for disabling contraband wireless devices once identified and invited comment on existing and future technological solutions that could be used to address this issue.[22] The Bureau recognized that a substantial number of state corrections officials advocated for a "jamming" solution or its equivalent, and sought comment on ways in which the Commission could authorize jamming solutions in correctional facilities.[23] Throughout this proceeding, the wireless industry expressed concern regarding the deployment of jamming solutions in correctional facilities, not only from a legal perspective, but from a policy standpoint. Specifically, large wireless providers argued that jamming systems are indiscriminate, potentially interfering with legitimate wireless devices inside the prisons and in the surrounding areas, including emergency communications.[24] The

[15] *Id.* at 6611-13, paras. 14-15; 6617-18, paras. 26-27.

[16] *Id.* at 6636, para. 77.

[17] *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) (*Contraband First R&O and Contraband First FNPRM*, respectively).

[18] *Contraband First R&O*, 32 FCC Rcd at 2337, para. 1.

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

[20] *Contraband First FNPRM*, 32 FCC Rcd at 2337, para. 2.

[21] *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) (*Contraband Refresh PN*).

[22] *See id.* at 7910-13.

[23] *Id.* at 7913-14.

[24] *See, e.g.,* CTIA Reply Comments, GN Docket No. 13-111, at 8 (rec. July 14, 2017) (CTIA 2017 Reply Comments); CTIA Comments, GN Docket No. 13-111, at 13-14 (rec. Sept. 16, 2020) (CTIA 2020 Comments); CTIA Reply Comments, GN Docket No. 13-111, at 14-15 (rec. Oct. 1, 2020) (CTIA 2020 Reply Comments); T-Mobile Reply Comments, GN Docket No. 13-111, at 6 (rec. July 17, 2017) (T-Mobile 2017 Reply Comments); T-Mobile Comments, GN Docket No. 13-111, at 17-18 (rec. Sept. 16, 2020) (T-Mobile 2020 Comments); AT&T Reply Comments, GN Docket No. 13-111, at 21-24 (rec. July 17, 2017) (AT&T 2017 Reply Comments); AT&T Reply Comments, GN Dockets No. 13-111, at 11-13 (rec. Oct. 1, 2020) (AT&T 2020 Reply Comments).

wireless providers also contended that, done properly, jamming would be as costly as MAS.[25] On the issue of containing harmful interference, the Bureau sought comment in the *Contraband Refresh PN* on whether there was "potential for wireless providers to voluntarily deploy base stations in the vicinity of a correctional facility that would, in effect, result in the blocking of their own signals in all or part of a correctional facility, thereby not resulting in a violation of section 333."[26] The wireless industry opposed the concept of Commission-mandated self-jamming for both legal and policy reasons.[27]

9. Public safety stakeholders also noted the potential for wireless jammers to interfere unintentionally with public safety communications in and around correctional facilities.[28] As NPSTC explained, "[p]ublic safety communications often operate in frequency bands that are adjacent to band segments licensed to commercial wireless carriers. Under Part 90 of the Commission's rules, dedicated segments of the 700 MHz and 800 MHz bands are licensed to state and local jurisdictions for the operation of public safety communications systems."[29] NPSTC also observed that "FirstNet operates the Nationwide Public Safety Broadband Network (NPSBN) in segments of the 700 MHz band spectrum dedicated for that purpose."[30] Because commercial wireless carriers use the 600 MHz, 700 MHz, and 800 MHz bands in proximity to public safety communications, NPSTC asserted that "[a]ny jammers deployed would need to utilize extremely narrow filters to confine the jamming only to the respective commercial wireless band segments."[31]

10. In 2021, the Commission acted upon Congress's concern about the public safety threat posed by contraband devices and the request in an Explanatory Statement to the Commission's appropriation that the Commission adopt rules requiring wireless providers to immediately disable devices properly identified as contraband.[32] Through the *Contraband Second R&O*, the Commission established a regulatory framework requiring wireless providers to disable contraband wireless devices in correctional facilities upon the submission of a qualifying request by a designated correctional facility

[25] *See, e.g.,* CTIA 2020 Comments at 14 (arguing that jamming is "quick and cheap only when done in an unsophisticated, brute force manner…"); T-Mobile 2020 Comments at 19 (contending that the costs to deploy and operate precision jamming systems are roughly equivalent to the costs of deploying MAS solutions); AT&T 2020 Reply Comments at 11 (arguing that any reasonably-installed jamming system would be as costly as managed access).

[26] *Contraband Refresh PN*, 35 FCC Rcd at 7913-14; *see also* 47 U.S.C. § 333.

[27] *See, e.g.,* CTIA 2020 Comments at 13-15 (arguing that, in addition to its reasons for generally opposing third-party jamming, self-jamming would be "fundamentally antithetical" to sound network design, further increase the cost as a result of having to set up jamming systems at each correctional facility, and be against legal precedent); T-Mobile 2020 Comments at 18 (contending that self-jamming would still remain susceptible to legal liability as intentional interference); Verizon Comments, GN Docket No. 13-111, at 9 (Sept. 16, 2020) (Verizon 2020 Comments) (arguing that self-jamming faces the same legal and technical challenges as third-party jamming).

[28] Comments of the National Public Safety Telecommunications Council (NPSTC), GN Docket 13-111, at 3 (Sept. 15, 2020) (NPSTC 2020 Comments).

[29] *Id*.

[30] *Id*.

[31] *Id*. NPSTC also suggested that "if jammers are ultimately allowed, each jamming device authorized must be tested to ensure there is no interference to public safety or FirstNet communications." *Id*.

[32] *See* Explanatory Statement to 2021 Consolidated Appropriations Act, Book IV, 166 Cong. Rec. H8311, H8440 (daily ed. Dec. 21, 2020) (2021 Explanatory Statement); *see also 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 Sen. James Lankford et al., to Chairman Pai, FCC, GN Docket No. 13-111 (Sept. 16, 2020).

official (DCFO).[33] The adopted framework includes a two-phase authorization process through which an entity—including, but not limited to, a solutions provider, equipment manufacturer, or correctional facility—may seek Commission authorization to deploy a CIS at a correctional facility that will provide the information necessary for a DCFO to submit qualifying requests to disable contraband wireless devices at correctional facilities.[34] In phase one, a prospective CIS operator may submit an application to the Bureau describing the legal and technical qualifications of its system as well as a test plan that can be adapted to the circumstances for each planned deployment at a specific correctional facility.[35] Once approved under phase one, the CIS operator may begin marketing and selling its approved technology to correctional facilities and perform on-site testing at individual correctional facilities.[36] In phase two, the CIS operator must test its approved CIS at each of the individual correctional facilities where it intends to use the CIS as the basis for submitting qualifying requests and must file a self-certification with the Commission following successful testing.[37] After both phases are complete, a DCFO may begin submitting qualifying requests to wireless providers to disable contraband devices that have been detected by a certified CIS.[38]

11. In the *Contraband Second FNPRM*, the Commission sought further comment on the relative effectiveness, viability, and cost of additional solutions, including those raised in the Explanatory Statement, such as the use of "quiet zones," geolocation-based denial (also known as geofencing) and carrier network-based solutions, beacon technology, and E-MAS.[39]

B. Current Status of Contraband Interdiction System Deployment

12. As reflected in the Commission's Universal Licensing System (ULS) records, the Bureau to date has processed over 1,900 leasing arrangements across 31 states authorizing the use of CISs (MAS and detection systems) at correctional facilities. Moreover, since the Commission adopted the CIS device disabling framework in the *Contraband Second R&O*, the Bureau has approved: (1) 16 individual DCFOs in seven states; (2) the applications of eight separate solutions provider entities authorizing Phase 1 marketing and testing of CIS for use in the submission of device disabling qualifying requests;[40] and (3)

---

[33] *See 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, 36 FCC Rcd 11813 (2021) (*Contraband Second R&O and Contraband Second FNPRM,* respectively); 47 CFR § 20.23.

[34] *Contraband Second R&O*, 36 FCC Rcd at 11821-38, paras. 21-62.

[35] *Id.* at 11821-24, paras. 22-29; 47 CFR § 20.23(b)(1)-(2).

[36] *Contraband Second R&O*, 36 FCC Rcd at 11823, para. 25; 47 CFR § 20.23(b)(2).

[37] *Contraband Second R&O*, 36 FCC Rcd at 11824-28, paras. 30-38; 47 CFR § 20.23(b)(3).

[38] *Contraband Second R&O*, 36 FCC Rcd at 11828-38, paras. 39-62; 47 CFR § 20.23(c).

[39] *Contraband Second FNPRM*, 36 FCC Rcd at 11843-49, paras. 75-89. The Commission received seven comments and one reply comment in response to the *Contraband Second FNPRM. See, e.g.*, Comments of ShawnTech Communications Inc. (rec. Aug. 13, 2021) (ShawnTech 2021 Comments); Comments of T-Mobile USA, Inc. (rec. Sept. 13, 2021) (T-Mobile 2021 Comments); Comments of AT&T Services, Inc. (rec. Sept. 13, 2021) (AT&T 2021 Comments); Comments of CTIA (rec. Sept. 13, 2021) (CTIA 2021 Comments); Comments of OmniProphis Corporation (rec. Sept. 14, 2021) (OmniProphis 2021 Comments); Comments of Cell Command, Inc. (rec. Sept. 14, 2021) (Cell Command 2021 Comments); Reply Comments of OmniProphis Corporation (rec. Oct. 13, 2021) (OmniProphis 2021 Reply Comments).

[40] *Wireless Telecommunications Bureau Approves Five Contraband Interdiction System Certification Applications Under Phase One of the Authorization Process*, GN Docket No. 13-111, Public Notice, DA 23-547 (WTB 2023) (approving applications respectively filed by: CellBlox Acquisitions, LLC (CellBlox); ShawnTech Communications, Inc.; Tecore Networks; SOC, LLC; and OmniProphis Corporation); *see also Wireless Telecommunications Bureau Approves Trace-Tek, LLC's Contraband Interdiction System Certification Application Under Phase One of the Authorization Process*, GN Docket No. 13-111, Public Notice, DA 24-242 (WTB 2024) (approving an application filed by Trace-Tek, LLC); *Wireless Telecommunications Bureau Approves SDF, Inc.'s*

(continued….)

34 Phase 2 self-certifications, each authorizing use of a deployed and site-tested CIS at a specified correctional facility for the purpose of submitting qualifying requests to wireless providers seeking the disabling of contraband wireless devices.[41]

C. Current Status of RF Jamming Solutions

13. *Limitations on Non-federal Use of Jamming Technology in the United States*. Section 333 of the Communications Act prohibits any person from willfully or maliciously interfering with or causing interference to the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government.[42] In this *Third Further Notice*, we seek comment below on a possible definition of a "jamming solution,"[43] but also refer herein to jamming technology or jamming operations where more appropriate in context. Because such transmitters are used to willfully interfere with Commission-licensed or -authorized stations, non-federal entities currently are prohibited from using jamming technology to interfere with contraband wireless devices in correctional facilities.[44]

14. The wireless industry has consistently advocated against any Commission action to permit jamming solutions, citing the statutory constraint.[45] The wireless industry has also maintained, for both policy and technical reasons, a distinct preference for solutions like MAS or detection systems, arguing that those are more effective and present less risk of interference.[46] Advocates for jamming solutions in large part concede that section 333 of the Act prohibits state and local government agencies from using jammers.[47] Officials from state and local correctional agencies and other corrections

(Continued from previous page)
Contraband Interdiction System Certification Application Under Phase One of the Authorization Process, GN Docket No. 13-111, Public Notice, DA 24-1033 (WTB 2024) (approving an application filed by SDF, Inc.); *Wireless Telecommunications Bureau Approves Hawks Ear Communications LLC's Contraband Interdiction System Certification Application Under Phase One of the Authorization Process*, GN Docket No. 13-111, Public Notice, DA 25-234 (WTB 2025) (approving an application filed by Hawks Ear Communications, LLC). The Commission recently approved CellBlox's portable system, separate from the Commission's 2023 approval of a fixed CIS. *See Wireless Telecommunications Bureau Approves CellBlox Acquisitions, LLC's Second Contraband Interdiction System Certification Application Under Phase One of the Authorization Process*, GN Docket No. 13-111, Public Notice, DA 25-646 (WTB 2025).

[41] The current DCFO list can be found at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices/list-designated-correctional. The current CIS/correctional facility approval status tracker can be found at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices/disabling-process.

[42] *See* 47 U.S.C. § 333.

[43] *See infra* para. 20.

[44] *See, e.g.,* Federal Communications Commission, *Jammers*, https://www.fcc.gov/enforcement/areas/jammers (last updated Dec. 20, 2022); Federal Communications Commission, Jammer Enforcement, https://www.fcc.gov/general/jammer-enforcement (Apr. 2020); *Enforcement Advisory: WARNING: Jammer Use is Prohibited; Prohibition Applies to use by the Public and State and Local Government Agencies*, Public Notice, Advisory, 29 FCC Rcd 14737 (EB 2014); *FCC Enforcement Advisory, Cell Jammers, GPS Jammers, and Other Jamming Devices*, Public Notice, 27 FCC Rcd 2309 (EB 2012); *FCC Enforcement Advisory, Cell Jammers, GPS Jammers, and Other Jamming Devices*, Public Notice, Advisory, 26 FCC Rcd 1327 (EB 2011).

[45] *See, e.g.*, CTIA 2017 Comments at 8 (stating that jamming by non-Federal entities is illegal under Section 333 of the Act); T-Mobile 2017 Comments at 6-7 (arguing that the Act prohibits the use of jamming devices.)

[46] *See, e.g.*, CTIA 2020 Comments at 3-4, 13-15; T-Mobile 2020 Comments at 3, 17-19; T-Mobile Reply Comments, WT Docket No. 13-111, at 7-8 (rec. Oct. 1, 2020) (T-Mobile 2020 Reply Comments); AT&T 2020 Reply Comments at 9-13.

[47] 47 U.S.C. § 333. *See, e.g.,* CellAntenna Reply, GN Docket No. 13-111, at 5 (Dec. 28, 2017) (CellAntenna 2017 Reply Comments); Oklahoma Corrections Professionals Comment, GN Docket No. 13-111, at 1 (July 15, 2013) (OCP 2013 Comments).

stakeholders have supported jamming and advocated for federal legislative change.[48] These supporters suggest that when properly deployed and calibrated, jamming technology is effective and can be contained to a particular geographic area.[49] Consequently, a number of DOC directors and state prosecutors have recently renewed calls for using jamming technology to combat the contraband problem.[50] For example, in 2024, Bryan Stirling, then director of South Carolina's DOC, indicated that other CIS solutions have been implemented in South Carolina, but nonetheless expressed a preference for Commission authority to implement jamming in the state's prisons, while also protecting people outside the prison walls.[51] Most recently, South Carolina Attorney General Alan Wilson called on the Commission and Congress to allow the state to jam cell phones in state prisons, citing recent reports finding that illegal cell phones are the primary tool inmates use to perpetrate criminal activity.[52] In Georgia, Attorney General Christopher Carr submitted a letter to the Commission in 2024 advocating for reconsideration of the "FCC's prohibition on the use of cell phone jamming devices in state and local jails and prisons."[53] Mr. Carr noted that the BOP has recognized the potential value of cell phone jammers in

[48] *See* Bryce Peterson, et al., Urban Institute, Interdiction Technologies and Strategies for Contraband Cell Phones at 6 (2022), https://www.urban.org/sites/default/files/2022-07/Interdiction%20Technologies%20and%20Strategies%20for%20Contraband%20Cell%20Phones.pdf; John Shaffer, et al., Urban Institute, Cell Phone Jamming Technology for Contraband Interdiction in Correctional Settings at 8 (2023), https://www.urban.org/sites/default/files/2023-07/Cell%20Phone%20Jamming%20Technology%20for%20Contraband%20Interdiction%20in%20Correctional%20Settings.pdf#:~:text=Although%20most%20correctional%20agencies%20in%20the%20United,Cumberland%2C%20Maryland%2C%20in%20January%202018%20(NTIA%202018) (2023 Urban Institute Report). These reports were funded by an award from the United States Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

[49] 2023 Urban Institute Report at 8.

[50] *See, e.g.*, Alex Brizee, The Idaho Statesman, *After deadly escape, Idaho lawmakers call for tech to jam prison cell phones* (Mar. 31, 2025), https://www.corrections1.com/legal/after-deadly-escape-idaho-lawmakers-call-for-tech-to-jam-prison-cellphones (inmates carrying out a coordinated escape plan via contraband cell phones that led to the injury of three correctional officers and further homicides); Craig Monger, *Alabama Department of Corrections courting technology to block cell phone use in Alabama prisons* (June 20, 2023), https://1819news.com/news/item/alabama-department-of-corrections-courting-technology-to-block-cell-phone-use-in-alabama-prisons (Alabama Department of Corrections Commissioner John Hamm believes the best way to combat the problem would be cell phone jammers); J.T. Mitchell, *MDOC commissioner: State prisons should be allowed to jam cellphones* (May 31, 2023), https://www.supertalk.fm/mdoc-commissioner-state-prisons-should-be-allowed-to-jam-cellphones/ (Mississippi Department of Corrections Commissioner Burl Cain believes that the easy solution to the problem is to allow jamming in state prisons).

[51] *See* David Sherfinski, *US prisons use new tech to dial down illegal cellphones* (Jan. 29, 2024), https://www.context.news/digital-rights/us-prisons-use-new-tech-to-dial-down-illegal-cellphones.

[52] *See* News Release, South Carolina Attorney General Alan Wilson, *State Grant Jurors issue rare report on continued problem of organized crime run from within state prisons using contraband cellphones* (July 9, 2025), https://www.scag.gov/about-the-office/news/state-grand-jurors-issue-rare-report-on-continued-problem-of-organized-crime-run-from-within-state-prisons-using-contraband-cellphones/; SC Jury Reports at 3. The SC Jury Reports recommend that jamming would immediately eliminate criminal activity within state prisons. SC Jury Reports at 4. The South Carolina legislature created the State Grand Jury in 1989 as an investigative body to investigate and indict criminal activity across the state. *See* South Carolina Attorney General's Office, State Grand Jury, https://www.scag.gov/inside-the-office/state-grand-jury/ (last visited Sept. 3, 2025).

[53] Letter from Christopher Carr, Georgia Attorney General, to Chairwoman Jessica Rosenworcel, FCC, at 1 (June 4, 2024) (Carr Letter); *see also* Angelina Salcedo, *Deadly gang-ordered hit sparks renewed push by Georgia AG to block contraband phones in prisons and jails* (Mar. 5, 2025), https://www.11alive.com/article/news/state/deadly-gang-hit-georgia-ag-chris-carr-push-to-block-contraband-phones-in-prisons-and-jails/85-83a40400-26cf-4067-a584-95c711b8d6b0 (murder of two boys orchestrated by an incarcerated gang member using an illegal cellphone).

federal penitentiaries.[54] The BOP, in collaboration with the Commission and the National Telecommunications and Information Administration (NTIA), has in fact tested micro-jamming technology at correctional facilities in Maryland and South Carolina to determine whether the technology could block inmate calls from a contraband device in a housing unit.[55] NTIA subsequently released a report on the results of the testing in South Carolina, which could be characterized as showing that the technology could be effective in fighting contraband cell phone use in correctional facilities.[56] In response to the Georgia Attorney General's letter, then-Chairwoman Rosenworcel agreed that contraband wireless devices in prisons pose a serious public safety hazard, but noted that jamming in state and local correctional facilities is currently prohibited by the Act and could potentially threaten public safety.[57] The Commission has referenced section 333 since its enactment in a variety of contexts and, as related to this proceeding, the Commission's Bureaus and Offices have uniformly interpreted section 333 to specifically prohibit the use of jammers in non-federal correctional facilities.[58]

15. *Recent Legislative Efforts to Allow Jamming Technology in United States*. In March 2025, Senator Tom Cotton of Arkansas and Representative David Kustoff of Tennessee introduced federal legislation, the Cellphone Jamming Reform Act of 2025, intended to permit state prisons to use jamming systems to prevent inmates from using contraband cell phones.[59] The bills under consideration state that, notwithstanding any other provision of law, the Commission may not prevent a state or federal

[54] *See* Carr Letter at 2. Other stakeholders have recognized the dangers of the lack of the ability to implement jamming solutions in state correctional facilities as compared to federal facilities where jamming is not prohibited by law. *See, e.g.*, Nate Gartrell, The Mercury News, *Federal prison will take California's 'most dangerous' Aryan Brotherhood inmates* (Apr. 15, 2025), https://www.corrections1.com/gang-and-terrorist-recruitment/federal-prison-will-take-californias-most-dangerous-aryan-brotherhood-inmates (during the trial of Aryan Brotherhood members in California, prosecutors argued initially for moving the inmates out of the state prison system where they could easily obtain contraband phones and order murders, arsons, robberies, and shakedowns, to federal prison to keep the public safe).

[55] *See* Press Release, Department of Justice, NTIA, *National Telecommunications and Information Administration Releases Report on Effectiveness of Micro-Jamming Contraband Cellphones in Prisons* (Sept. 25, 2019), https://www.justice.gov/archives/opa/pr/national-telecommunications-and-information-administration-releases-report-effectiveness. The BOP notes in the release that it will continue to evaluate interception technologies and work with its partners and Congress to achieve cost-effective options to combat this threat to corrections and public safety. *Id.*

[56] Frank H. Sanders, Geoffrey A. Sanders, and John E. Carroll, Technical Report NTIA TR-19-541, Emission Measurements of a Contraband Wireless Device Jammer at a State Prison (2019), https://its.ntia.gov/publications/download/TR-19-541.pdf.

[57] *See* Letter from Chairwoman Jessica Rosenworcel, Federal Communications Commission, to Christopher Carr, Georgia Attorney General (July 30, 2024). The letter included a staff appendix that provided additional information regarding the views of the Chairwoman (not the full Commission) and staff at the time. Today, while recognizing the parameters of the Act, we explore creative solutions to provide the corrections community with additional tools to help resolve this public safety issue.

[58] *See supra* note 44.

[59] Press Release, Cotton, Kustoff Introduce Bill to Keep Cellphones Out of Jails (Mar. 26, 2025), https://www.cotton.senate.gov/news/press-releases/cotton-kustoff-introduce-bill-to-keep-cellphones-out-of-jails (last visited Sept. 3, 2025); https://kustoff.house.gov/media/press-releases/kustoff-cotton-introduce-legislation-jam-cellphones-prisons (last visited Sept. 3, 2025). We also note that a bipartisan bill to increase federal criminal penalties for smuggling a contraband cell phone into a federal prison, introduced by Senator Jon Ossoff and named "Lieutenant Osvaldo Albarati Stopping Prison Contraband Act," passed the Senate in September 2024. *See* S. 5284, 118th Cong., 2nd Sess. (2024).

correctional facility from operating a jamming system in housing units.[60] In a letter to congressional leaders in support of the pending federal legislation, a bipartisan coalition of state attorneys general reiterated the severity of the problem that continues to escalate as a critical threat to public safety.[61] The attorneys general noted that while they have access to some technological interdiction solutions, they are unable to deploy jamming systems in state correctional facilities because they are restricted by federal law.[62] They urge the passage of legislation that would enable them to deploy what they consider to be "the most effective tool available," i.e., jamming systems.[63]

16. *International Jamming Deployments*. Jamming technology has been tested and deployed internationally at various correctional facilities. Some countries, such as Australia, have permitted the operation of jammers in certain correctional facilities for many years after testing showed that jammers were successful in stopping the illicit use of phones by inmates, while not causing interference to outside mobile phone users.[64] Other countries, such as France and Canada, have more recently selectively tested or implemented jamming technology to counter the evolving threat of contraband devices in prisons.[65] In addition, in countries that have authorized the use of jamming devices in correctional facilities, such as India, officials are studying new jamming technologies to improve on the existing jamming solutions in place at certain prisons.[66] We recognize that jamming solutions, like any RF system, present engineering challenges. For example, a New Zealand jamming system was removed after causing interference to new safety systems, such as corrections officers' safety alarms.[67] Engineering challenges with regard to preventing interference to legitimate phone use outside the prison perimeter are particularly acute in urban areas, for example, in many prisons in Latin America.[68] Countries such as Argentina, Brazil, and Chile that have deployed jamming systems in prisons in densely populated areas note that authorized users have

[60] *See* H.R. 2350, 119th Cong., 1st Sess. (2025). We note that a similar bill was introduced in the House in 2023 and referred to the Committee on Energy and Commerce, but it saw no further action and is no longer active. *See* H.R. 2380, 118th Cong., 1st Sess. (2023).

[61] The Attorneys General of Georgia, Tennessee, North Carolina, and the U.S. Virgin Islands, joined by Attorneys Generals of several other states and territories, sent the letter to Congress urging passage of legislation allowing states to deploy cell phone jamming systems in jails and prisons. *See* Letter from Jonathan Skrmetti, Tennessee Attorney General, et al., to the Honorable John Thune, Senate Majority Leader, et al., at 1-2 (Mar. 26, 2025), https://ncdoj.gov/wp-content/uploads/2025/03/2025-3-phone-jamming.pdf (last visited Sept. 3, 2025).

[62] *Id*. at 2.

[63] *Id*.

[64] *See* Australian Communications and Media Authority, *Phone jammers*, https://www.acma.gov.au/phone-jammers (last visited Sept. 3, 2025) (noting that in Australia, corrective services has an exemption to operate mobile phone jammers at certain correctional facilities after trials of jammers were conducted).

[65] *See, e.g.*, IPS Innovative Prison Systems/ICJS Innovative Criminal Justice Solutions, Inc., *Exploring Future-Focused Solutions in the French Prison Administration*, Interview with Laurent Ridel (Oct. 19, 2023), https://justice-trends.press/exploring-future-focused-solutions-in-the-french-prison-administration/#:~:text=In%20our%20maximum%20security%20facilities%2C%20we%27ve%20even,jamming%20systems%20to%20disrupt%20mobile%20phone%20signals; Anja Karadeglija, The Canadian Press, *Federal, Quebec prisons to launch pilot project on jamming cellphone, drone signals* (Mar. 7, 2025), https://www.ctvnews.ca/montreal/article/federal-quebec-prisons-to-launch-pilot-project-on-jamming-cellphone-drone-signals/.

[66] Atul Mathur, Time of India, *Delhi govt looks for new tech to block mobile signals at three jail complexes* (Nov. 24, 2024), https://timesofindia.indiatimes.com/city/delhi/delhi-government-seeks-advanced-signal-blocking-technology-for-jails-to-curb-illegal-phone-use/articleshow/115632553.cms.

[67] Marty Sharp, Stuff, *Costly cellphone jamming technology ditched in all prisons* (Dec. 14, 2022), https://www.stuff.co.nz/national/crime/130732335/costly-cellphone-jamming-technology-ditched-in-all-prisons.

[68] *See generally* 5G Americas, Mobile Signal Jammers in Latin America (2018), https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_WP_Bloqueadores_AmLat_Aug._2018_EN.pdf.

experienced blocked calls or deterioration in the quality of mobile communications in the neighborhoods and areas surrounding the prisons.[69]

17. Other countries' experiences with jamming clearly demonstrate that proper engineering is necessary to prevent harmful interference to authorized users, and these case studies are instructive in evaluating any proposal to authorize the deployment of jamming solutions solely in the correctional facility context.[70] As discussed in detail below, we believe that properly deployed transmitters that are part of a carefully engineered jamming solution can be effective and that we should facilitate tailored use as an available option for DOCs.

III. THIRD FURTHER NOTICE OF PROPOSED RULEMAKING

18. Today, we take a significant step towards ensuring that U.S. corrections officials are able to access a full range of RF technologies for use in combatting contraband wireless device use in correctional facilities. We seek to remove barriers to the deployment and viability of these technologies in a manner that both complies with section 333 of the Act and addresses the risk that authorized users may receive harmful interference. Thus, in this *Third Further Notice*, we propose to deauthorize, for purposes of Commission licensing, subscriber operation of contraband wireless devices. We also propose to leverage our existing leasing process as a preferred approach to licensing jamming solutions, thereby providing correctional officials with additional methods to address a demonstrable public safety threat. Below, we describe our proposed deauthorization rule and seek comment on a variety of considerations, including the costs and benefits. We then address ways in which the Commission can authorize eligible entities to deploy jamming solutions to combat the use of contraband wireless devices in correctional facilities, while ensuring that our rules afford consistent regulatory treatment across technologies deployed for this purpose. We also propose and seek comment on restrictions that might prove necessary to ensure that jamming solutions are limited to this targeted use, and to mitigate the risk that these solutions are deployed in contexts other than a correctional facility environment. Finally, we seek further comment on other technological solutions, and whether the Commission should take regulatory steps to support their development and deployment.

19. As discussed above, the Commission has explored multiple technological solutions that might be used to combat contraband wireless devices, if consistent with section 333 of the Communications Act's prohibition against willful or malicious interference.[71] In addition to supporting MAS and detection systems, the Commission has collected a record on other potential solutions, such as "quiet zones" and beacon technology, and has asked stakeholders to comment on their legality and challenges to their deployment.[72] In this *Third Further Notice*, as we explore other methods to combat contraband wireless device use, including jamming solutions, we recognize that any RF solution, if improperly engineered or maintained, can disrupt the ability of non-contraband, authorized devices located outside a correctional facility or within the facility, if permitted in certain areas, to connect to a wireless provider network, including potentially impacting public safety communications. We further recognize, as an economic reality, that the costs associated with any RF solution, whether MAS, detection, or jamming solutions, are case-specific to each correctional facility and its surrounding RF environment. Although today's action is focused on expanding corrections officials' options, stakeholders, particularly departments of correction, are cautioned that a jamming solution may not be

[69] *Id*. at 23-27.

[70] *See generally* 2023 Urban Institute Report at 4-7 (identifying implementation considerations such as overall efficacy, containment accuracy, no option to whitelist, long-term health effects, challenges to rehabilitation, and cost).

[71] *See, e.g., Contraband NPRM*, 28 FCC Rcd at 6636, para. 77.

[72] *See, e.g*., *Contraband First R&O*, 32 FCC Rcd at 2380-83, paras. 122-32; *Contraband Refresh PN*, 35 FCC Rcd at 7912; *Contraband Second R&O*, 36 FCC Rcd at 11843-47, paras. 75-85.

technically feasible in all correctional facility contexts, and that the costs of any RF solution to address this problem, including long sought-after jamming solutions, can rise commensurate with the extensive engineering and ongoing network maintenance required to limit harmful interference solely to the intended target of contraband wireless devices located in correctional facilities.

A. Definition of Jamming Solution

20. As a threshold matter, we propose to define the term "jamming solution" as "the deployment of RF transmitter(s) within a correctional facility to prevent contraband wireless devices from establishing or maintaining a connection with a network."[73] We emphasize that this definition is solely applicable in the context of combatting contraband wireless devices in correctional facilities and incorporates the concept that such a solution disrupts a network connection on affected spectrum bands in a specific geographic area. We seek comment on this proposed definition and any alternatives that commenters believe will further our goals in this proceeding.

21. We recognize that a jamming solution is intended to prevent connection to the wireless network altogether and therefore has different functionality than currently deployed CISs (i.e., MAS[74] and detection systems[75]) operating through lease arrangements with wireless providers. CIS is defined in our leasing rules as "… a 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 to obtain identifying information from such contraband wireless devices."[76] Unlike a jamming solution, a MAS allows authorized devices and emergency communications to connect with the wireless network, while transmissions to or from unauthorized devices are ultimately terminated. The Commission adopted the current definition of CIS in the leasing rules to reflect operation of not only MASs, but also detection systems, the latter of which transmits signals for the primary purpose of acquiring identifying information from a contraband wireless device.

22. We find it necessary to propose a definition of jamming solution in the context of our proposed framework that involves, as a preferred approach to licensing such solutions, leveraging our existing leasing process, but that also includes an overlay licensing fallback option in certain circumstances. To provide clarity for stakeholders regarding both licensing frameworks, we therefore propose to incorporate a definition of a "jamming solution": (1) as another type of CIS where appropriate to facilitate leasing arrangements, with certain special provisions solely applicable to jamming solutions where warranted;[77] and (2) to authorize overlay licensees to provide such a solution where certain eligibility criteria are met.[78]

B. Deauthorizing Subscriber Operation of Contraband Wireless Devices

23. Today, we propose to address the prohibition in section 333 by deauthorizing subscriber operation of contraband wireless devices located within a correctional facility. Specifically, we propose to amend our rules and the rights granted under licenses we have issued, such that operations in this specific context would not be authorized by the Commission within the meaning of section 333. This approach would, we believe, allow DOCs to employ jamming solutions, or other similar technologies,

[73] *See* Appx. A (proposed addition to rule 1.9003). *See also infra* para. 27-28 (seeking comment on a proposed definition of "correctional facility" in the context of deauthorizing subscriber operations of contraband wireless devices).

[74] *See supra* note 11.

[75] *See supra* note 13.

[76] *See* 47 CFR § 1.9003.

[77] *See infra* para. 36.

[78] *See infra* para. 72.

without violating section 333, and would provide an additional tool to prevent criminal activity stemming from unauthorized communications within and to those outside a correctional facility.[79] Below, we discuss and seek comment on the details of our proposed deauthorization rule, as well as distinct jamming solution licensing mechanisms. We also seek comment on a potential safe harbor for wireless providers to the extent they might be liable for unauthorized operation of subscriber devices that fall within the proposed deauthorization rule.[80] We anticipate that our multipronged approach will facilitate DOC deployment of effective, focused jamming solutions in correctional facilities to increase public safety, while incentivizing wireless provider participation. We also seek comment on any alternative approaches that commenters believe will, consistent with the current statutory framework, provide DOCs with additional potential technological solutions to the issue of contraband wireless device use.

1. Subscriber Authority Rule

24. The Commission does not currently allow the use of jamming technologies by non-federal corrections officials because these solutions willfully interfere, in violation of section 333, with radio communications of stations licensed or authorized by the Commission.[81] Some commenters have misinterpreted the statutory term "authorized," arguing that operation of a device that is "unauthorized" under state law, regulation, or correctional facility policy also has no commensurate Commission authority to operate as a licensing matter.[82] Under current Commission rules, however, wireless providers may legally transmit RF signals within the boundaries of their geographic area license, including areas within those boundaries where a correctional facility may be located. Under our current rules, subscribers operating devices in connection with those licensed services are authorized under that same wireless provider license pursuant to section 1.903(c) of the Commission's rules.[83] Today, we propose a key change to the authorization status, as it relates to Commission licensing, of subscribers operating contraband wireless devices on commercial wireless networks in correctional facilities, which will enable the Commission to authorize jamming solutions in a narrow context in compliance with section 333 of the Act. This action will provide maximum regulatory flexibility to DOCs in their efforts to solve a critical

[79] We note that certain criminal statutes may be relevant to the deployment of jamming solutions in correctional facilities, such as those in Title 18 that may directly or indirectly impose restrictions on RF jamming and the equipment used for that purpose. *See, e.g.,*18 U.S.C. § 545 (establishing a penalty for importation of illegal equipment); 18 U.S.C. § 1352 (prohibiting, subject to certain limited exceptions, willful or malicious interference with any communications line either controlled by the U.S. Government "or used or intended to be used for military or civil defense functions of the United States."); 18 U.S.C. § 1367(a) (prohibiting such interference to non-government satellite transmissions). We clarify, however, that today's proposed deauthorization approach and licensing framework focus on actions within the Commission's jurisdiction to authorize jamming solutions in correctional facilities.

[80] Such liability arguably could result from, for example, a wireless provider continuing to authenticate a device on its network when operation of the device, previously licensed under the blanket authorization of that wireless provider, is no longer licensed under the Act and the Commission's rules.

[81] Commission authorization of RF energy transmissions is required pursuant to section 301 of the Act. 47 U.S.C. § 301.

[82] *See*, *e.g.*, Global Tel*Link Corp. Request for Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Creation of New Rule(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities, Petition for Rulemaking, PRM11WT (filed July 20, 2011) at 16-17 (questioning whether CMRS devices that are illegal to possess due to state criminal statute have a valid FCC authorization and asserting that federal government cannot authorize use of wireless devices by inmates in any correctional facility where possession or use of such devices is illegal by state law or federal policy).

[83] 47 CFR § 1.903(c) ("Authority for subscribers to operate mobile or fixed stations in the Wireless Radio Services . . . is included in the authorization held by the licensee providing service to them. Subscribers are not required to apply for, and the Commission does not accept, applications from subscribers for individual mobile or fixed station authorizations in the Wireless Radio Services.").

public safety need. Further, to help prevent harmful interference to legitimate users, a long-standing wireless industry concern, our lead proposal, as discussed below, would involve the participation of wireless providers as spectrum lessors.

25. As a threshold matter, we propose to amend section 1.903(c)[84] to create an exception regarding subscriber operation of a "contraband wireless device."[85] Specifically, we propose to amend the rule to make clear that subscriber contraband wireless device operation of any fixed or mobile station in the Wireless Radio Services (WRS) is not authorized by the Commission.[86] As such operation would not be considered to be "licensed or authorized by or under [the] Act,"[87] there is no statutory protection against willful or malicious interference by other technologies, such as jamming solutions, that would be licensed under our proposed process.[88] We refer to this proposal throughout as the "deauthorization rule" or "deauthorization approach." We tentatively conclude that we have the authority to propose this approach pursuant to section 303 of the Act, which provides the Commission with expansive powers and duties to make rules governing wireless operations that are required by the public convenience, interest, or necessity.[89] In particular, portions of section 303 direct the Commission to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class"; to "[d]etermine the location of classes of stations or individual stations"; to "establish areas or zones to be served by any station"; to "prescribe the qualifications of station operators"; and to "[m]ake such rules and regulations and prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of [the Act]."[90] We seek comment on this tentative conclusion, and on our deauthorization approach more generally.

26. We propose to apply the deauthorization rule to subscriber operation of a contraband wireless device that is used within a correctional facility in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy, and seek comment on this approach. This expansive approach is consistent with the Commission's definition of "contraband wireless device" as applied in our current CIS leasing context,[91] and recognizes that there are a number of jurisdictions that, while prohibiting the possession or use of contraband wireless devices in correctional facilities, do not apply statutory criminal penalties for a violation.[92] We propose to take this more flexible approach to deauthorization of contraband wireless devices in order to enable us to authorize jamming solutions. We note, however, that in the 2021 *Contraband Second R&O*, the Commission adopted the framework permitting DOC officials with an approved CIS to request that wireless providers disable contraband wireless devices. In so doing, the Commission took a narrower view of "contraband wireless devices" and limited disabling of such devices to those "used in violation of state or federal criminal statutes."[93] The Commission clarified that CIS providers "operating at correctional facilities located in states where

[84] *Id.*

[85] *See* 47 CFR § 1.9003 (defining "contraband wireless device" as "any wireless device, including the physical hardware or part of a device, such as a subscriber identification module (SIM), that is used within a correctional facility in violation of federal, state or local law, or a correctional facility rule, regulation or policy.").

[86] Such authorization to transmit is required under the Act. *See* 47 U.S.C. § 301.

[87] 47 U.S.C. § 333.

[88] *Id.*; *see also M.C. Dean, Inc.*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 13010, 13022, para. 29 (2015) (discussion of "stations" as used in section 333 of the Act).

[89] 47 U.S.C. § 303.

[90] 47 U.S.C. § 303(b), (d), (h), (l)(1), (r).

[91] *See supra* note 85.

[92] *See supra* note 5.

[93] *Contraband Second R&O*, 36 FCC Rcd at 11826, para. 31; *see also* 47 CFR § 20.23(b)(3)(ii)(B).

possession or use of contraband devices has not been criminalized in the penal code will not be eligible" to utilize the disabling framework.[94] The restrictive approach in the disabling context was based on the premise that the ability to request that a wireless provider cease service to a contraband wireless device should be limited to those states that address this important public safety concern by criminalizing possession/use of contraband devices in correctional facilities, rather than those that merely impose administrative sanctions for an inmate's violation of a prison regulation. We seek comment, however, on whether to apply to our deauthorization rule the more restrictive approach taken in the CIS disabling context. Should the proposed deauthorization rule apply only to those states that have criminal penalties for the possession or operation of contraband wireless devices, consistent with the Commission's section 20.23 framework for CIS disabling? Would this approach, while incentivizing states to enact criminal penalties for contraband device possession, still meet the public safety goal of thwarting prisoners' criminal activity? Commenters should address the costs and benefits of our proposed approach or the alternative upon which we seek comment, if preferred.

27. We propose to apply the deauthorization rule to subscriber operations of contraband wireless devices used in "correctional facilities," as defined in our existing CIS leasing context. Section 1.9003 defines correctional facility as "any facility operated or overseen by federal, state, or local authorities that houses or holds criminally charged or convicted inmates for any period of time, including privately owned and operated correctional facilities that operate through contracts with federal, state or local jurisdictions."[95] Applying this definition in the context of deauthorizing subscriber operations of contraband wireless devices would promote consistency across interdiction technologies, similar to our proposal to align our deauthorization approach with the definition of "contraband wireless device" in our existing CIS leasing framework.

28. We recognize, however, that our proposed deauthorization rule would apply broadly to contraband wireless devices located in correctional facilities that include local facilities, e.g., city or county jails, often located next to, or relatively near, other government facilities (e.g., a city hall, courthouse, etc.) or residential areas. This proximity presents an increased risk of interference to authorized devices if a jamming solution is not properly engineered, deployed, and maintained. If a jamming solution is carefully engineered, deployed, and maintained, is there an increased risk of harmful interference from implementation in local correctional facilities, particularly as compared to a MAS solution that also implements an RF technology requiring a very limited area of operation and careful engineering to minimize the risk of harmful interference? We seek comment on whether it is necessary to restrict the application of our deauthorization rule and subsequent authorization of jamming solutions to a particular type(s) of correctional facility. In this regard, we also seek comment on the extent to which contraband devices are used in local facilities, and whether local municipalities are seeking these particular RF solutions that, as stated, require extensive technical expertise to engineer and require associated costs to install and maintain. Where are states more likely to invest in carefully deployed, properly engineered and maintained jamming solutions? Should we consider the security level of the correctional facility (e.g., minimum, medium, maximum), or the average length of time of inmate incarceration, in this analysis? Commenters advocating for a restriction should consider our goal of reaching those facilities where contraband wireless device use is a serious public safety threat,[96] and should also address the argument that a properly engineered and maintained jamming solution is

[94] *Contraband Second R&O*, 36 FCC Rcd at 11826, para. 31.

[95] 47 CFR § 1.9003.

[96] For example, we note that in the *Contraband Second R&O*, the Commission established a framework for corrections officials using an authorized CIS to request wireless providers disable contraband wireless devices located in "permanent" correctional facilities, a more restrictive approach. *See Contraband Second R&O*, 36 FCC Rcd at 11821, para. 21; *see also* 47 CFR § 20.3 (defining a "Contraband Interdiction System" as a "system comprised of one or more stations that is used only at a permanent correctional facility . . .").

substantially less likely to cause harmful interference to authorized users, notwithstanding the proximity issue.

29. Below we seek detailed comment on authorizing jamming operations on spectrum bands traditionally used by wireless providers in commercial network deployments.[97] This approach directly results from our proposal to deauthorize subscriber operation of a contraband wireless device that is currently authorized under a wireless provider's license. We recognize, however, that today's more advanced end-user devices also transmit/receive on bands outside of traditional commercial bands. We therefore seek comment below on whether we should expand the scope of our deauthorization approach to facilitate jamming solutions that might address scenarios of contraband wireless device use not necessarily relying on spectrum commonly deployed in subscriber-based commercial wireless networks, while remaining consistent with section 333.[98] Although the record in this proceeding to date does not reflect that these types of devices are currently used as contraband in correctional facilities, we seek comment on whether failing to specifically deauthorize their operation in a correctional facility, through whatever manner is appropriate, as it relates to authority under section 301 of the Act, would provide a loophole that could be exploited by inmates.

2. Section 316 License Modification

30. Section 316 of the Act states that "any station license or construction permit may be modified by the Commission . . . if in the judgment of the Commission such action will promote the public interest, convenience and necessity."[99] Today, we propose a rule change to deauthorize certain operations that would be promulgated pursuant to the Commission's rulemaking authority consistent with the Administrative Procedure Act.[100] As additional legal support for this approach, we also hereby propose, pursuant to section 316 of the Act, to modify any and all licenses affected by the proposed rule change, if adopted and made effective, that would eliminate authority for WRS subscribers to operate contraband wireless devices in correctional facilities.[101] Courts have held that the Commission can exercise this section 316 authority by rulemaking,[102] and modifications adopted by rulemaking do not necessarily need to be reflected in the individual licenses issued to licensees.[103] We believe that this proposed modification is within our authority under the Act, is in the public interest and, given that its scope is limited to deauthorizing subscriber operation of contraband wireless devices in correctional facilities, does not result in a fundamental change to any underlying wireless provider license. We seek comment on this proposal.

---

[97] These bands currently track those listed within "Included Services" for purposes of leasing under part 1, subpart X of our rules. *See infra* paras. 39-40.

[98] *See infra* paras. 109-119.

[99] 47 U.S.C. § 316. We note that that this authority has been interpreted not to extend to any "fundamental change" to the terms of a license. *See Cellco Partnership v. FCC*, 700 F.3d 534, 543-44 (D.C. Cir. 2012) (section 316's power to modify existing licenses does not allow the Commission to fundamentally change those licenses); *see also Community Television v. FCC*, 216 F.3d 1133, 1140-41 (D.C. Cir. 2000).

[100] *See* 5 U.S.C. § 553.

[101] *See* Appx. A (proposed revision to rule 1.903(c)).

[102] *Cellco P'ship*, 700 F.3d at 542; *Celtronix Telemetry, Inc. v. FCC*, 272 F.3d 585, 589 (D.C. Cir. 2001).

[103] *See, e.g., Use of the 5.850-5.925 GHz Band*, ET Docket No. 19-138, First Report and Order, Further Notice of Proposed Rulemaking, and Order of Proposed Modification, 35 FCC Rcd 13440, 13463, para. 53 (2020) (Commission modified certain licenses in a rulemaking pursuant to section 316 without the need to make changes to licenses in ULS).

3. Safe Harbor to Proposed Deauthorization Rule

31. The proposed deauthorization rule would make subscriber operation of any contraband wireless device in a correctional facility a violation of section 301 of the Act and proposed revised section 1.903(c) of the Commission's rules.[104] We seek to make available increased opportunities for technological solutions that can address the contraband device problem, while anticipating wireless industry concerns regarding potential liability for rule violations stemming from deauthorization in this context. We recognize that wireless providers might also be liable for continuing to authenticate and provide service to such devices following deauthorization. We therefore propose to create a safe harbor, to the extent necessary, for wireless providers that engage in good faith negotiations with DOCs that are actively seeking an RF solution to this issue, including a jamming solution. We believe that this approach is consistent with our goal of expanding corrections officials' options to address a difficult public safety issue, while incentivizing stakeholder cooperation in this endeavor.

32. Specifically, we propose a "safe harbor" wherein the Commission would not take enforcement action against a wireless provider arguably in violation of section 301 of the Act for unauthorized operation on its network of contraband wireless devices in a correctional facility under the following circumstances. First, the safe harbor would apply to a wireless provider licensed in a geographic area where no DOC is actively seeking to implement an RF solution, including jamming, to combat contraband wireless device use. In this regard, we do not believe it is in the public interest to hold a wireless provider liable for possible unauthorized operation of a contraband wireless device where the relevant DOC is not attempting to implement an RF solution by, for example, deploying a jamming solution through a contract with a solutions provider and actively seeking a spectrum lease arrangement with the relevant wireless provider(s) licensed in that area. Second, the proposed safe harbor would apply to a wireless provider where it actively participates in good faith negotiations (or has successfully completed such negotiations) with the DOC/solutions provider that is seeking to lease spectrum to authorize operation of a CIS, including a jamming solution.

33. We clarify that, under our proposal, where a party actively seeks authority as lessee for a jamming solution to combat contraband wireless devices and negotiates in good faith, but a wireless provider fails to negotiate in good faith, the wireless provider would not be eligible for the proposed safe harbor. We also clarify that, under our proposed approach, a wireless provider would not qualify for a safe harbor if it responds to a DOC/solutions provider request for a jamming solution by indicating that it is only willing to lease spectrum for a MAS or detection system deployment. We seek comment on this proposal, including whether a wireless provider should be eligible for the proposed safe harbor in the absence of a good faith lease arrangement, but where it can demonstrate that a DOC's jamming solution poses an unreasonable risk of interference to authorized subscribers or otherwise is not technically feasible as sought to be deployed. We also seek comment on whether to extend the proposed safe harbor to future instances where a wireless provider actively facilitates the implementation, at a DOC/solutions provider's request, of an alternative technological solution, such as geolocation or beacon technology, discussed below, in the applicable correctional facility.

34. We believe our proposal to establish a safe harbor will address any potential wireless industry concerns about liability for deauthorized operations, while also encouraging wireless providers to work with correctional facilities to combat the problem of contraband wireless device use. We seek comment on this proposal and on whether there are additional liability concerns regarding potential unauthorized transmissions in violation of section 301 and proposed revised section 1.903(c) of the Commission's rules. Commenters should specifically describe instances where they believe a wireless provider should be further shielded from enforcement action, including the costs and benefits of such an approach. Also, we are not aware of any instance where a wireless provider directly owned and installed base stations within a correctional facility to effectively block signals from its macro-network pursuant to

[104] *See* 47 U.S.C. § 301; Appx. A (proposed revision to rule 1.903(c)).

a contract with a DOC. We seek to encourage stakeholder consideration of a range of options and therefore seek comment on the prospect of wireless providers engaging directly with DOCs to install transmitters for the purpose of effectuating a jamming solution. Should we expand the scope of a prospective safe harbor to include instances where a wireless provider elects to directly employ a jamming solution in a correctional facility through a contract with a DOC?

C. Facilitating the Authorization of Jamming Solutions Under Section 301

35. We seek to ensure that eligible entities are able to access and receive Commission authorization to implement jamming solutions to combat the use of contraband wireless devices in correctional facilities. We recognize the concerns raised by some stakeholders regarding the possible impact that authorizing the operation of a jamming solution, if not implemented properly, may have on the spectrum environment. We seek to create an authorization framework that balances those important interests and concerns with the significant and growing security challenges that contraband wireless devices pose to DOCs, law enforcement authorities, and the general public. Thus, we seek comment below on narrowly tailored authorization mechanisms that would advance our goal of removing unnecessary barriers to facilitate expedited deployment of an expanded range of technological solutions to combat this problem, while ensuring that authorized wireless network operations are not subject to harmful interference. We also seek to ensure that jamming solutions are limited to the context of correctional facilities. We seek comment on the proposals below, including their associated costs and benefits.

1. Authorization of Jamming Solutions

a. Spectrum Leasing

36. Section 301 of the Communications Act requires a valid Commission license for non-federal operation of a radio frequency transmitting device.[105] This statutory requirement is reflected in the Commission's rules, which require a license (or lease arrangement with a licensee) to operate a station in the WRS.[106] To be effective, a jamming solution deployed in a correctional facility will necessarily include base stations transmitting on frequencies licensed to and used by WRS licensees to provide commercial service to their subscribers. Accordingly, any jamming solution requires Commission authorization to transmit on wireless providers' exclusively licensed spectrum.[107] Today, we propose to authorize jamming solutions in correctional facilities by substantially leveraging our existing leasing regime used for CIS deployment in correctional facilities.[108] We seek comment above on a proposed definition of "jamming solution" to distinguish it, where relevant, from other CISs.[109] Importantly, however, we also propose to amend our current definition of CIS by: (1) incorporating jamming solutions as a type of CIS for purposes of administrative efficiency and to achieve regulatory harmony across technologies where feasible and appropriate; and (2) refining the CIS definition to better describe current CISs that have the capability of preventing contraband wireless devices from ultimately connecting to a wireless provider network, while also distinguishing between contraband and non-contraband wireless devices in the area of CIS operation (e.g., MAS).[110] We seek comment generally on this proposed leasing

[105] 47 U.S.C. § 301.

[106] 47 CFR §§ 1.903, 1.9001.

[107] 47 U.S.C. §§ 301 (requiring a license for the "transmission of energy or communications or signals by radio"), 310(d) (requiring application to the Commission for the transfer of any rights under a license to another party, such as a managed access provider).

[108] *See generally* 47 CFR §§ 1.9020 (spectrum manager leasing arrangements); 1.9030 (long-term *de facto* transfer leasing arrangements); 1.9035 (short-term *de facto* transfer leasing arrangements).

[109] Below we propose special provisions related to jamming solutions in the leasing context, given the risk of harmful interference associated with such solutions if not carefully engineered.

[110] *See* Appx. A (proposed amendment to rule 1.9003 definition of "Contraband Interdiction System").

approach to authorizing jamming solutions, which we believe will reduce complexity and associated regulatory burdens and, most importantly, will further promote stakeholder engagement on this important issue. We seek comment below on whether all aspects of the existing leasing regime are appropriate, or whether certain refinements are necessary.

37. *Leasing Arrangement Framework and Types of Leases*. When the Commission adopted its first set of comprehensive secondary markets rules more than two decades ago, it recognized the public interest benefits of permitting "additional spectrum users to gain ready access to spectrum," thus enabling the "provision of new and diverse services and applications to help meet the ever-changing needs of the public."[111] Under these long-standing rules, a licensee in any of the "included services" set forth in section 1.9005 of the Commission's rules may lease its exclusive spectrum usage rights for any purpose permitted and authorized under the license.[112] Spectrum leasing arrangements[113] can take two forms: spectrum manager leasing arrangements;[114] or *de facto* transfer leasing arrangements, which can be either long-term (more than one year) or short-term (one year or less).[115] Spectrum manager leasing arrangements generally do not require prior Commission approval; rather, the licensee/lessor must notify the Commission in advance of commencing operations.[116] In contrast, *de facto* transfer spectrum leasing arrangements are typically subject to the Commission's general approval procedures, under which the Commission must grant the application prior to the parties putting the proposed spectrum leasing arrangement into effect.[117]

38. As stated, our goal is to leverage our existing leasing rules used for CIS deployment as much as possible to reduce regulatory burdens. We therefore seek comment on the extent to which our part 1 rules require amendment to effectuate authorization through lease arrangements of transmitters operating on wireless provider licensed spectrum to deploy jamming solutions in correctional facilities. We seek comment on the specific proposals below and whether we should require any additional information to be filed with the leasing application that would necessitate a rule change to existing part 1

---

[111] *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, WT Docket No. 00-230, Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 20604, 20619, para. 32 (2003) (*Secondary Markets R&O*).

[112] *See* 47 CFR § 1.9001 *et seq*. Licensees holding exclusive use rights are permitted to engage in spectrum leasing whether their operations are characterized as commercial, common carrier, private, or non-common carrier. *Id.* § 1.9001(b).

[113] Section 1.9003 defines a "spectrum leasing arrangement" as "[a]n arrangement between a licensed entity and a third-party entity in which the licensee leases certain of its spectrum usage rights in the licensed spectrum to the third-party entity, the spectrum lessee." *Id.* § 1.9003. The arrangement may involve the leasing of any amount of licensed spectrum, in any geographic area or site encompassed by the license, for any period of time during the term of the license authorization. *Id.*

[114] *Id.* §§ 1.9010, 1.9020. A licensee/lessor is deemed to have *de facto* control over the leased spectrum if it satisfies two conditions: (i) the licensee/lessor retains responsibility for lessee compliance with Commission policy and rules; and (ii) the licensee/lessor retains responsibility for interactions with the Commission, including all filings required under the license authorization and applicable service rules directly related to the leased spectrum. *Id.* § 1.9010(b).

[115] *Id.* §§ 1.9003, 1.9030(b).

[116] *Id.* § 1.9020(e) (requiring 21 days advance notice for spectrum manager leasing arrangements greater than one year in length, or 10 days advance notice for arrangements of one year or less in length). The Commission reviews the notifications to ensure that all necessary technical and other information is correctly submitted, but the subject spectrum leasing arrangement may be implemented without waiting for such review, unless the parties to the spectrum manager leasing arrangement have requested on the form that the arrangement become effective upon Commission acceptance of the notification. Spectrum manager leasing notifications require no prior public notice before the Commission may accept them.

[117] *Id.* §§ 1.9030(a), 1.9035(a).

leasing rules. Is it necessary to revise any other existing leasing rules or add new rules to effectuate the authorization of jamming solutions in correctional facilities?

39. *Included Services*. We seek comment on the applicability of the bands currently set forth in our part 1 leasing rules as "included services,"[118] and therefore eligible for leasing, to the deployment of jamming solutions through lease arrangements. We note that many of the spectrum bands authorized in these radio services are currently being leased, in a substantial number of states, by wireless providers to CIS solutions providers to assist DOCs.[119] We seek to ensure that our approach to authorizing leasing arrangements for jamming solutions in correctional facilities does not inadvertently fail to include a relevant band deployed in commercial networks, thus creating a technical loophole for inmates to potentially exploit. Accordingly, we seek comment on whether additional bands beyond the recognized included services should be part of our proposed framework. To facilitate effective jamming solutions, how can we best ensure that new bands are incorporated into our framework if and when the Commission authorizes additional bands for commercial use by wireless providers? We also seek comment on whether a particular band or service currently specified as an included service should be excluded from a jamming solutions leasing framework and, if so, through what rationale.

40. Although our focus is removing barriers to jamming solutions that would necessarily be deployed on WRS bands commonly used in commercial networks, we also seek comment on whether there are bands not typically included in current CIS leasing arrangements that commenters believe should nonetheless be considered in authorizing jamming solutions. For example, should we include any Mobile Satellite Service (MSS) or Fixed Satellite Service (FSS) satellite bands that are authorized under part 25?[120] Is there evidence that those bands, or any other bands not listed in our part 1 leasing rules as "included services," are currently used in serving contraband wireless devices and therefore present an issue for DOCs?[121] We ask that commenters supporting inclusion of other bands for jamming solutions through leasing arrangements indicate which bands the Commission should consider as included services, and whether there is a regulatory bar that must be overcome, address any associated costs, and describe in detail the need for the operation of jamming technology in these bands in correctional facilities. We also ask commenters to consider the international treaty implications of permitting jamming solutions in satellite bands, specifically the potential for harmful interference to any foreign spacecraft that may cover the United States.

41. *Eligibility Criteria*. We find it in the public interest to propose eligibility criteria for those seeking authorization to deploy jamming solutions as a lessee under part 1 of our rules.[122] We believe that such an approach is appropriate to avoid the unwanted proliferation of jamming solutions in contexts beyond the public safety-related use in a correctional facility. As stated, we are mindful that the wireless industry has historically opposed the use of jamming technology, with a particular concern regarding the ability to contain a jamming signal to correctional facility premises, and/or that entities unrelated to DOCs might also seek Commission authorization for a jamming solution in other contexts. We believe that proposing strict eligibility restrictions is vital to ensure that use of jamming solutions is on a limited scale for a very specific public safety purpose. We also seek comment on whether, in the interest of maintaining technological neutrality and harmonizing procedures across CISs, we should

[118] *Id.* § 1.9005 (setting forth a list of various services to which leasing policies and rules apply, which includes "Wireless Radio Services in which commercial or private licensees hold exclusive rights ….").

[119] *See, e.g.,* FCC, *CIS Lease Agreements by Correction Facility*, https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices/cis-lease-agreements (last visited Sept. 3, 2025).

[120] *See generally* 47 CFR pt. 25.

[121] We separately seek comment below on how to authorize such part 25 operations in a jamming solutions context. *See infra* para. 119.

[122] *See generally* 47 CFR pt. 1, subpt. X.

require the eligibility criteria set forth below for all CIS leases. Our current streamlined leasing procedures require a solutions provider seeking to lease spectrum for MAS and/or detection systems to include in their application a brief description of the system sufficient for staff to determine that the lease is in fact for a CIS.[123] Should we build upon and strengthen our current approach and therefore apply the criteria set forth below for all CIS leases, including those for jamming solutions? We seek comment on whether to take such an expanded approach.

42. We propose that an entity will be eligible for authorization to engage in jamming solutions through a leasing arrangement if it is: (1) a DOC with authority over the correctional facility for which the lease is sought; or (2) a solutions provider that has entered into a contract with a DOC with authority over the correctional facility for which the lease is sought. We also propose that the applicant is required to provide a certification as an attachment to the FCC Form 608 stating that the applicant: (1) is eligible for authorization to engage in jamming solutions; and (2) seeks to deploy equipment that has a valid part 2 equipment authorization, as discussed below.[124] Should we require, as a condition of the lease, that the lessee must deploy the specific equipment in its jamming solution that it certified in its attachment has a valid part 2 equipment authorization, without substitution or modification? Should we require that entities seeking authority to operate transmitters as part of a jamming solution provide proof of the contractual arrangement with the correctional facility by, for example, including a copy of the contract with any lease filing? Would it be in the public interest to require disclosure of any particular lease terms to the Commission in the application process, subject to any appropriate protections sought for proprietary information under current rules?[125] We seek comment on the above approach to establishing the requisite eligibility criteria to lease spectrum for purposes of deploying a jamming solution in a correctional facility.

43. We seek comment on whether to expressly include wireless provider licensees as entities eligible to provide jamming solutions through lease arrangements, which in certain circumstances might include the need to lease spectrum from another wireless provider in the limited geographic area of a correctional facility to achieve a comprehensive spectrum solution. Are wireless providers interested in, independent of leasing to DOCs/solutions providers, directly participating in resolving this public safety issue by entering into a contract with a DOC for the purpose of operating a jamming system within a correctional facility? To the extent wireless provider licensees seek to operate transmitters that provide jamming solutions, we seek comment on whether such licensees should be subject to the same or similar requirements proposed herein for DOCs and solutions providers that provide jamming solutions.

44. We also seek comment on whether we should consider, as an eligibility criterion, a geographical component regarding the location of a correctional facility. For example, should we first take a measured approach, perhaps limiting eligibility for authorization of jamming solutions to DOCs/solutions providers seeking jamming solutions in correctional facilities located in rural areas? Would excluding from a lease authorization structure arrangements with DOCs/solutions providers seeking solutions for more densely-populated areas reduce the potential for harmful interference to authorized devices, given the challenges presented in managing RF technologies in certain environments? Such an approach might permit the Commission and key stakeholders to acquire experience with jamming technology and its potential impacts before possible expansion of the framework, but would prevent a segment of correctional facilities from near-term implementation of an additional tool to combat

[123] *See Contraband First R&O*, 32 FCC Rcd at 2350, para. 33 (establishing the Commission expectation that parties to a lease would include in their applications a brief description of their system sufficient to establish that the proposed lease is for a CIS in a correctional facility); *id*. at 2350, paras. 33-34 (noting that the Commission would establish internal procedures to ensure that qualified spectrum lease filings for CIS are identified and properly handled under the streamlined process).

[124] *See infra* paras. 120-24.

[125] *See* 47 CFR § 0.459.

contraband wireless device use. Are DOCs primarily interested in jamming solutions for rural facilities, or do they seek to deploy in urban/suburban areas as well? Should DOCs/solutions providers first be required to demonstrate that a proposed solution can be sufficiently targeted so as to not impact authorized users, particularly in a less rural environment? What are the costs and benefits of taking an incremental approach? If we were to initially limit eligibility for authorization of jamming technology to rural correctional facilities, how should we define "rural," given that the Commission has defined this term in different ways depending on context.[126] If we were to limit eligibility to deploy jamming solutions based on geographic considerations, how should we treat suburban areas? To what extent would authorizing jamming solutions in non-rural areas be problematic, or are DOCs/solutions providers committed to properly engineering, maintaining, and updating the network as necessary to avoid causing harmful interference to non-contraband devices located either within or outside the correctional facility located in such areas? We believe that the above proposed eligibility restrictions will achieve the key public interest benefit of authorizing jamming solutions only in correctional facilities. We seek comment on our proposed eligibility restrictions, including whether we should consider any other means of limiting access to authorized jamming solutions.

45. *Good Faith Negotiations.* We propose to adopt a good faith negotiation rule—akin to current section 20.23(a) of the Commission's rules[127]—that would require wireless providers to engage in good faith lease negotiations with eligible entities seeking to deploy a jamming solution in a correctional facility.[128] Section 20.23(a) requires that "CMRS licensees must negotiate in good faith with entities seeking to deploy a Contraband Interdiction System (CIS) in a correctional facility."[129] In the *Contraband First R&O*, the Commission emphasized that "the effectiveness of CIS deployment requires all carriers in the relevant area of the correctional facility to execute a lease with the CIS provider," and thus, "if one CMRS licensee in the area fails to engage in lease negotiations in a reasonable time frame or at all, the CIS solution will not be effective."[130] The Commission allowed CIS providers to seek Special Temporary Authority (STA) to operate if unable to reach an agreement with the commercial mobile radio service (CMRS) licensee after a 45-day period of good faith negotiation on the part of the solutions provider, coupled with lack of good faith on the part of the wireless provider.[131]

---

[126] *See*, *e.g.*, *Facilitating the Provision of Spectrum-Based Services to Rural Areas and Promoting Opportunities for Rural Telephone Companies to Provide Spectrum-Based Services, et al*, WT Docket No. 02-381, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 19078, 19087, para. 11 (establishing a baseline definition of "rural area" as those counties with a population density of 100 persons per square mile or less, based upon the most recently available Census data); *Partitioning, Disaggregation, and Leasing of Spectrum*, WT Docket No 19-38, Report and Order and Second Further Notice of Proposed Rulemaking, 37 FCC Rcd 8825, 8838, para. 43 (adopting a statutory definition of "rural area" from the MOBILE NOW Act for the Commission's Enhanced Competition Incentive Program, which is defined as any area except (1) a city, town, or incorporated area that has a population of more than 20,000 inhabitants; or (2) an urbanized area contiguous and adjacent to a city or town that has a population of more than 50,000 inhabitants). *See also* 47 CFR § 1.60001(d).

[127] 47 CFR § 20.23(a). This rule section refers to wireless providers as "CMRS licensees," as the part 20 rules apply only to CMRS licensees and that is also the typical regulatory status of such licensees. *Id.*

[128] *See* Appx. A (proposed rule 1.9041).

[129] 47 CFR § 20.23(a).

[130] *See Contraband First R&O*, 32 FCC Rcd at 2360-61, para. 63.

[131] *See id.*; 47 CFR § 20.23(a) (". . . Upon receipt of a good faith request by an entity seeking to deploy a CIS in a correctional facility, a CMRS licensee must negotiate toward a lease agreement. If, after a 45 day period, there is no agreement, CIS providers seeking Special Temporary Authority (STA) to operate in the absence of CMRS licensee consent may file a request for STA with the Wireless Telecommunications Bureau (WTB), accompanied by evidence demonstrating its good faith, and the unreasonableness of the CMRS licensee's actions, in negotiating an agreement. The request must be served on the CMRS licensee no later than the filing of the STA request, and the CMRS licensee may file a response with WTB, with a copy served on the CIS provider at that time, within 10 days (continued….)

46. Today, to ensure wireless provider cooperation for this key public safety purpose, we propose to require a wireless provider to engage in good faith negotiations with a DOC, or with a solutions provider that has executed a contract with a DOC, that seeks Commission authorization to deploy a jamming solution in a correctional facility via a leasing arrangement. If, after a 45-day period, there is no good faith agreement,[132] we propose that the DOC/solutions provider may apply for a non-exclusive overlay license, as discussed below. By facilitating the implementation of additional tools for DOCs/solutions providers, including jamming solutions, we seek to incentivize secondary markets transactions that feature the involvement and cooperation of wireless providers. Because wireless providers that fail to negotiate in good faith toward a leasing arrangement would not be eligible for our proposed safe harbor, as noted above, the Commission potentially could take enforcement action for possible unauthorized operation of contraband wireless devices in a correctional facility in violation of section 301 of the Act and our proposed amended rule section 1.903(c).[133] We anticipate that the prospect of such a consequence could further incentivize wireless providers to negotiate in good faith and rely on our preferred leasing approach when responding to DOC/solutions provider requests for jamming solutions. Although below we propose to provide an overlay license fallback approach to leasing arrangements, we recognize that there may be instances where stakeholders fail to reach a lease agreement due to the bad faith of *either* party. To provide proper incentives for stakeholders on either side of a transaction, we propose that DOCs and their contracted solutions providers also are subject to a good faith negotiation requirement to discourage sham negotiations undertaken to avoid the Commission-preferred leasing process in favor of directly seeking what we clearly intend as a fallback overlay authorization.

47. We seek comment on this proposal and whether we should revise our approach. We believe that common considerations exist in negotiating lease agreements for existing CISs and proposed jamming solutions in a correctional facility environment. Are there additional distinguishing factors in play with respect to negotiating leases for the deployment of jamming solutions, thus necessitating a negotiation period lengthier than 45 days? We note that the Commission, in the *Contraband First R&O*, did not specifically define the term "good faith negotiations" as it specifically pertains to section 20.23(a), but instead provided "factors to be considered when determining whether there is good faith."[134] We seek comment on whether and how we should specifically define "good faith negotiations" or elaborate on relevant factors to be considered in making the determination. Are the same factors relevant for lease

(Continued from previous page)
of the filing of the STA request. If WTB determines that the CIS provider has negotiated in good faith, yet the CMRS licensee has not negotiated in good faith, WTB may issue STA to the entity seeking to deploy the CIS, notwithstanding lack of accompanying CMRS licensee consent.").

[132] As used throughout this *Third Further Notice*, by lack of a "good faith agreement" or lack of a "good faith leasing arrangement," we mean that when there is no agreement, there is evidence the entity seeking to deploy a jamming solution negotiated in good faith, and there is evidence the CMRS licensee negotiated in bad faith. *See* Appx. A (proposed rule 1.9041(e)).

[133] *See supra* paras. 31-34; Appx. A (proposed amendment to rule 1.903(c)).

[134] *Contraband First R&O*, 32 FCC Rcd at 2360-61, para. 63 n.216 (citing 47 CFR §§ 90.677(c) (for mandatory relocation negotiations, factors relevant to a good faith determination include: whether the party has made a bona fide offer to relocate the incumbent to comparable facilities, the steps the parties have taken to determine the actual costs of relocation, and whether either party has unreasonably withheld information requested by the other party that is essential to accurate estimations of costs and procedures), 76.65(b) (violations of the duty to negotiate in good faith may include: refusal by an entity to negotiate, refusal to designate a representative with authority to make binding representations, acting in a manner that unreasonably delays negotiations, refusal to put forth more than a single, unilateral proposal, and failure to respond to a proposal)). The Commission further noted that "[h]ere, such factors might also include whether the parties entered into timely discussions while providing appropriate points of contact, whether a model lease with reasonable terms was offered, etc." and "the Commission may take additional steps as necessary to authorize CIS operations should we determine there is continued lack of good faith negotiations toward a CIS lease agreement." *Id.* at 2360-61, para. 63.

negotiations to operate base station transmitters as part of a jamming solution? If not, we ask commenters to propose factors for possible incorporation into a Commission rule. Stakeholders should specifically address the questions above, as well as provide comments on the costs and benefits of the proposed approach and any alternatives.

48. *Technical Rules*. To provide flexibility for stakeholders and maintain consistency with our current CIS leasing approach, we propose to apply to jamming solutions in correctional facilities our current secondary markets approach to compliance with technical rules. Accordingly, an entity seeking to deploy a jamming solution in a correctional facility would enter into a part 1 leasing arrangement(s) with a wireless provider to operate on the provider's licensed frequencies. Under our leasing rules, a lessee would be subject to the same technical limits as the lessor, as set forth in band-specific radio service rules (e.g., complying with power limits and out-of-band emission limits to protect adjacent band licensees).[135] A DOC or solutions provider seeking to use a jamming solution would therefore be required to comply with a variety of, and possibly differing, technical rules that are set forth under various parts of the Commission's rules governing spectrum typically used in commercial wireless networks, including, for example, parts 22, 24, 27, 30, and 96.

49. As in the current CIS leasing context, we generally believe that parties to a lease arrangement are best positioned to agree on technical details that not only comply with the technical limits of various applicable radio service rule parts, but that address the potential for harmful interference to a lessor's licensed operations from the lessee's operations limited to a particular correctional facility. Although our rules specify technical limits that are not to be exceeded, we anticipate that a lessor wireless provider will include contractual provisions that address its lessee's operational parameters and obligations. We recognize that wireless providers often deploy commercial networks at less than the maximum radiated power afforded under our rules,[136] both for engineering and cost reasons. Accordingly, today's MAS solutions providers that operate in the very limited geographic area of a correctional facility also typically use a fraction of the radiated power afforded to wireless providers under the service rules applicable to a spectrum band used in commercial deployments. We note that these reduced parameters may be reflected in contract provisions between stakeholders that establish alternative limits to the maximum levels reflected in our technical rules.

50. We seek comment on whether the introduction of jamming solutions, even when authorized through leasing arrangements negotiated at arms-length, requires a stricter regulatory framework from a technical perspective than our current maximum levels set forth across various service rules to best ensure that authorized wireless devices are not subjected to harmful interference. We request that commenters provide detailed analysis in support of any proposed alternative technical parameters. If such rules are needed, what are appropriate technical parameters to govern jamming deployments through leasing in a correctional facility environment? Should we establish more restrictive technical limits for jamming solutions than those established for wireless provider commercial operations in flexible use bands?[137] Should we require a DOC or solutions provider lessee to use narrowly tailored means to

---

[135] *See* 47 CFR §§ 1.9020(b)-(d) (spectrum manager leasing arrangements), 1.9030(b)-(d) (long-term *de facto* transfer leasing arrangements), 1.9035(b)-(d) (short-term *de facto* transfer leasing arrangements).

[136] Although the Commission permits an effective radiated power (ERP) of up to 500 watts per channel, depending on the tower height, the majority of cellular or PCS cell sites in urban and suburban areas operate at an ERP of 100 watts per channel or less. *See* FCC, *Human Exposure to Radio Frequency Fields: Guidelines for Cellular Antenna Sites*, (Oct. 15, 2019) https://www.fcc.gov/consumers/guides/human-exposure-radio-frequency-fields-guidelines-cellular-and-pcs-sites. We find that this is the case even where our rules in certain radio service permit even higher power levels, for example, up to 1640 watts/MHz in Broadband PCS. *See* 47 CFR § 24.232.

[137] We note that Australia has required more stringent OOBE limits for jamming operations permitted at two correctional facilities both in New South Wales: the Goulburn Correctional Complex in Goulburn and the Lithgow Correctional Centre in Marrangaroo. *See* Australian Government, Federal Register of Legislation, *Radiocommunications (Exemption – Corrective Services NSW) Determination 2021*, (Mar. 31, 2025)

(continued….)

achieve the goal of combatting contraband wireless device use, which will vary from a technical perspective, depending on the particular correctional facility? For example, should we prohibit use of a jamming solution across an entire 5G band(s), some with bandwidths as large as 100 MHz, where a jamming solution could be targeted on the control channel portion of a band? We seek comment on how to implement a narrowly tailored jamming solution, while balancing the cost tradeoffs associated with deploying an effective solution that does not cause harmful interference to authorized users. To what extent would a measured approach decrease the risk of harmful interference, increase efficiencies, and impact the overall costs of deploying a jamming solution?

51. Further, we seek comment on how DOCs, as the primary advocates for additional tools to combat contraband wireless device use, intend to deploy jamming solutions to avoid harmful interference to wireless provider networks in a manner that accounts for differences in how commercial wireless networks are deployed, for example, the use of time division duplexing (TDD) versus frequency division duplexing (FDD).[138] Should we require those seeking to deploy jamming solutions to adjust their technical parameters based on the specific technology the wireless providers use to provide a signal that covers a correctional facility? To what extent should we adopt technical rules applicable to jamming solutions that distinguish between the potential for harmful interference in bands using FDD versus those using TDD? Or, in a leasing scenario, should any such distinctions be addressed solely through leasing arrangements and the underlying contractual agreements between wireless providers and solutions providers? Are specific measures needed to prevent harmful interference to a wireless provider's base stations in a TDD context, for example taking into consideration the desired v. undesired signal levels in a TDD pattern? Should we require, in a TDD context, synchronization between a solutions provider deploying a jamming solution and the wireless provider offering service to an area that includes a correctional facility to avoid unwanted transmissions during the wireless provider's base station transmit timeslot? Are different considerations raised where a jamming solution is deployed in bands using FDD and seeks to cause interference to the contraband wireless device's ability to receive a base station's downlink transmissions?

52. To minimize the risk of harmful interference to authorized users, should we set specific limits on: radiated power (e.g., limiting transmitter output power to 1-watt or 5-watt maximum) or power spectral density[139] per band, out-of-band emission (OOBE) limits, field strength limit at a correctional facility boundary, power flux density (PFD) limit measured at a certain point from a transmitter, and/or Signal to Interference Noise Ratio (SINR) at the boundary of proposed jamming operations? Are more stringent restrictions required, in particular PFD or OOBE limits, in order to protect authorized operations outside of the boundary of the leased service area and users of immediately adjacent or nearby frequency bands? If so, what are the appropriate limits? If we impose more restrictive limits, would the efficacy of the jamming solution be compromised? Would providers of jamming solutions find it necessary to internalize a guard band to comply with our technical rules? Would adopting stricter limitations on

(Continued from previous page)
https://www.legislation.gov.au/F2021L01613/latest/text (section 10(8)(c) of the legislation states that a jamming operator must not cause radio emissions with a power spectral density greater than - 128.5 dBm/kHz on non-designated frequencies outside of a relevant facility).

[138] FDD allows simultaneous radio transmission and reception between a subscriber's device and a base station by providing two simultaneous but separate frequencies (aka channels). In a TDD system used, for example, in 3.7-4.0 GHz and the Upper Microwave Flexible Use (UMFUS) bands, a common channel is shared between the uplink (subscriber to base station transmission) and downlink (base station to subscriber transmission), with the resource being switched in time. *See Amendment of Part 27 of the Commission's Rules to Govern the Operation of Wireless Communications Services in the 2.3 GHz Band*, Order on Reconsideration, 27 FCC Rcd 13651, 13654, para. 4 n.10.

[139] *See Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27 and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, Third Report and Order, 23 FCC Rcd 5319, 5329-30, paras. 24-25 (2008) (adopting a power spectral density model by establishing equivalent isotropically radiated power (EIRP) caps on a "per megahertz of spectrum bandwidth" basis rather than on a "per emission" basis).

transmitter power levels in an effort to help prevent harmful interference to authorized users, potentially resulting in a substantial increase in the number of transmitters required to be deployed, drive up the cost of deploying and maintaining a jamming solution? Conversely, if DOCs/solutions providers seek to deploy a jamming solution that operates band-wide with multiple licensees within a band, are there any current technical rules or policies in any of the included services that might hinder operation of a jamming solution across the band that might require revision? Should any of our technical rules be more permissive to foster an effective jamming solution in the limited context of correctional facilities?

53. We seek comment on whether technical parameters should vary depending on various factors including, but not limited to: whether the deployment is in a rural, suburban, or urban location; the size of the correctional facility and the topography of the surrounding area; the materials used in constructing the facility; and the proximity of wireless provider networks in the area, including the proximity of wireless provider service to residential/office locations, highways, and the corresponding strength of those RF signals entering the correctional facility. We also seek comment on how to adequately protect public safety communications from harmful interference potentially caused by jamming solutions. Are there appropriate technical measures, including filters, that could protect first responder communications near correctional facilities that deploy a jamming solution? What agreements should be in place to prevent interference to public safety communications? In addition, we seek comment on whether additional measures would need to be in place to protect first responder and priority communications using commercial wireless spectrum, such as FirstNet, Verizon's Frontline, and T-Mobile's T-Priority. Are there other spectrum bands that support public safety communications that might require specific protection against potential harmful interference from jamming solutions?

54. We also seek comment on the potential effect of jamming solutions on the public's ability to receive Wireless Emergency Alerts (WEA), which federal, state, Tribal, territorial, and local officials rely on to send critical notifications concerning emergencies. Could the use of jamming solutions by correctional officials prevent the wireless providers that participate in WEA (Participating CMS Providers) from delivering WEAs in or near facilities employing jamming solutions? Would this result in Participating CMS Providers being unable to comply with the Commission's WEA rules, including its geographic accuracy requirements?[140] Do emergency managers have concerns that the use of jamming solutions would put the public at risk? If the use of jamming solutions did prevent the delivery of WEAs, what effect could this have on the safety of correctional officials, prisoners, and other individuals during emergencies?

55. *Solutions Providers with Existing Lease Arrangements for CIS Operation.* We recognize that some proposed eligible entities (e.g., current CIS solutions providers) have existing leases with wireless carriers to operate MAS and/or detection systems in correctional facilities across the United States. Although we propose to implement additional requirements, such as eligibility and certification requirements, for entities seeking to enter a leasing arrangement for jamming solutions, we seek to avoid adding unnecessary regulatory burdens on wireless providers and their current CIS lessees. We therefore seek comment on whether we should permit solutions providers with existing CIS leases that seek authority for jamming operations to file a lease modification application, rather than file a new FCC Form 608 for a spectrum manager or *de facto* transfer leasing arrangement. If so, what information or certifications should we require to be filed with the modification application to support the lessee's eligibility to engage in jamming operations?[141] We ask commenters to discuss the pros and cons of this

[140] *See* 47 CFR § 10.450(a) ("A Participating CMS Provider must deliver any Alert Message that is specified by a circle or polygon to an area that matches the specified circle or polygon. A Participating CMS Provider is considered to have matched the target area when they deliver an Alert Message to 100 percent of the target area with no more than 0.1 of a mile overshoot.").

[141] *See supra* para. 42 (seeking comment, for example, on whether we should require proof of the contractual arrangement with the correctional facility for jamming services).

approach, and to provide any other proposals on ways in which an existing leasing arrangement could be modified to reflect authorization of a newly proposed jamming solution.

56. *Immediate Approval Procedures.* We also seek comment on whether leases for the operation of jamming systems, consistent with our approach to CISs, should be subject to the Commission's immediate approval procedures. The Commission's rules require that the parties to a *de facto* transfer spectrum leasing arrangement file an application for approval of the lease with the Commission.[142] Parties to a spectrum manager lease must file a notification of the spectrum leasing arrangement with the Commission and can commence operations without prior Commission approval after a short period.[143] The Commission's rules provide for expedited processing (by the next business day) of all categories of spectrum leasing applications and notifications.[144] To be accepted for expedited processing, any application or notification must be "sufficiently complete," including information and certifications relating to a lessee's eligibility and qualification to hold spectrum, and lessee compliance with the Commission's foreign ownership rules.[145] *De facto* transfer spectrum leasing applications must also be accompanied by the requisite filing fee.[146] Long-term *de facto* transfer spectrum leasing applications and spectrum manager leasing notifications must meet three additional criteria for immediate approval or processing.[147] First, the lease cannot involve spectrum that may be used to provide an interconnected mobile voice and/or data service and that would result in a geographic overlap with licensed spectrum "in which the proposed spectrum lessee already holds a direct or indirect interest of 10 [percent] or more."[148] Second, the licensee cannot be "a designated entity or entrepreneur subject to unjust enrichment requirements and/or transfer restrictions under applicable Commission rules."[149] Finally, the spectrum leasing arrangement cannot "require a waiver of, or declaratory ruling pertaining to, any applicable Commission rules."[150]

57. In the *Contraband First R&O*, the Commission determined that qualifying long-term *de facto* transfer spectrum leasing applications and spectrum manager leasing notifications for CISs would be subject to immediate processing and approval.[151] The Commission reasoned that because these

[142] 47 CFR §§ 1.9030(a), (e), 1.9035(a), (e).

[143] *Id.* § 1.9020(e)(1). Under general notification procedures, spectrum manager leases for more than one year must be filed at least 21 days prior to the date of operation. *Id.* § 1.9020(e)(1)(ii). Spectrum manager leases of one year or less must be filed at least 10 days prior to the date of operation. *Id*. § 1.9020(e)(1)(ii). We note that under immediate approval processes, acceptance of the notification will be reflected in ULS on the next business day following the day the application is filed, and spectrum manager lessees may operate upon acceptance consistent with the terms of the leasing arrangement. *Id.* § 1.9020(e)(2)(ii).

[144] *Id.* §§ 1.9020(e)(2)(iii), 1.9030(e)(2)(iii), 1.9035(e)(2); *see also Second Secondary Market Report and Order*, 19 FCC Rcd at 17512, para. 14 n.42 ("[U]nder the immediate approval process, spectrum leasing parties must submit qualifying applications and include the requisite filing fees. The [Wireless Telecommunications] Bureau will then process the application overnight and . . . indicate in our Universal Licensing System (ULS) that the application has been approved."). Applications and notifications are filed on FCC Form 608, "FCC Application or Notification for Spectrum Leasing Arrangement." 47 CFR § 1.913(a)(5).

[145] 47 CFR §§ 1.9020(e)(1)(i), (e)(2)(i), 1.9030(e)(1)(i), (e)(2)(i), 1.9035(e)(1).

[146] *Id.* §§ 1.9030(e)(1)(i), (e)(2)(i), 1.9035(e)(1); *see also id.* § 1.9020(e)(1)(i).

[147] *Id.* §§ 1.9020(e)(2)(i)(A)-(D), 1.9030(e)(2)(i)(A)-(D). All short-term *de facto* transfer spectrum leasing applications are processed via immediate approval procedures. *See id.* § 1.9035(e).

[148] *Id.* §§ 1.9020(e)(2)(i)(A), 1.9030(e)(2)(i)(A).

[149] *Id.* §§ 1.9020(e)(2)(i)(B), 1.9030(e)(2)(i)(B).

[150] *Id.* §§ 1.9020(e)(2)(i)(C), 1.9030(e)(2)(i)(C). Short-term *de facto* lease applications must also meet this requirement. *Id.* § 1.9035(e)(1).

[151] *See Contraband First R&O*, 32 FCC Rcd at 2348, para. 28.

"qualifying spectrum leases for CISs do not raise the potential public interest concerns that would necessitate prior public notice or more individualized review, we believe that removing this unnecessary layer of notice and review is appropriate."[152] We seek to harmonize our CIS leasing rules to accommodate jamming solutions within the framework where feasible. As our proposed revised definition of CIS in our leasing rules would include jamming solutions, qualifying leases for jamming solutions in correctional facilities would be subject to immediate processing and approval. We seek comment on whether this is the appropriate approach for these types of lease applications. We also seek comment on whether there is a compelling reason to exclude leasing arrangements for jamming solutions from immediate processing procedures. Commenters supporting such an exclusion are requested to provide details regarding why an application for lease of spectrum for deployment of a jamming solution, if otherwise complete and meeting the Commission's requirements, would necessitate lengthier Commission review than that of current CIS lease arrangements subject to expedited processing.

58. *Regulatory Status.* In the *Contraband First R&O*, the Commission explained that when a CIS provider enters into a spectrum lease agreement with a wireless provider with a CMRS regulatory status, the regulatory status of the lessor applies to the lessee, and the lessee would be subject to common carrier obligations, unless it specifically sought a change in regulatory status.[153] In addition, a change in status at that time required the filing of a modification application to be placed on a 30-day public notice.[154] To reduce burdens and expedite the leasing process for CISs, the Commission waived this requirement for CIS operators, finding it appropriate to permit a CIS operator to indicate in the exhibit to its lease application whether it is PMRS or CMRS for regulatory status purposes, and the approved or accepted spectrum lease would subsequently reflect that regulatory status.[155] The Commission granted a waiver of section 20.9 of its rules at that time, rather than amend the rule, because there was a pending proceeding to eliminate the rule altogether.[156] The waiver enabled CIS operators to be treated as PMRS without having to file a modification application with the Commission.

59. We believe that a PMRS presumption is most applicable to eligible DOCs/solutions provider entities seeking to deploy jamming solutions, which we understand are not intended to provide a service that meets the CMRS definition.[157] We therefore seek comment on applying the PMRS presumption to all spectrum leasing arrangements entered into for the provision of jamming solutions,

[152] *Id.* The Commission determined that it would permit CIS leases to be subject to immediate approval processes, even where a solutions provider has a clear spectrum overlap by leasing spectrum from several wireless providers in the same geographic area that would otherwise make an applicant ineligible for immediate approval procedures pending review of mobile spectrum holdings. The Commission found that the typical competition concerns were not present in the CIS context and acknowledged that "CISs are not providing service to the public and generally there is only one CIS provider in a particular correctional facility." *Id*. at 2348, para. 29.

[153] *Id.* at 2351, para. 36; *see* 47 U.S.C. § 332(c)(1).

[154] *Contraband First R&O*, 32 FCC Rcd at 2351, para. 36.

[155] *Id.* at 2352, para. 39 n.130 ("Pursuant to our streamlined leasing process, spectrum leasing parties seeking a lease for a CIS in a correctional facility will include a brief description of the CIS sufficient to enable the Commission staff to determine that the lease is in fact for a CIS. In this submission, the parties will also identify whether they request PMRS or CMRS regulatory status."); *see also* FCC Form 608, Main Form, at 2-3.

[156] *Contraband First R&O*, 32 FCC Rcd at 2352, para. 39. In 2019, the Commission removed section 20.9 from its rules, eliminating the requirement that CIS operators file a separate modification application to reflect PMRS regulatory status. *See Amendments to Harmonize and Streamline Part 20 of the Commission's Rules Concerning Requirements for Licensees to Overcome a CMRS Presumption*, Report and Order, 32 FCC Rcd 10731, 10737-10739, paras. 14-18 (2017).

[157] 47 CFR § 20.3 (defining "commercial mobile radio service"). *See also id.* (defining "private mobile radio service" as "[a] mobile service that meets neither paragraph (a) nor paragraph (b) definitions of commercial mobile radio service set forth in this section. A mobile service that does not meet the paragraph (a) definition of commercial mobile radio service in this section is presumed to be a private mobile radio service . . .").

unless the lessee includes an exhibit to its lease application indicating that it is CMRS for regulatory status purposes, thereby aligning the treatment of regulatory status for jamming solutions with other CIS operations, e.g., MAS and detection systems. We ask that commenters discuss the costs and benefits of applying the same approach to assigning regulatory status to entities seeking to provide jamming solutions via leasing arrangements as that which the Commission adopted in the *Contraband First R&O*.

60. *911-Related Leasing Rules.* We seek comment on the possible effects on wireless emergency/911 calls and public safety communications of the deployment of jamming solutions in correctional facilities as contemplated in this *Third Further Notice*. As the Commission's Public Safety and Homeland Security Bureau (PSHSB) has generally noted, "[w]ireless 9-1-1 calls and public safety communications are put at risk by the use of jamming devices" and public safety organizations have expressed concerns with the potential for cell jammers to block 911 calls and disrupt critical public safety radio communications.[158] Section 9.10 of the Commission's rules mandates that CMRS 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.[159] The requirement to transmit 911 calls from non-service-initialized phones was adopted based on the Commission's determination that user validation procedures could cause a dangerous delay or interruption of the 911 assistance process.[160] Importantly, however, the Commission has afforded Public Safety Answering Points (PSAPs) the discretion *not* to accept 911 calls transmitted from a CIS provider at a correctional facility.[161] Further, under current Commission rules, a 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.[162]

61. Section 9.10 of the Commission's rules sets forth 911 requirements applicable to CMRS providers, including requirements to support basic 911 and Enhanced 911 (E911), outdoor and indoor location accuracy, and text-to-911.[163] In the *Contraband First R&O*, the Commission agreed with commenters that delivering emergency calls to PSAPs facilitates public safety services and generally serves the public interest, and acknowledged the overriding importance of ensuring availability of emergency 911 calls from correctional facilities.[164] The Commission then amended its rules to require CIS providers regulated as PMRS to route all 911 calls to the local PSAP, and clarified that the CIS

[158] *See* Putting an End to Illegal Cell Phone Use in Prisons, FCC Public Safety and Homeland Security Bureau (2010), https://transition.fcc.gov/pshs/docs/summits/Combating-Contraband-Cell-Phones-in-Prison-Handout-v4.pdf (PSHSB 2010 Handout). The handout also states that "[s]tate communications officials have expressed concern about jammers bleeding interference outside the prison and disrupting police and firefighter frequencies which are close to cell phone frequencies." *Id*. at 2. *See also* NPSTC 2020 Comments at 3; Association of Public-Safety Communications Officials-International, Inc. (APCO) Comments, WT Docket 13-111, at 2 (Sept. 16, 2020) (cell signal jammers placed within a correctional facility could block a legitimate call to 911 and interfere with the wireless communications of first responders).

[159] *See* 47 CFR § 9.10(b).

[160] *See Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102, Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 18676, 18692-93, paras. 31-32 (1996). 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).

[161] *See* 47 CFR § 9.10(r).

[162] *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*, PS Docket No. 08-51, Notice of Proposed Rulemaking, 30 FCC Rcd 3449, 3451-52, para. 5 (2015).

[163] *See* 47 CFR § 9.10.

[164] *Contraband First R&O*, 32 FCC Rcd at 2353-54, para. 44.

provider, not the CMRS wireless provider licensee, is responsible for passing through E911 calls to the PSAP, unless the PSAP indicates it does not want to receive such calls.[165] The Commission found that this overall approach to 911 call forwarding was consistent with the Commission's guidance clarifying that the 911 rules requiring mobile wireless carriers to forward all wireless 911 calls to PSAPs, without respect to the call validation process, and does not preclude carriers from blocking fraudulent 911 calls from non-service initialized phones pursuant to applicable state and local law enforcement procedures.[166]

62. Our understanding is that jamming solutions block calls on all affected frequencies and, unlike MAS, are unable to allow 911 calls to be transmitted to a PSAP. We seek comment on whether it is in fact technically infeasible for the operator of any type of jamming solution to satisfy, under any circumstances, the 911-related requirements in part 1 and section 9.10 of the Commission's rules. Commenters citing a technical inability to comply with these rules should describe which particular requirements are not feasible and why. We ask that commenters provide details regarding any scenario where a jamming system, including any type of system under development, could be deployed in a correctional facility in a way that permits the transmission of 911 calls to a PSAP.

63. Although we separately seek comment below on the treatment of 911 for jamming operations in an overlay licensing context,[167] we seek comment from stakeholders on how emergency calls from wireless devices are addressed today in a correctional facility environment. We are aware that some state DOC officials have indicated that correctional facilities typically do not allow *any* calls from within, including emergency calls.[168] In contrast, we seek comment as to how 911 calls are routed today if made from an authorized phone that might be used, for example, by counsel during visitation or by a vendor serving the premises that requires emergency services. Are such calls routed to a local PSAP or to internal DOC personnel, including perhaps internal DOC firefighting and/or medical personnel? Are such calls handled differently if made from an inmate using a contraband wireless device? To what extent have PSAPs opted to not receive calls from correctional facilities regardless of whether the source of the call is authorized by the correctional facility? We seek comment on the effect, if any, that the deployment of jamming solutions within a correctional facility, resulting from our proposed deauthorization of subscriber operation of contraband wireless devices, would have on emergency calls made from within or in the immediate vicinity of a correctional facility.

64. Based on the record in this proceeding thus far, including our assumption that current jamming solutions are not capable of permitting impacted calls to reach a PSAP, we seek comment on the prospect of not applying the Commission's 911 and E911 rules to entities that have entered into leasing arrangements for the provision of jamming solutions in correctional facilities, if ultimately regulated as PMRS, whether it be a DOC directly or through its contracted solutions provider. We recognize that this approach contrasts with current E911 transmission regulations for CIS lessees, but would take into

---

[165] *See id.* at 2353-54, paras. 44-46; *see also* 47 CFR §§ 1.9020, 1.9030, and 1.9035.

[166] *See Contraband First R&O*, 32 FCC Rcd at 2354, para. 46 n.152 (citing *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 In the Matter of 911 Call-Forwarding Requirements for Non-Service Initialized Phones*, Notice of Proposed Rulemaking, 30 FCC Rcd 3449 (2015)).

[167] *See infra* para. 87 (seeking comment on proposed part 90 overlay licensee 911 obligations).

[168] *See*, *e.g.*, FCC, Workshop on Contraband Cell Phone Use in Prisons, Transcript at 16 (2010), https://www.fcc.gov/news-events/events/2010/09/workshopwebinar-on-contraband-cell-phone-use-in-prisons ("there are no legal cell phone calls on prison property in South Carolina. None. There are no legal 911 calls. There are no legal calls home. There are no legal emergency calls because it is against the law."); Comments of South Carolina Department of Corrections, WT Docket No. 09-30, at 2 (rec. Mar. 16, 2009) ("In all our facilities and in most other correctional institutions the mere possession, let alone use, of a cell phone by inmates, staff or visitors is illegal. Thus any jamming solely within such an institution will not lead to disruptions of calls to 9-1-1 or any other call by law abiding users.").

consideration both the potential limitations and intended purpose of jamming solutions, as well as the potential realities of current 911 call treatment in the correctional facility environment upon which we seek comment today. To the extent jamming solutions are included in our proposed revised definition of CIS, we seek comment on whether it is necessary to modify existing leasing rules related to the provision of 911 service in the context of CIS leasing.[169] Finally, as stated, we are not aware of a CMRS wireless provider currently providing CIS in a correctional facility through a contract with a DOC. We again seek comment on how to treat a CMRS wireless provider, for 911 regulatory purposes, that opts to deploy base stations as part of a jamming solution, if the developing record indicates wireless provider interest in participating at that direct level to address this public safety issue. If so, what rule revisions are necessary to reflect the apparent technical limitations of jamming solutions, if deployed directly by wireless providers, with respect to passage of 911 calls to PSAPs?

65. *Interference-Related Leasing Rules.* We seek comment on leasing rules and the issue of potential interference to non-contraband, authorized devices within a correctional facility and/or interference to authorized devices outside of the correctional facility perimeter. Our current leasing rules require all lessees to comply with rules requiring responsibility for ensuring non-interference with co-channel and adjacent channel licensees applicable to the lessor/licensee under the license.[170] However, primary responsibility for such compliance depends on the type of lease. For example, under a spectrum manager lease, the lessor/licensee has "direct responsibility and accountability for ensuring that their spectrum lessees comply with [the interference-related service] rules, including responsibility for resolving all interference disputes."[171] In contrast, under a *de facto* transfer lease, the spectrum lessee has primary responsibility for ensuring compliance with the Commission's policies and rules, including interference rules applicable to the lessor/licensee.[172] Thus, in the event of a harmful interference scenario under a *de facto* transfer lease, the "Enforcement Bureau will first approach the authorized spectrum lessee, and the lessee will be expected to bring its operations into compliance with the Commission's requirements."[173] We seek comment on whether to retain this existing hierarchy of responsibility in the context of a proposed framework that would authorize jamming solutions in correctional facilities. Does our proposal to permit jamming solutions in such a limited context warrant revisions to our rules relating to interference resolution? In the case of a spectrum manager lease under our proposed jamming authorization framework, is it practical and appropriate for direct responsibility and accountability to apply to the licensee/lessor, where unwanted harmful interference would likely be to the licensee/lessor's authorized subscribers? Commenters seeking a rule revision are requested to address how this risk differs from that currently existing with deployment of transmitters for MAS and detection systems. Should we specify in the jamming solutions context that the lessee is primarily responsible for interference resolution caused by its jamming operations?

---

[169] *See, e.g.,* 47 CFR §§ 1.9020(d)(8) (under spectrum manager leases "[i]f E911 obligations apply to the licensee (see § 9.10 of this chapter), the licensee retains the obligations with respect to leased spectrum."), 1.9030(d)(8) (under long-term de facto transfer leases, "to the extent the licensee is required to meet E911 obligations (see § 9.10 of this chapter), the spectrum lessee is required to meet those obligations with respect to the spectrum leased under the spectrum leasing arrangement insofar as the spectrum lessee's operations are encompassed within the E911 obligations."), 1.9035(d)(4) (under short-term de facto transfer leases: "[i]f E911 obligations apply to the licensee (see § 9.10 of this chapter), the licensee retains the obligations with respect to leased spectrum. A spectrum lessee entering into a short-term de facto transfer leasing arrangement is not separately required to comply with any such obligations in relation to the leased spectrum.").

[170] *See id.* §§ 1.9010(b)(1)(ii), 1.9020(d)(1), 1.9030(d)(1), 1.9035(d); *see also Secondary Markets R&O*, 18 FCC Rcd at 20665, para. 142.

[171] *Secondary Markets R&O*, 18 FCC Rcd at 20653, para. 108.

[172] *Id.* at 20664, 20675, paras. 137, 172-73.

[173] *Id.* at 20664, para. 138.

66. *Community Notification.* The Commission's rules require a CIS operator to notify the community in which the correctional facility is located 10 days prior to deploying a CIS that prevents communications to or from mobile devices, or that obtains identifying information from the device.[174] We seek comment on whether we should apply the community notification requirement to deployments of jamming solutions, to the extent that jamming solutions are proposed to be included within a revised definition of CIS for purposes of part 1 leasing arrangements. We also seek comment on whether the existing notification requirement has been effective in contributing to corrective action by DOCs in cases, if any, where users outside of the correctional facility were negatively impacted. Conversely, are there relevant DOC security reasons for not mandating such a notification requirement, or perhaps eliminating the current notification requirement applicable to CIS? Is it in the public interest to continue to require inherently sensitive information regarding the status of CIS deployments, specifically focused on preventing contraband wireless device use, to be made publicly available, where inmates potentially are able to obtain real-time updated deployment information on a per-facility basis nationwide?

67. *Notification to Solutions Providers of Wireless Provider Technical Changes.* In the *Contraband Second R&O*, the Commission adopted rules requiring advance notice from wireless providers to MAS operators of certain technical changes to the wireless providers' networks.[175] Specifically, the Commission adopted rules requiring CMRS wireless provider licensees leasing spectrum to MAS 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.[176] The Commission also adopted an exception to this requirement where the technical changes are required due to emergency and disaster preparedness.[177] In adopting this notice requirement, the Commission reasoned that "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."[178] We anticipate that jamming solutions providers may face virtually identical network engineering challenges as those presented for deployment of MAS. We therefore seek comment on applying to wireless providers the advance notification rule to assist jamming system operators in maintaining the effectiveness of jamming solutions deployed in a correctional facility. What are the costs and benefits of applying our current notification structure to jamming solutions? Are there differences in the operation of MAS compared to jamming solutions that would necessitate amendments to our current advance notification criteria?

68. *Length of Lease.* Under the Commission's rules, the term of a spectrum leasing arrangement may not be longer than the term of the underlying lessor's license.[179] However, a licensee and spectrum lessee that have entered into an arrangement with a term continuing to the end of the current license authorization may, contingent on the Commission's grant of the license renewal, extend the

[174] *See* 47 CFR §§ 1.9020(n); 1.9030(m), 1.9035(o).

[175] *See Contraband Second R&O*, 36 FCC Rcd at 11838-43, paras. 63-74; *see also* 47 CFR § 20.23(d).

[176] *See Contraband Second R&O*, 36 FCC Rcd at 11838-39, para. 74; *see also* 47 CFR § 20.23(d)(1).

[177] *See* 47 CFR § 20.23(d)(3).

[178] *Contraband Second R&O*, 36 FCC Rcd at 11839-40, para. 66.

[179] 47 CFR § 1.9040(a)(2). All spectrum leasing arrangements must provide that "[i]f the license is revoked, cancelled, terminated, or otherwise ceases to be in effect, the spectrum lessee has no continuing authority or right to use the leased spectrum unless otherwise authorized by the Commission." *Id.*

spectrum leasing arrangement into the term of the renewed license authorization.[180] We seek comment on whether to apply the current part 1 lease term requirements to leasing arrangements for jamming solutions. Although we seek to provide regulatory flexibility where feasible, we seek comment on whether a revised approach is warranted here, given the contractual collaboration between solutions providers implementing jamming solutions and DOCs. For example, should we amend our rules to specify that the length of the lease for the provision of jamming services may only be as long as the length of the contractual arrangement with the applicable DOC, with possible extensions? What are the costs and benefits of such a restriction? Should we strengthen our approach to CISs generally and revise our current rules to take this approach for MAS and detection systems?

69. *Subleasing.* Pursuant to sections 1.9020(l) and 1.9030(k) of the Commission's rules, a spectrum lessee in a spectrum manager or long-term *de facto* transfer leasing arrangement may sublease its leased spectrum usage rights with the licensee's consent and through the licensee's establishment of privity with the spectrum sublessee.[181] In our proposed framework, an eligible entity—whether a lessee DOC or lessee solutions provider under contract—would be implementing jamming solutions to combat contraband device use in a specific correctional facility. Under this framework, we believe that the ability to sublease to a third party would raise practical and technical issues, particularly with respect to system security, oversight of operations, and increased risk of harmful interference. Accordingly, we propose to not allow subleasing under the proposed jamming framework and seek comment on this proposal. We also note that, while our current leasing rules do not specifically address this issue, our ULS records do not reflect any requests to sublease in the CIS context. We therefore seek comment on whether we should clarify in our rules that subleasing is not permitted for any CIS in the interest of harmonizing our leasing rules across technologies.

70. *Construction Attribution.* Our current leasing rules generally allow a lessor to attribute the construction activities of its lessee to the lessor's performance requirements. Under a spectrum manager leasing arrangement, the licensee/lessor remains responsible for compliance with any construction and performance requirements applicable to the leased spectrum, but may attribute to itself the build-out or performance activities of its spectrum lessee(s) for purposes of compliance with any such requirements.[182] Similarly, under a long-term *de facto* transfer spectrum leasing arrangement, the licensee/lessor may attribute to itself the buildout or performance activities of its spectrum lessee(s) for purposes of compliance with any such requirements.[183] We note that our current leasing rules do not specifically address the issue of a wireless provider seeking to use a current CIS lessee's construction as

[180] *Id*. §§ 1.9020(m) (spectrum manager leases), 1.9030(l) (long-term *de facto* transfer leases), 1.9035(n) (short-term *de facto* transfer leases). The Commission must be notified of the renewal of the spectrum leasing arrangement at the same time that the licensee submits its application for license renewal. *See id.* § 1.949. In addition, the spectrum lessee may operate under the extended term, without further action by the Commission, until such time as the Commission shall make a final determination with respect to the renewal of the license authorization and the extension of the spectrum leasing arrangement into the term of the renewed license authorization.

[181] *Id.* §§ 1.9020(l) (spectrum manager subleasing), 1.9030(k) (long-term *de facto* transfer subleasing). The licensee must submit a notification regarding the spectrum subleasing arrangement in accordance with the applicable notification procedures set forth in this section. *Id.* §§ 1.9020(l), 1.9030(k). Subleasing is not permitted under a short-term *de facto* transfer lease. *Id.* § 1.9035(m).

[182] *Id.* § 1.9020(d)(5) (spectrum manager lease construction/performance requirements).

[183] However, such attribution is not available to a licensee/lessor under a short-term *de facto* transfer spectrum leasing arrangement. *See id.* §§ 1.9030(d)(5) (long-term *de facto* transfer lease construction/performance requirements), 1.9035(d)(3) (short-term *de facto* transfer lease construction/performance requirements); *see also First Secondary Markets R&O*, 18 FCC Rcd at 20676, para. 177 ("[S]hort-term leasing arrangements are expressly designed to be temporary in nature, and therefore cannot be counted to establish that the licensee is meeting the purposes and policies underlying our buildout rules, including the goal of ensuring establishment of service in rural areas.").

part of a performance requirement compliance showing, though our ULS records do not reflect that such a showing has been made to date. Due to the nature of jamming solutions deployed to prevent "service" in a limited public safety-related circumstance, however, we propose to not allow a licensee/lessor(s) to rely on its lessee(s) deployment of a jamming solution for purposes of satisfying the performance requirements of the underlying license.[184] We seek comment on this proposal, and whether we should clarify in our rules that such construction attribution is not permitted for any CIS.

71. *ECIP Holding Period Exception.* In July 2022, the Commission established the Enhanced Competition Incentive Program (ECIP), which among other things, modified the Commission's leasing rules to provide incentives for stakeholders to engage in qualifying transactions that make spectrum available in rural areas for advanced wireless services.[185] In adopting ECIP, the Commission also sought to facilitate new opportunities for small carriers and Tribal Nations to increase access to spectrum, while incorporating provisions to ensure against program waste, fraud, and abuse.[186] In this regard, the Commission adopted several measures to protect the integrity of ECIP, including a five-year holding period during which licensees cannot further partition, disaggregate, assign, or lease licenses assigned through ECIP.[187] The Commission, however, adopted an exception to the holding period for lease arrangements involving CIS providers, deeming CIS deployment in correctional facilities as vital to public safety.[188] Because leasing arrangement entered into for the provision of jamming solutions would likewise promote public safety, we propose to apply the exception to the ECIP holding period for lease arrangements involving providers of jamming solutions in correctional facilities. We seek comment on this proposal.

b. Non-Exclusive Overlay Licensing

72. As discussed in detail above, our lead proposal to authorize jamming solutions in correctional facilities is to apply our existing secondary markets framework. Because this proposal leverages a market-based authorization approach wherein stakeholders collaborate in good faith in the furtherance of public safety, in the same way that parties have successfully negotiated in good faith for CIS deployments to date, we fully anticipate that authorization of jamming solutions via leasing will occur in the vast majority of cases. That said, because our overarching goal is to facilitate solutions to help resolve this pressing public safety issue, we propose, as a method of last resort, an authorization path available only when parties fail to reach a leasing arrangement negotiated in good faith.[189] In such cases, we propose to permit eligible entities to directly apply for an overlay license, provided certain conditions are met, to increase flexibility for jamming solutions in correctional facilities and to incentivize market-based solutions in the first instance. We believe that an overlay construct is an appropriate mechanism for authorizing jamming solutions where DOCs/solutions providers seek lease arrangements in good faith, but the wireless provider is unwilling to enter into the leasing arrangement on a good faith basis.

73. We seek comment on the approach described below, including the appropriate application, licensing, operating, and technical rules applicable to the proposed jamming overlay license

[184] This proposal extends to all of the licensee's build-out obligations where it is required to construct and operate one or more specific facilities, cover a certain percentage of the population or geographic area, or provide "substantial service."

[185] *Partitioning, Disaggregation, & Leasing of Spectrum*, WT Docket No. 19-38, Report and Order and Second Further Notice of Proposed Rulemaking, 37 FCC Rcd 8825, 8825-26, paras. 1-2 (2022).

[186] *Id.* at 8825-26, paras. 1-2.

[187] *Id.* at 8846-47, paras. 67-69.

[188] *Id.* at 8847-48, paras. 71-73.

[189] The Commission took similar steps in the *Contraband Second R&O* by requiring CMRS licensees to negotiate in good faith with entities seeking to deploy a CIS, and providing that a solutions provider could seek special temporary authority in instances where no agreement was reached after a 45-day period. *See* 47 CFR § 20.23(a).

framework. We seek comment on the appropriate details associated with this potential backstop approach to develop a robust record for Commission consideration, including its costs and benefits. We also seek comment on whether there are other exigent circumstances in which a direct overlay license may be preferrable to a leasing arrangement.

74. *Statutory Authority and Mutual Exclusivity*. Consistent with our proposed deauthorization rule, we believe that a non-exclusive overlay licensing approach complies with section 333 of the Act, as the overlay licensee would be licensed to transmit under section 301 of the Act and would be permitted to cause interference to the operations of subscribers using contraband wireless devices that are no longer authorized under the wireless provider's license. We also believe that a non-exclusive, eligibility-based licensing approach is consistent with our statutory authority under section 309(j) of the Act.[190] Section 309(j) generally requires that the Commission assign initial licenses through use of competitive bidding when mutually exclusive applications for such licenses are accepted for filing.[191] We seek comment on an overlay licensing approach that would *not* result in receipt of mutually exclusive applications requiring resolution through competitive bidding. Mutual exclusivity would not occur under our proposal because, if the criteria for applying for an overlay license are met, wireless providers would no longer have exclusive use rights to spectrum in the relevant geographic area of a correctional facility. Under our proposal, absent a good faith leasing arrangement, DOCs/solutions providers would be eligible to receive an overlay license to operate on the identical spectrum used in that geographic area by the relevant wireless provider, effectively resulting in spectrum sharing. We therefore propose, pursuant to section 316 of the Act, to modify any and all licenses affected by overlay licensing for jamming solutions, if adopted and made effective, which would eliminate the wireless providers' exclusive use rights to their licensed spectrum in certain limited geographic areas.[192] This approach provides additional legal support for our proposed overlay licensing framework, and is consistent with our above proposed license modification in the context of our proposal to deauthorize subscriber operations of contraband wireless devices.[193] We seek comment on this proposed modification as applied in our overlay licensing construct.

75. In addition, we seek comment on an approach that would permit more than one applicant to serve a given correctional facility, at a DOC's option, which also results in spectrum sharing in the defined geographic area and the absence of mutual exclusivity. We seek comment on implementing an approach whereby applications for new overlay licenses would be placed in a processing "queue" and would be reviewed and processed in the order in which they are filed. We believe that this approach ensures that eligible entities can apply for and receive a Commission license to deploy jamming solutions in correctional facilities to combat contraband wireless device use. This would also afford a DOC the flexibility to contract, at its option, with more than one solutions provider to deploy at a given correctional facility, which is consistent with the approach some DOCs have taken with CIS solutions (i.e., contracting for fixed CIS and mobile CIS through potentially different solutions providers at the same correctional facility). We seek comment on this approach and any suggested alternatives.

76. *Overlay Licensing Through Part 90*. Currently, wireless providers that provide service across several spectrum bands to contraband wireless devices in correctional facilities are regulated through service and technical rules set forth in a number of rule parts, for example, parts 22, 24, 27, 30, 90, and 96. Providers of jamming solutions must necessarily transmit on bands used to provide

[190] 47 U.S.C. § 309(j)(2)(A).

[191] *Id.* § 309(j)(1) ("If, consistent with the obligations described in paragraph (6)(E), mutually exclusive applications are accepted for any initial license or construction permit, then, except as provided in paragraph (2), the Commission shall grant the license or permit to a qualified applicant through a system of competitive bidding that meets the requirements of this subsection.").

[192] *Id.* § 316.

[193] *See supra* para. 30.

commercial wireless service to counteract contraband wireless device use in correctional facilities. For administrative ease, in lieu of authorizing non-exclusive overlay jamming solutions by spectrum band through each of these many rule parts, we propose to adopt a new, standalone subpart within part 90 of the Commission's rules to address the use of overlay licenses for jamming solutions in correctional facilities, and we seek comment on our proposal. What are the costs and benefits of this approach? Would our proposal to establish standalone rules in a single rule part governing the licensing and technical requirements of overlay jamming operations be more efficient and provide greater clarity for stakeholders? Would placing rules governing overlay jamming solutions operations in multiple separate rule parts be confusing and burdensome for stakeholders? We propose to define "jamming solution" in a new part 90 subpart that would only apply in a correctional facility context in the same way as proposed above in the leasing rules, and we seek comment on whether there is any reason not to mirror, for overlay licensing purposes, the language ultimately adopted in the leasing construct.[194]

(i) Overlay Licensing and Operating Rules

77. We seek comment below on a multitude of issues associated with implementing a fallback alternative overlay licensing model, in the event it proves necessary, for jamming solutions in correctional facilities for a vital public safety purpose, while seeking to prevent harmful interference to authorized wireless devices within and outside a correctional facility.

78. *Eligibility Restrictions.* To effectuate an overlay licensing framework, we propose that eligibility requirements for jamming operations mirror those for leasing arrangements to the greatest extent possible, but with limited differences as discussed below. Accordingly, we propose to limit eligibility to apply for an overlay license to DOCs with authority over the correctional facility for which authority to operate a jamming solution is sought and solutions providers that have entered into a contract with a DOC with authority over the correctional facility for which authority to operate a jamming solution is sought. We believe that such an eligibility restriction can help ensure that only certain entities can be authorized consistent with our overall goal of facilitating solutions that combat contraband wireless device use. Consistent with our above authorization framework that first seeks to leverage a secondary markets approach through leasing arrangements, we also propose that, to be eligible to seek an overlay license for a jamming solution: (1) the entity must have attempted to negotiate a lease arrangement with the relevant wireless provider in good faith; and (2) the wireless provider must have acted in bad faith during the negotiation process resulting in no lease arrangement.[195]

79. Further, we recognize that there may be a fact-specific circumstance where a mix of Commission authorization vehicles for jamming solutions may be necessary. For example, a solutions provider may be able to negotiate lease arrangements with two wireless providers for a given correctional facility, but unable to reach a good faith agreement with a third wireless provider serving that same geographic area. In such a case, we believe it is in the public interest to permit the solutions provider to apply for an overlay authorization for bands/specific frequencies at a given correctional facility for which it has not reached a good faith leasing arrangement, so as to prevent an incomplete spectrum solution in that correctional facility. We believe that these eligibility restrictions will help achieve the key public interest benefit of enabling jamming solutions in this limited public safety context where our preferred approach fails. We seek comment generally on these proposed eligibility restrictions, and on whether we should consider any other eligibility restrictions and/or entry criteria in an overlay licensing model.

80. *Overlay Licensing Bands.* We seek comment on whether, in an overlay licensing framework, we should limit the authorization of jamming solutions to those bands typically used by wireless providers to provide commercial service to subscribers, identified as "included services" in the

[194] *See supra* para. 20 (seeking comment on the following proposed definition of a jamming solution: "the deployment of RF transmitter(s) within a correctional facility to prevent contraband wireless devices from establishing or maintaining a connection with a network.").

[195] *See supra* paras. 45-47.

leasing context discussed above.[196] We seek comment on the inclusion of each band (or block within a band), currently set forth as an included service in our leasing rules, in our proposed overlay license framework. We seek comment on whether the authorization of jamming operations by issuing non-exclusive overlay licenses in bands currently licensed to wireless providers would require an amendment to section 2.106 of the U.S. Table of Allocations, including potentially the addition of a table footnote applicable to relevant bands. In addition, as discussed in detail below,[197] we seek comment on whether to allow jamming solutions in correctional facilities to prevent the operation of unlicensed devices, such as Wi-Fi devices or other part 15 devices, and how this would work in our overlay licensing framework. Below we seek specific comment on the extent to which unlicensed bands are used in conjunction with the operation of contraband wireless devices—which operate under the unlicensed device rule—and on what approach we might use to authorize jamming solutions in unlicensed bands.[198]

81. *License Area.* In proposing an overlay licensing mechanism for jamming operations when leasing fails, our goal is to provide a last resort option to the corrections community to implement a jamming solution, while protecting authorized users from harmful interference. We recognize the need for an applicant, when seeking an overlay license for authority to operate at a specific correctional facility, to submit all information necessary to determine the license area and additional showings for authority to operate for Commission review and prior approval.[199] We acknowledge that the spectrum use in this context must be carefully managed through network engineering given the potential presence of authorized, non-contraband devices located outside a correctional facility or within the facility, if permitted in certain areas, and the possible impact that an improperly configured and operated jamming solution may have on authorized uses of these bands.

82. We seek comment on a licensing model in which the overlay license area would be confined to the geographic area affected by our proposed subscriber operation deauthorization rule, so as to comply with section 333 of the Act. We seek comment on permitting an applicant, most likely a solutions provider, to seek authority to transmit in a geographic area that is based upon its agreement with a DOC, which could involve the entire area within the perimeter of a correctional facility or a defined smaller area within the correctional facility. We seek comment on the necessary information and level of detail that should be provided to the Commission in describing the requested license area, for example, the name and address of the facility, the exact coordinates of the leased spectrum boundaries, or a shapefile reflecting the requested area. We also seek comment on the appropriate mechanism by which this information should be provided to the Commission.

83. *License Term/Renewal.* The Commission historically has established 10-year license terms for WRS licensees.[200] We seek comment on the appropriate license term if we implement our overlay license proposal. Commercial wireless provider licensees seek certainty and flexibility in implementing their networks and clearly benefit from a 10-year (or in some bands a 15-year) term, for administrative certainty and planning purposes. We recognize that operation in this limited public safety context is inextricably tied to the underlying arrangement with a DOC, if contracting with a solutions provider. We also recognize that spectrum use in this context must be carefully managed through precise network engineering, given the potential presence of authorized devices in the vicinity of a correctional facility and the possible impact that a jamming solution may have on authorized users of these bands. We therefore seek comment on whether we should issue an overlay license for a shorter period, noting that the Commission has granted shorter license terms in other bands as a means to manage and ensure

[196] *See supra* paras. 39-40.

[197] *See infra* paras. 110-18.

[198] *Id.*

[199] *See infra* paras. 104-08.

[200] *See, e.g.*, 47 CFR §§ 24.15, 27.13, 30.103.

periodic reevaluation of possible interference issues.[201] Should the initial license term mirror the contractual terms with a DOC for each individual facility to ensure the license authorization does not exceed the jamming solutions provider's contract with the correctional facility? Similarly, we seek comment on the appropriate term to apply for any subsequent license renewal.

84. We also seek comment on how we should address compliance with the Commission's renewal standard at the end of any license term. The WRS proceeding established the process for renewing a geographic license.[202] Specifically, it provided that a geographically-licensed WRS licensee will meet our renewal standard if it can make various certifications, e.g., for a licensee in its initial license term with no interim performance requirement, the licensee must certify that it has met its final performance requirement and continues to use its facilities to provide at least the level of service required by its final service requirement through the end of the license term.[203] Services subject to this geographic-based renewal standard include those under part 90.[204] We seek comment on whether to require overlay licensees for jamming operations to make a "renewal showing," for instance, certifying that it is operating consistent with its authorization to operate at specific correctional facilities with which the licensee continues to have a contract to perform jamming operations. We believe that requiring some kind of a renewal showing, consistent with our WRS rules, would facilitate efficient spectrum use by ensuring that overlay licensees for jamming operations continue to use the spectrum productively and in compliance with Commission rules during their initial license terms. We seek comment on the costs and benefits of imposing a renewal requirement for these licensees. We also invite commenters to submit alternate proposals for the appropriate license terms and renewal showings.

85. *Regulatory Status.* We seek comment on applying the PMRS presumption—similar to the regulatory status that we seek comment on for leasing arrangements above—to any overlay licenses issued for the provision of jamming operations as discussed herein.[205] Would applying this presumption to eligible entities in the overlay license model help align with the services to be provided, which are not intended to provide CMRS service as defined in the statute and our rules?[206]

86. *Secondary Market Transactions.* We seek comment on allowing overlay licensees for jamming solutions to engage in secondary market transactions only where the licensee is engaging in a transfer of control of the licensee, and not permitting assignment, partitioning, or disaggregation to another party. We likewise seek comment on not permitting overlay licensees to lease the non-exclusively licensed spectrum, which is not permitted under current secondary markets rules.[207] Are such limitations necessary in the jamming solutions overlay context, where different considerations may be relevant, including that the request for authority would be limited a relatively small service area of a correctional facility, and that such authority would be available only to entities that meet strict eligibility requirements as a DOC or solutions provider following the failure of good faith leasing negotiations? Or should we permit alienability conditioned upon the assignee, for example, making a showing that it too

[201] For example, the Commission has granted five-year license terms for some authorizations in the part 87 service following required coordination with the Aerospace & Flight Test Radio Coordinating Council, Inc. *See, e.g.*, ULS file nos. 0011530568, 0011477923.

[202] *See Amendment of Parts 1, 22, 24, 27, 74, 80, 90, 95, and 101 to Establish Uniform License Renewal, Discontinuance of Operation, and Geographic Partitioning and Spectrum Disaggregation Rules and Policies for Certain Wireless Services*, WT Docket No. 10-112, Second Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 8874 (2017) (*WRS Renewal Reform Second R&O and FNPRM*).

[203] *Id.* at 8883-84, para. 21.

[204] *Id.* at 8962, Appx. H.

[205] *See supra* paras. 58-59.

[206] *See* 47 U.S.C. § 332; 47 CFR § 20.3 (defining "commercial mobile radio service").

[207] *See* 47 CFR pt. 1, subpt. X; *see also id.* § 1.948.

meets all underlying requirements to be an overlay licensee in this specific, limited context? Commenters should address the costs and benefits of these potential limitations and any alternatives that we should consider.

87. *911 Call Transmission Requirements.* We discuss above the 911 requirements in section 9.10 of our rules and whether/how they apply to lessees seeking to provide jamming solutions in correctional facilities. Due to the nature of jamming technology, which generally prevents the transmission of emergency calls to a PSAP when blocking calls on any frequency, we seek comment on whether to refrain from applying the Commission's 911 and E911 rules to PMRS overlay licensees authorized to provide jamming solutions in correctional facilities. We seek comment on whether there are considerations in the overlay license context that are different from considerations in the leasing context discussed above with regard to the treatment of 911 for jamming operations.[208] We recognize that there exists a range of base station functionalities available for use in correctional facilities, from MAS that can permit a call to connect with an internal network, but then dropping it, to brute force jamming (currently permitted in some other countries) that blankets the designated area with RF energy such that no connection from any device to a wireless network is possible. We ask stakeholders to discuss whether it is technically feasible for a licensee that deploys any type of jamming solution to satisfy the requirements in section 9.10 of the Commission's rules, and if not, which particular requirements are not feasible and why.

88. *Performance Requirements.* Due to the nature of jamming operations, we believe it unnecessary to impose performance requirements on the overlay licensee, and seek comment on this proposal. The Commission typically establishes performance requirements to ensure that spectrum is intensely and efficiently utilized, and it has applied different performance and construction requirements to different spectrum bands based on considerations relevant to those bands and the services provided.[209] Here, the jamming solutions context is arguably different from the provision of commercial services where performance requirements are used to ensure that licensed spectrum does not lie fallow. Although we believe that operation through an overlay license in satisfaction of a contract with a correctional facility for public safety purposes meets our goal of ensuring spectrum usage, we seek comment on whether an overlay licensee should be required to meet some form of construction obligation.

(ii) Technical Parameters for Overlay Licenses

89. We seek detailed comment on the specific technical requirements that we should apply to an overlay license for jamming solutions in correctional facilities. We anticipate significant stakeholder input in this area, given the importance of facilitating successful jamming operations to thwart illegal contraband wireless device use in correctional facilities, while preventing harmful interference to authorized operations. Commenters are requested to provide technical details and analysis in support of any recommended action, including an evaluation of the impact of their proposals on other radio services. Among other issues, these studies and analyses should address how entities seeking to deploy jamming solutions plan to protect co- and adjacent channel, geographically proximate licensees, and also protect

[208] *See supra* paras. 60-64.

[209] *See, e.g., Service Rules for Advanced Wireless Services H Block—Implementing Section 6401 of the Middle Class Tax Relief and Job Creation Act of 2012 Related to the 1915–1920 MHz and 1995–2000 MHz Bands*, WT Docket No. 12-357, Report and Order, 28 FCC Rcd 9483, 9558–59, para. 195 (2013); *see also Amendment of the Commission's Rules with Regard to Commercial Operations in the 1695–1710 MHz, 1755–1780 MHz, and 2155–2180 MHz Bands*, GN Docket No. 13-185, Report and Order, 29 FCC Rcd 4610, 4659–60, para. 135 (2014); *Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, GN Docket No. 12-268, Report and Order, 29 FCC Rcd 6567, 6877–78, para. 764 (2014). For auctioned services, the Act requires that the Commission's rules include "performance requirements, such as appropriate deadlines and penalties for performance failures, to ensure prompt delivery of service to rural areas, to prevent stockpiling or warehousing of spectrum by licensees or permittees, and to promote investment in and rapid deployment of new technologies and services." 47 U.S.C. § 309(j)(4)(B).

out-of-band spectral neighbors from harmful interference. Additionally, commenters should compare their recommendations to the technical requirements applicable to existing licensees as authorized under the pertinent service rules. Recognizing that testing of jamming technologies has occurred at federal correctional facilities in the United States as well as at international correctional facilities, we seek comment on the challenges and issues that stakeholders have experienced when testing or deploying jamming technology. What solutions have stakeholders implemented or are developing to address those challenges, specifically, the hardware, software, and processes required, as well as the costs entailed in deploying such solutions? To inform our analysis regarding whether rule revisions may be necessary, we welcome the results of technical studies and analyses regarding the types of jamming solutions that have been further tested or deployed, and the potential for jamming solutions to cause co-channel or adjacent channel harmful interference to authorized operations.

90. We also seek comment on how our proposal to authorize jamming solutions through an overlay license might impact non-contraband devices located within a correctional facility. These include so-called "white-listed devices" approved for use by select correctional facility personnel (i.e., administrators, corrections staff, on-premises vendors, contractors, medical personnel). We note that at least one jurisdiction—the District of Columbia—has regulations affirmatively allowing legal counsel visiting inmates to possess and use wireless devices.[210] In addition, several states appear to allow limited use of wireless devices by visitors or employees of the correctional facility, and even inmates in some cases, when the facility provides authorization for an individual to possess and operate a wireless device.[211] These devices that operate within a correctional facility in some jurisdictions would not be considered "contraband" under state law, regulation, or policy, and therefore, under our proposed targeted deauthorization rule, operation or use of these devices would remain authorized by the Commission for purposes of section 301 of the Act, and protected against willful or malicious interference under section 333 of the Act. We seek detailed comment as to how correctional facilities and solutions providers with which they contract intend to deploy jamming solutions, while limiting the impact to only contraband devices within a correctional facility. Commenters that propose particular techniques to address this issue should also indicate whether their proposal should be incorporated into our technical rules and, if so, provide specific requirements.

91. *Power Limits.* We seek comment on the appropriate power limits that should be applied to jamming operations in correctional facilities under an overlay license. We recognize that a jamming

[210] D.C. Code § 22-2603.02(e) ("It is not unlawful for an attorney . . . during the course of a visit for the purpose of legal representation of the inmate . . . to (1) possess a cellular telephone or other portable device . . . for use by the attorney . . . and not for the personal use of any inmate. . . "). The Commonwealth of Kentucky also specifically states that attorneys are "permitted access to a telephone, unless an emergency or the security of the jail requires otherwise," though it is unclear if this privilege extends to using a mobile phone. *See* Ky. Admin. Reg. Title 501, Chapt. 3, Regulation 140, Section 1(4)(a)(6).

[211] *See*, *e.g.*, Ala. Code § 14-11-50 (possession prohibited except "when authorized by the person in charge of the prison...or by an officer of the institution empowered to give that authorization"); Cal Penal Code § 4575(a) (possession prohibited by any inmate "who is not authorized to possess that item"); Colo. Rev. Stat. Ann. § 18-8-204 (prohibits portable electronic communication devices "except those . . . authorized by the executive director of the department of corrections"); 11 Del. C. § 1256(a)(3) (contraband is a "cellular telephone, or any prohibited electronic device not specifically authorized or approved by the Commissioner or designee"); Fla. Stat. Ann. § 944.47(1)(c) (possession of contraband is unlawful "except as authorized by the officer in charge of such correctional facility"); Idaho C. § 18-2510 ("Excluded from this definition is any device having communication capabilities that has been approved by the facility head for investigative or institutional security purposes or for conducting other official business."); Illinois (720 ILCS 5/31A-0.1) (electronic contraband includes cellular communications equipment brought into or possessed in a penal institution without the written authorization of the Chief Administrative Officer"); LA Rev. Stat. Ann Sec 14:402(D)(9) (contraband includes any telecommunications equipment "unless authorized by the warden of the facility"); S.C. Code Ann. § 24-3-980 (unlawful for inmate to "possess a telecommunications device unless authorized to do so by the director"); Tenn. Code Ann. § 41-1-115 (entitled "Persons authorized to possess otherwise prohibited items").

solution using relatively high power levels could cover large correctional facilities more economically, but that use of higher power increases the potential for harmful interference to authorized devices, particularly if not properly engineered, installed, and maintained. We understand that power limits in radio service used in CMRS deployments vary band-by-band, and that, as noted above, wireless providers and CIS solutions providers typically deploy systems with base stations operating at a fraction of the maximum permitted power levels.[212] We seek comment on whether we should apply the power limits applicable to each band in the respective service rules or, in the alternative, implement a uniform power limit for overlay jamming operations, recognizing that device standards and network designs evolve.[213] We seek comment on whether a uniform approach would provide sufficient flexibility to enable successful operation of transmitters utilizing jamming solutions, which necessarily must overcome a wireless provider's signal that connects to contraband wireless devices. Is there a way to regulate power limits that does not unnecessarily constrain jamming technological advancements, while also allowing for successful operations in a manner that does not create harmful interference to authorized users in widely deployed commercial bands?

92. Should we adopt varying power levels for overlay licenses based on bands in operation, as is done for CMRS licenses today? Should we permit higher power levels in certain geographic areas, such as rural areas, with significantly less power available for jamming solutions operating in non-rural areas? Should we establish power limits for overlay licensee operation based on the size of the correctional facility at issue? Should we apply the power spectral density (PSD) model to transmitters deployed as part of a jamming solution, which would be consistent with the Commission's approach in virtually all flexible use, commercial service bands?[214] What are the costs and benefits of taking this approach, which has been implemented to achieve parity amongst varying technologies in the commercial services? Commenters advocating for higher power should also address how much more power they believe is necessary to effectively serve correctional facilities in rural areas, and provide comment on how the Commission should define rural areas in this specific context.

93. Further, consistent with our seeking comment above on approaches to prevent harmful interference in the leasing context,[215] should we also generally require overlay licensees to use narrowly tailored means in implementing ta jamming solution to achieve the goal of combatting contraband wireless device use, which will vary from a technical perspective depending on the particular correctional facility? For example, should we prohibit use of jamming technology across an entire 5G band(s) where a jamming solution could be targeted on the control channel portion of a band, which would require less overall radiated power and potentially reduce the risk of harmful interference to authorized devices? Should we require licensees to adjust their technical parameters contingent on what technology the wireless provider is using in the particular correctional facility, for example, deployments in FDD or TDD bands?[216] Given the absence of a leasing arrangement in an overlay license scenario, are specific measures needed to prevent harmful interference to a wireless provider's base stations in a TDD context, for example taking into consideration the desired v. undesired signal levels in a TDD pattern? Should we require, in a TDD context, synchronization between a solutions provider deploying a jamming solution and the wireless provider offering service to an area that includes a correctional facility to avoid unwanted transmissions during the wireless provider's base station transmit timeslot? We seek comment on possible ways to address power or other technical limitations that would further the goal of increasing

[212] *See supra* note 136.

[213] *See, e.g.*, 47 CFR §§ 22.535 (part 22 effective radiated power limits), 22.565 (part 22 transmitting power limits), 24.132 (part 24 power limits), 24.232 (part 24 broadband PCS power limits).

[214] *See supra* note 139 (explaining power spectral density model).

[215] *See supra* para. 50.

[216] *See supra* para. 51 (discussing the distinction between TDD and FDD in the context of the deployment of jamming solutions and relevant considerations).

options for DOCs, while avoiding harmful interference to wireless provider networks and non-contraband wireless devices generally.

94. *Out of Band Emission Limits.* Various Commission rule parts (e.g., 22, 24, 27, 30, and 96) set forth a range of OOBE limits that apply to the bands where wireless provider licensees could potentially deploy effective jamming solutions.[217] To protect adjacent band licensees from harmful interference, we seek comment on whether we should apply to overlay jamming operations the existing OOBE limits pertaining to the relevant bands wireless providers use in providing service to the geographic area that includes correctional facilities. We seek comment on whether there is a technical rationale for adopting emissions limits for overlay jamming solutions that are more restrictive than those currently applicable to wireless provider base station emissions in each respective band. Are the current wireless provider OOBE limits sufficient to protect the range of adjacent band services if these limits are applied to new jamming solutions? Are stricter OOBE limits required for jamming transmissions to protect adjacent band licensees? Should we establish more restrictive OOBE limits to protect other nearby spectrum neighbors not operating in immediately adjacent bands? Commenters should address specific concerns and potential solutions for each band of interest. Commenters supporting different emission limits for jamming operations should make specific proposals, supported by technical justifications and analyses on how those emission limits would better protect operations in adjacent or other nearby spectrum bands.

95. *Field Strength Limit and Market Boundaries.* Implementation of an overlay licensing structure for jamming operations based on geographic service areas requires a mechanism to ensure that such operations do not cause interference to co-channel systems operating along common geographic borders, which in all likelihood are the authorized subscriber devices of wireless providers operating in the area adjacent to a correctional facility. We seek comment on whether we should adopt a new, uniform field strength or power flux density limit that will apply to jamming overlay licensees, if commenters believe that existing field strength limits set forth in the Commission's rule parts governing commercial wireless services are not sufficient to protect co-channel adjacent market users.[218] We note that the existing technical rules for each radio service were tailored to account for the allocations in the bands where the services were authorized to operate. Since we are proposing to authorize operations that could raise issues not anticipated when the flexible technical rules were initially adopted for a particular commercial radio service, we seek comment on whether modified or additional technical protections are required, as well as the costs and benefits of any alternative approach.

96. *Intermodulation Interference*. Intermodulation interference occurs within a radio receiver when signals in use at a given location pass through active non-linear elements of the first stages of the receiver causing it to receive "ghost" signals that were not part of the original signal.[219] The "mixing" of signals within the receiver explains how two or more signals, widely separated (in frequency), can cause interference to a separate desired channel.[220] In an overlay licensing structure for jamming operations, where there is a possibility that jamming signals could "mix" within the receiver of a radio operated in or around the prison facility (particularly radios used by public safety and first responder officials), there is

[217] *See, e.g.*, 47 CFR §§ 22.359 (part 22 emission limitations), 24.133 (part 24 emission limits), 24.238 (part 24 broadband PCS emission limitations).

[218] *See, e.g.*, *id.* §§ 22.983, 24.236, 27.55.

[219] Intermodulation products are categorized according to "order." Thus, in the case of two-frequency (F1 and F2), third-order intermodulation, the intermodulation products (P) are calculated by: $P_{intermod.}$ = 2*F1-F2 and $P_{intermod.}$ = 2*F2 - F1. The fifth order, two frequency intermodulation products are calculated by: $P_{intermod.}$ = 3*F1 - 2*F2 and $P_{intermod.}$ = 3*F2 - 2 *F1. *See Improving Public Safety Communications in the 800 MHz Band,* WT Docket No. 02-55-357, Report and Order, Fifth Report and Order, Fourth Memorandum Opinion and Order, 19 FCC Rcd 19469, 15023–24, para. 91 n.276 (2004).

[220] *See id.* at para. 91.

the potential for intermodulation interference. We therefore seek comment on the likelihood of jamming operations causing intermodulation interference and what technical solutions, if any, are available to mitigate such interference during the design of a jamming solution. We also seek comment on what methods could mitigate such interference, should it occur after a jamming solution is installed and operating.

97. *Interference Resolution Procedures.* In addition to considering technical requirements applicable to overlay licensees, we seek comment on whether to implement strict responsibility for eliminating harmful interference to authorized devices. Should operators utilizing jamming technologies be required to respond to every complaint of interference to an authorized in-band or adjacent band licensee with full cooperation and utmost diligence to abate objectionable interference in the shortest practicable time? In addition, we seek comment on the appropriate obligations of an operator using jamming solutions following receipt of a complaint of harmful interference to a non-contraband wireless device. Should such an operator be required to immediately shut down all operations until it can ensure that the interference issue has been resolved? Would such an obligation unintentionally allow inmates or other stakeholders to circumvent a jamming solution?

98. We seek comment on whether we should adopt standardized procedures for reporting any such harmful interference and implementing a solution. For example, should we require overlay licensees to establish some type of common electronic means of receiving initial notification of harmful interference complaints from in-band and adjacent band licensees? If so, should we require that it specify a single, common point (for example, a single, nationwide email address or web page) so that an affected entity need not provide multiple notices to different overlay licensees in the same geographic area? If a notification requirement is adopted, what information should be included in the initial harmful interference complaint? Should we require that the initial harmful interference complaint include, at a minimum: the specific geographical location where the interference occurred or is occuring, the date and time or times at which the harmful interference occurred or is occurring; frequency/band that is affected; a description of the scope and severity of the harmful interference; the source of the harmful interference if known; and the relevant ULS information regarding the party suffering the harmful interference, including a single point of contact? Should we also impose a response time on the overlay licensee? For example, would it be appropriate to require the operator to respond no later than 24 hours after receipt of the initial notification?

99. Finally, we seek comment on whether we should require overlay licensees receiving an initial notification of harmful interference to perform a timely analysis and identification of the harmful interference, including, whenever necessary, an immediate on-site visit. Should we require that licensees complete this analysis and initiate corrective action within 48 hours of the initial complaint? Are there other specific requirements that we should consider as it pertains to the jamming device operator conducting an interference analysis? We ask stakeholders to discuss whether we should consider alternatives or additions to the interference resolution mechanisms discussed above.

100. *RF Exposure.* We propose to require jamming solutions to comply with the RF exposure rules set forth in sections 1.1307, 2.1091, and 2.1093 of the Commission's rules that outline exposure limits, equipment authorization requirements, and other regulatory requirements that are based on the type of device, how it is deployed or used, the power of its transmissions, and the proximity of its antenna and radiating structures to a person's body.[221] To maintain RF exposure compliance, the operation of any transmitter utilizing jamming technology can be highly dependent on how it is installed and operated with respect to the exposure conditions set forth in sections 1.1307, 2.1091, and 2.1093; therefore, in addition to the routine evaluation currently required for parts 22, 24, 27, 30 and 96 devices,[222] clear installation and user operating instructions/requirements may be necessary for installers and end users to satisfy RF

[221] *See* 47 CFR §§ 1.1307(b), 2.1091, and 2.1093.

[222] *See, e.g.*, *id.* §§ 22.379 (part 22 RF exposure), 24.52 (part 24 RF exposure).

exposure requirements. In addition, as required by our rules, applications for equipment authorization shall contain a statement confirming compliance with the RF exposure limits for both the fundamental and unwanted emissions.[223] Are there additional provisions we should implement for transmitters utilizing jamming technology?[224] For example, should we specifically require some type of routine RF exposure evaluation, currently required for operators in certain circumstances, for any transmitters authorized under our proposed framework and, if so, would any amendments to the Commission's rules be necessary? We also seek comment on whether to prohibit any transmitters implementing a jamming solution that are designed to be deployed where the radiating structure(s) is/are within 20 centimeters of the user or other persons, as defined for portable devices in section 2.1093(b) of the Commission's rules.[225]

101. *Canadian and Mexican Border Coordination.* We recognize that use of certain bands for potential jamming solutions, i.e., those used in commercial wireless service deployments, must not cause harmful interference across international borders and must comply with the requirements of current and future international agreements regarding operation in their vicinity.[226] We seek comment on whether compliance with existing bilateral agreements is sufficient in the context of overlay licensing for jamming solutions, or whether additional limits on transmissions are required to prevent harmful interference to operations across international borders. If commenters believe that additional protections (e.g., stricter limits, larger coordination distances, or other technical criteria) are required in this regard, we ask for specific technical comments.

102. *Other Technical Requirements and Limitations.* We seek comment on how other current technical limits for operations in bands commonly used to provide commercial wireless service should be applied to jamming operations in correctional facilities in an overlay licensing framework. For example, should we apply the existing frequency stability, duty cycle, synchronization requirements, and other limits that apply to CMRS base stations and devices, as set forth in the service rules for the respective band of operation, to jamming solutions? Are there factors in the existing technical limits that could hinder the range of services we explore in this *Third Further Notice*? If existing technical limits are insufficient to protect against harmful interference potentially caused by jamming solutions as contemplated in this *Third Further Notice*, commenters should offer specific limits, with a justification of why those limits are needed and an analysis of how they might impact in-band and adjacent band authorized operations in the bands under consideration. We also seek comment on the applicability to jamming operations of various coordination, notification, and other rules currently applicable to 800 MHz cellular terrestrial base stations to protect public safety operations. As jamming solutions are designed to block all communications, public safety operations would not be subject to the "near-far interference" situation caused by operations near a base station.[227] To help resolve the near-far issue and protect public

[223] *See id.* §§ 2.1091(d) and 2.1093(d).

[224] For example, the RF exposure evaluation requirements of 47 CFR § 2.1091 for mobile device exposure conditions subject to MPE limits, and 47 CFR § 2.1093 for portable device exposure conditions subject to SAR limits, are different. *See* KDB Publication Number 447498 - Mobile and Portable Device, RF Exposure, Equipment Authorization Procedures, 1.1307, 2.1091, 2.1093; https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?switch=P&id=20676.

[225] 47 CFR § 2.1093(b).

[226] *See, e.g.*, FCC, *Canadian Agreements by Frequency*, https://www.fcc.gov/canadian-agreements-frequency (last visited Sept. 3, 2025); FCC, *Mexican Agreements by Frequency*, https://www.fcc.gov/mexican-agreements-frequency (last visited Sept. 3, 2025).

[227] "Near-far interference" refers to interference that arises when a cellular system operates in close proximity to a public safety system. Specifically, this type of interference occurs where a public safety mobile/portable unit receives a stronger signal from a nearby, adjacent channel commercial base station rather than from the desired, distant public safety transmitter. The Commission addressed this "near-far" interference problem when it re-banded the 800 MHz band. *See Improving Public Safety Communications in the 800 MHz Band*, WT Docket No. 02-55, (continued….)

safety, the Commission, among other actions, implemented sections 22.913(b) and (c), 22.970, 22.971, 22.972, and 22.973.[228] These rules may not directly apply to jamming solutions, but we nonetheless seek comment on whether some form of accommodation is needed for jamming operations at 800 MHz or any other bands adjacent to public safety operations to ensure the continued reliability of public safety networks and avoid harmful interference. Finally, we seek comment on any other limitations that the Commission should consider in conjunction with the proposed deauthorization rule and the issuance of an overlay licensee to authorize jamming solutions in correctional facilities.

103. *Other Licensing and Operational Rules.* Finally, we seek comment on whether there are any other relevant service rules that we should consider including in an overlay licensing framework for jamming solutions. Commenters should address how the service rules we might adopt that govern jamming solutions could encourage the efficient use of spectrum resources, while also protecting against harmful interference to in-band or adjacent band authorized users. We also invite comment on the costs and benefits associated with authorizing jamming solutions as discussed in this *Third Further Notice*, and ask that commenters provide detailed technical and economic data to support their suggestions. We recognize that there are a range of tradeoffs to consider, including different costs and benefits associated with issuing overlay licenses in correctional facilities on wireless provider licensed spectrum, balanced against the potential for harmful interference to authorized users. We seek comment on whether there are other studies, standards, efforts, or analyses that we should consider in this proceeding. If so, we ask that commenters identify such undertakings and explain why they warrant consideration. We also invite comment on other possible approaches to authorizing jamming solutions in correctional facilities that we should consider in addition to those discussed in this *Third Further Notice*, as well as the costs and benefits of such alternative approaches.

(iii) Application Process and Procedures

104. As described above, we propose a fallback overlay licensing framework for authorizing jamming solutions by eligible entities where parties are unable to execute a good faith leasing arrangement pursuant to our streamlined leasing procedures. Below, we seek comment on the details as to how an interested party would obtain such a license, including what supporting documentation should be required for each step of the proposed process. Our goal is to authorize operations via a conditional overlay license to operate at a specific correctional facility, in a specified geographic area, with access to certain bands on a non-exclusive basis. We propose that an overlay license would be conditioned on the successful completion of testing of the jamming system at the correctional facility that would be reviewed and approved by the Commission prior to the issuance of final authority to operate at the facility. We propose a multi-step application process that includes: (1) submission of an application with supporting information demonstrating that the licensee is prepared to deploy an effective jamming solution without causing harmful interference to authorized devices; (2) Commission review of the application and, where in the public interest, an initial grant of a conditional overlay license; (3) satisfaction of the condition of the license grant through on-site testing; and (4) provision of final Commission authority to operate at the facility following successful testing. We seek comment on this approach.

105. As an initial step, we propose that an eligible entity seeking an overlay license would be required to submit an FCC Form 601 in ULS that provides: administrative information, a certification regarding its eligibility, a certification that it seeks to deploy equipment as part of a jamming solution with a valid part 2 equipment authorization, a brief description of its jamming solution, the requested technical parameters (as developed through this *Third Further Notice*), the proposed service area and geographic boundaries of the requested license area, and a showing as to how the proposed system will not cause harmful interference to authorized devices. We seek comment regarding what specific

(Continued from previous page)
Report and Order, Fifth Report and Order, Fourth Memorandum Opinion and Order, and Order, 19 FCC Rcd 14969, 14972-73, para. 2 (2004).

[228] *See id.*; 47 CFR §§ 22.913(b)-(c), 22.970, 22.971, 22.972, 22.973.

additional information should be required to be filed along with the application, noting that applicants may request confidential treatment of information contained in their applications consistent with section 0.459 of the Commission's rules.[229] As proposed, the non-exclusive overlay licensing application process is available only upon the failure of good faith negotiations of the parties to execute a leasing arrangement.[230] Should we therefore require an applicant to file an attachment to its FCC Form 601 sufficiently demonstrating that it attempted to negotiate in good faith, that the wireless provider acted in bad faith during the negotiation process, and that as a result, the parties were unable to enter into a lease agreement?[231] We seek comment on what would constitute a sufficient demonstration of bad faith in the exhibit. Regarding service area, should we require that the applicant submit the name and address of the facility, the specific services to be provided and frequency bands requested, and the service area requested for the overlay license, including specific coordinates and/or map? Should the application include, as an attachment, a copy of the applicant's contract with the DOC to provide jamming services at the particular correctional facility? Alternatively, would it be sufficient for the applicant to provide a certification that a contract with a DOC exists to provide jamming services at the facility? We anticipate that entering into a contractual agreement between a jamming solutions provider and a DOC is a key step in demonstrating that the solutions provider is ready and able to deploy its system at a given correctional facility. In connection with an applicant's overlay licensing application, we propose to require an applicant to include a declaration consistent with section 1.16 of the Commission's rules that its application contains truthful and accurate information.[232] This requirement is consistent with what we require of applicants in the CIS certification and disabling context.[233] Finally, the application would be required to be accompanied by the requisite filing fee, as required by the Act and our rules.[234] We propose to treat an overlay license application for jamming solutions as site-based for application fee purposes, given that the area of operation is limited to a specific correctional facility (e.g., the perimeter of the facility). We seek comment on each of these proposals, including related costs and benefits.

106. Following the initial grant of an overlay license for a jamming solution, as a condition of the grant, we propose that a DOC/solutions provider perform on-site testing at the correctional facility to demonstrate that the system will function as expected and within the boundaries of the overlay license service area, protecting authorized users both within and outside the boundaries from harmful interference. We seek comment on the nature of wireless provider participation in the testing and what details the conditional licensee will be required to provide the Commission following the testing. Currently, in the context of CIS qualifying requests and disabling, a CIS operator seeking to use the CIS to submit a qualifying request for disabling must test a certified CIS at each location where it intends to operate, and it must serve notice of the testing on all relevant wireless providers giving them an opportunity to participate in the tests.[235] Following testing, the CIS operator must certify to the Commission that the testing is complete and successful.[236] Should we adopt similar requirements in the

[229] *See* 47 CFR § 0.459 (detailing procedures to request withholding materials from public inspection).

[230] *See supra* paras. 45-47.

[231] *See* 47 CFR § 1.913(a)-(b). We note that a wireless provider may file a petition to deny pursuant to section 1.939 of the Commission's rules within the requisite time period if it seeks to contest a lack of good faith allegation. *See* 47 CFR § 1.939 (petitions to deny).

[232] *Id.* § 1.16.

[233] *See Wireless Telecommunications Bureau Provides Guidance for Filing Contraband Interdiction System Certification Applications and Self-certifications*, GN Docket No. 13-111, Public Notice, DA 21-1572 (WTB Dec. 17, 2021).

[234] *See* 47 U.S.C. § 158; 47 CFR § 1.1102.

[235] *See* 47 CFR § 20.23(b)(3).

[236] *Id*.

context of overlay licenses for jamming operations? Given the heightened concern regarding the potential for harmful interference in the jamming context, should we require that relevant wireless providers participate in the tests? Or is a requirement that the licensee provide the wireless carriers reasonable notice of testing sufficient?

107. We seek comment on what information conditional licensees must provide to the Commission to show successful testing and how such information should be provided, keeping in mind the goal of implementing jamming solutions while not causing harmful interference to authorized operations within and outside of the license service area. Should we require specific testing parameters, results, or certifications? How should signals be measured and what criteria should be used to evaluate such tests? Should we require that a jamming solutions provider meet certain criteria regarding its ability to contain its signal to the licensed area and not cause harmful interference to authorized wireless devices? Is such a requirement unnecessary or would it be beneficial in assessing the technical merits of a jamming solution? Should the testing criteria vary depending on whether the facility is in a rural or urban area? Following the filing and Commission approval of the on-site test results, we propose that a jamming solutions provider would be authorized to begin jamming operations. We seek comment on whether, and how often, we should require an overlay licensee to re-test the effectiveness of its system, particularly where technical or operational details of the deployment change in response to wireless provider network adjustments. We seek comment on the costs, benefits, and burdens to potential stakeholders of requiring a jamming solutions provider to obtain conditional authorization, test, and provide test results to the Commission for approval before commencing jamming operations, and of potentially requiring the relevant wireless providers to be part of the solution through mandatory involvement in the on-site testing process, and if so, to what extent.

108. In addition, we seek comment on whether there are alternatives to the proposed overlay licensing mechanism that would authorize jamming solutions where good faith leasing agreements cannot be reached. Commenters should include detailed descriptions of their proposals and should discuss the costs and benefits of the approach. Commenters should also discuss how their proposed approach would be implemented and the specific licensing, operational, and technical rules that would be required in order to ensure that the licensing mechanism protects against harmful interference to authorized users.

2. Authorizing Jamming Solutions on Other Spectrum

109. Our proposed deauthorization framework for permitting jamming solutions to combat contraband wireless devices in correctional facilities is predicated on the principle that subscribers are not authorized to operate such devices under section 1.903 of the Commission's rules.[237] However, because section 1.903 only pertains to fixed and mobile stations in the WRS, authority to operate contraband wireless devices using unlicensed Wi-Fi or other part 15 spectrum, or spectrum separately licensed under part 25, would not be affected by our proposed amendment to section 1.903.[238] The operation of other devices such as land mobile radios typically regulated by the Commission as Private Mobile Radio Services (PMRS),[239] satellite phones or terminals operating on dedicated satellite frequency bands,[240] or

[237] *See supra* para. 25.

[238] For example, Supplemental Coverage from Space (SCS) operations or the ancillary terrestrial component (ATC) of a Mobile Satellite Service (MSS). *See* 47 CFR §§ 25.115(q), 25.125(e) (licensing by rule as earth stations those terrestrial devices communications with satellites on SCS bands); *id.* § 1.9005(jj) (ATC authority licensed under part 25, although not a WRS subject to rule section 1.903, is an included service subject to lease arrangements under rule section 1.9005(jj)).

[239] PMRS is defined as a mobile service that is neither a CMRS nor the functional equivalent of a service that meets the definition of a CMRS. *See id.* § 20.3. PMRS generally refers to two-way radio systems used for internal communications within a single organization, like a business, community, or other entity. These systems are not for public use or resale.

[240] *See, e.g.*, Iridium satellite phones; Starlink Mini satellite terminals; phones with a Globalstar satellite connection.

devices licensed by rule under part 95,[241] also would not fall within the proposed deauthorization framework. Accordingly, we seek comment on whether contraband devices operating in such other radio services or on unlicensed spectrum are a substantial issue in correctional facilities and, if so, on the appropriate means to authorize jamming solutions to address this issue.

a. Unlicensed Operations Under Part 15

110. *Part 15 Equipment.* Part 15 of the Commission's rules permits, among other things, users to operate RF devices without a Commission-issued individual license.[242] These devices may generally operate across any spectrum band, except for bands specifically restricted to only spurious emissions.[243] Despite the ability to access broad swaths of spectrum, the majority of unlicensed devices used for communications (e.g., Wi-Fi and Bluetooth) typically only operate across a few discrete bands.[244] The Commission's part 15 rules are designed to ensure a very low probability that these devices will cause harmful interference to other authorized users of the same or adjacent spectrum.[245] Typically, devices operated on an unlicensed basis do so at low power over relatively short distances, and often employ various techniques, such as a contention-based protocol or listen-before-talk protocols, to facilitate coexistence with other radio services and reduce the risk of harmful interference to others as well as themselves.[246] Most common consumer electronic devices (e.g., laptops, tablets, smart speakers, and Wi-Fi routers) use equipment authorized by the Commission pursuant to part 15 of its rules, many of which use communications protocols such as Wi-Fi or Bluetooth. The primary operating condition for devices operating on an unlicensed basis is that the operator must accept whatever interference is received and must not cause harmful interference.[247] Should harmful interference occur, the operator is required to immediately correct the interference problem or to cease operation.[248]

111. As Wi-Fi equipment can be used to establish networks to provide internet access that is obtained via connection to an outside communications source, we seek comment on whether inmate use of Wi-Fi in a contraband wireless device is a current or anticipated problem in correctional facilities and ask stakeholders to specifically describe the nature of the problem, if any. For example, we seek comment on whether inmates are accessing Wi-Fi signals that are transmitted from inside a correctional facility (such as Wi-Fi hotspots that may be originating from another contraband wireless device or transmitter) or from outside the facility. Commenters should also discuss in detail the types of current or future technologies that are available to block, interfere with, or de-authenticate Wi-Fi transmissions (e.g., through the sending of a deauthentication signal to disrupt a Wi-Fi device's link to the Wi-Fi network); how the Commission should facilitate the authorization of those technologies; and whether any of these technologies include functions that might enable certain Wi-Fi devices to communicate, while blocking others located in the same limited geographic area. We also seek comment on whether correctional facilities are relying on any unlicensed devices essential for facility operation, such as wireless security cameras, and how these devices can be protected while jamming contraband Wi-Fi devices.

---

[241] *See, e.g.*, Family Radio Service; CB Radio Service; Multi-Use Radio Service.

[242] *See generally* 47 CFR pt. 15.

[243] *Id.* § 15.205.

[244] Wi-Fi devices typically access the 902-928 MHz, 2400-2483.5 MHz, 5 GHz, and 6 GHz bands. Bluetooth devices operate in the 2400-2483.5 MHz band.

[245] *See* 47 CFR § 15.5(b)-(c); *see also 5 GHz First R&O*, 29 FCC Rcd at 4218, para. 3.

[246] *See generally* 47 CFR §§ 15.15 (general technical requirements), 15.109 (radiated emission limits), 15.209 (radiated emission limits; general requirements), and 15.407(d)(6) (Operational restrictions for 6 GHz U-NII devices).

[247] *Id.* § 15.5(a)-(b).

[248] *Id.* § 15.5(b)-(c).

112. *Framework for Deauthorization of Contraband Part 15 Devices and Authorizing Part 15 Jamming Solutions.* As noted above, the deauthorization framework based on section 1.903 of our rules only applies to fixed and mobile stations in the WRS. If the Commission determines that jamming solutions should be authorized to cause interference to contraband wireless devices operating on unlicensed spectrum, such as those that communicate using Wi-Fi, we seek comment on the appropriate deauthorization approach to permit such action consistent with section 333 of the Act. As an initial matter, we seek comment on whether the definition of a contraband wireless device in section 1.9003 of our leasing rules is broad enough to cover unlicensed devices,[249] such that a cross-reference to the section 1.9003 definition in part 15 is sufficient, or whether we would need to replicate this definition within part 15 to ensure that it is applicable to unlicensed devices. With respect to deauthorization of contraband wireless devices operating on part 15 spectrum, is it necessary to adopt a part 15 provision expressly prohibiting the operation of such devices under part 15? Would this approach permit jamming solutions on part 15 spectrum, consistent with section 333 of the Act, because the contraband wireless devices would be operating without Commission authority and therefore not protected from interference? Alternatively, is a rule change unnecessary to comply with section 333 of the Act because part 15 devices already operate without any protection from interference that may be caused by the operation of an authorized radio station?[250] We seek comment on these issues.

113. For WRS, we are proposing to authorize DOCs/solutions providers to provide jamming solutions by requiring them obtain a license either through the Commission's part 1 leasing rules or a part 90 non-exclusive overlay license. Because Commission rules do not require a license to operate a part 15 device, the part 1 leasing approach does not apply in this instance to those seeking authorization for a jamming solution on unlicensed spectrum. Thus, we seek comment on the appropriate authorization framework for jamming solutions using part 15 spectrum. In lieu of leasing, should we require an operator of a jamming solution intended to prevent unlicensed contraband device use to obtain a part 90 overlay license for authorization to operate such equipment, which in this limited context would be unrelated to the status of lease arrangement negotiations? Should such a license be a separate part 90 authorization for part 15 spectrum use or should it be combined with a more expansive part 90 overlay license that covers a mix of licensed bands, as well as the bands most commonly used by unlicensed devices? Are there other alternatives available to license transmissions for which current operations are authorized on an unlicensed basis? Further, should we take an approach analogous to the procedures proposed herein for licensed operations, where an entity (if acting on behalf of a DOC) seeking such a license would certify that it: (1) has entered into a contractual agreement with a DOC that requires the solutions provider to block or otherwise deny access to unlicensed (e.g., Wi-Fi transmissions); and (2) is proposing to use equipment that has part 2 equipment authorization? We seek comment on the appropriate licensing requirements for jamming solutions intended to prevent unlicensed devices from communicating and to what extent we need to amend parts 15 and 90 of our rules.

114. Some stakeholders have expressed a belief that transmitting devices that are fully intended to cause harmful interference could arguably operate on commercial bands within the current part 15 rules *if their power levels are sufficiently low*.[251] We propose above, as it relates to bands typically associated with wireless provider commercial networks, that any Commission–authorized

[249] *Id.* § 1.9003 (A contraband wireless device is any wireless device, including the physical hardware or part of a device, such as a subscriber identification module (SIM), that is used within a correctional facility in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy).

[250] *Id.* § 15.5(b). This rule also provides that part 15 devices must accept interference from another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator. *Id*.

[251] *See* Detection Innovation Group's Expedited Petition for Rulemaking, GN Docket No. 13-111, at 7-9 (rec. Jul. 6, 2022), https://www.fcc.gov/ecfs/search/search-filings/filing/1070625651417 (arguing that its jamming system, which transmits on cellular frequencies, complies with the Commission's part 15 rules because its power levels will be within the radiated emission limits in the rules).

jamming solutions, regardless of the use of very low power levels, would only be so authorized through our proposed part 1 leasing[252] and/or part 90 overlay licensing mechanisms,[253] rather than through low-power part 15 authorized operation. As an additional measure, we propose, as discussed below, that the Commission will not certify transmitter(s) intended for use as part of a jamming solution under part 15 of the rules. We believe that this prohibition against part 15 equipment authorization for jamming solutions is necessary to ensure that operation based on the proposed deauthorization framework does not result in the production, marketing, and sale of unlicensed low-power, hand-held jamming solution devices. Moreover, we believe this proposed prohibition would aid in ensuring that jamming solutions are *only* authorized in the United States for operations in correctional facilities as proposed herein. Are there other safeguards the Commission should put in place to achieve the same result? We seek comment on these proposals.

115. *Technical Requirements*. Unlicensed operation is permitted under part 15 rules in multiple frequency bands. For example, popular Wi-Fi devices typically operate in the 2.4 GHz (2400-2483.5 MHz bands),[254] 5 GHz (5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz,[255] and 5850-5905 MHz[256] bands), and 6 GHz (5925-6425 MHz, 6425-6525 MHz, 6525-6875 MHz, and 6875-7125 MHz).[257] Other popular bands for unlicensed device operation include the 900 MHz band (902-928 MHz), 60 GHz band (57-71 GHz), and 90 GHz band (92-95 GHz) where various broadband wireless communications can be supported.[258] The part 15 rules also generally allow extremely *low power* operation across any spectrum band except the restricted bands.[259] However, ultra-wideband devices may operate over the restricted bands pursuant to specific technical requirements.[260] We seek comment on the specific bands for which we should authorize jamming solutions for unlicensed devices. Should the rules be flexible to permit jamming solutions for any band where unlicensed devices can operate, which would also include the same bands on which services allocated in the frequency allocation table operate, or only the most commonly used unlicensed bands?

116. Unlike licensed operations, where the technical rules typically assume an exclusive licensee, unlicensed operations in most bands require technical provisions to facilitate more intensive sharing of the bands among unlicensed devices and to protect authorized incumbent users from unlicensed operations. For example, frequency hopping systems operating in the 2.4 GHz band require a minimum number of hopping channels and limit the average time of occupancy on any channel.[261] Also, the

[252] *See supra* Section C.1.a.

[253] *See supra* Section C.1.b.

[254] *See, e.g., Amendment of Part 15 of the Commission's Rules Regarding Spread Spectrum Devices*, ET Docket No. 99-231, Second Report and Order, 17 FCC Rcd 10755 (2002).

[255] *See, e.g., Revisions of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz band*, ET Docket No. 13-49, First Report and Order, 29 FCC Rcd 4127 (2014).

[256] *See, e.g., Use of the 5.850-5.925 GHz Band*, ET Docket No. 19-138, First Report and Order, Further Notice of Proposed Rulemaking, and Order of Proposed Modification, 35 FCC Rcd 13440 (2020).

[257] *See, e.g., Unlicensed Use of the 6 GHz Band*, ET Docket No. 18-295 *et al.*, Report and Order, 35 FCC Rcd 3852 (2020) (*6 GHz R&O*); Third Report and Order, FCC 24-125 (rel. Dec. 13, 2024).

[258] 47 CFR §§ 15.245-15.258.

[259] *Id.* § 15.205.

[260] 47 CFR pt. 15, subpt. F.

[261] *Id.* § 15.247(a)(1)(iii). As another example, our part 15 rules applicable to several bands require use of Transmit Power Control (TPC) to limit the operating power to the minimum necessary for successful communications, and the maximum transmitter channel bandwidth for unlicensed devices operating in 5.925-7.125 GHz is limited to 320 megahertz to allow other users to share the band. *See id.* §§ 15.407(d)(10), 15.407(l)(11).

Dynamic Frequency Selection (DFS) mechanism is required for unlicensed devices operating in the 5.25-5.35 GHz and 5.47-5.725 GHz bands to protect radars operating in these bands.[262] Given these types of technical measures intended to facilitate successful spectrum sharing, how can we ensure that jamming solutions adequately protect authorized incumbent users operating on such spectrum from harmful interference?

117. We seek comment on what technical rules should apply to jamming solutions that are intended to prevent unlicensed devices from communicating. Although today we seek comment on the appropriate framework for authorizing the operation of jamming solutions on part 15 spectrum, including whether we should rely on part 90 for this purpose, we also seek comment on whether a jamming solution operator should comply either fully or in-part with the existing part 15 rules for each band in which it operates. Or should the technical rules for jamming solutions be specific to jamming solutions? We seek comment on the specific rules that either should or should not apply in each band of interest. For example, should the Commission allow the jamming solutions to transmit over entire bands used by unlicensed devices with one hundred percent duty cycle? What should be the transmit power limit and out-of-band emission limit characteristics for such jamming solutions? What other technical requirements should we consider for jamming solutions directed at unlicensed devices? How do we ensure that authorized services also operating in these bands are protected and can continue to operate as intended? We request comment on these issues, as well as relevant interference analyses to demonstrate how authorized incumbent users can be protected if a jamming solution is operating nearby and on the same or adjacent spectrum bands.

118. We also seek comment on what interference protection obligations jamming solutions should have with respect to unlicensed device operations that are permitted either within or near a correctional facility. Should jamming solutions be required to protect other unlicensed devices operating outside of the correctional facilities by, for example, complying with a field strength limit similar to those applicable to operations in licensed bands? We seek comment on whether the general rule requiring unlicensed devices to accept interference from authorized devices should be amended when such interference is caused by a jamming solution and whether, in such instances, the jamming solution operator should be obligated to adjust its system to ensure that interference to such unlicensed, yet authorized, operations is remedied. We request that commenters provide relevant interference analyses supporting the co-existence between jamming solutions and non-contraband unlicensed devices or justifications for requiring non-contraband unlicensed devices to have to accept interference from a jamming solution.

b. Part 25 Spectrum

119. Similarly, we seek comment on whether contraband devices that operate using part 25 (satellite communications) spectrum is a current or anticipated problem in correctional facilities. We ask stakeholders to specifically describe the nature of the problem and to discuss in detail the types of technologies, whether current or potentially under development, that can block or interfere with part 25 authorized transmissions. How should the Commission facilitate the authorization of those technologies, and do any of these technologies include functions that enable network connections for authorized devices that might be located in a correctional facility? How can these technologies protect other satellite services, including international satellite systems, from harmful interference?[263] Finally, if the

[262] *Id.* § 15.407(h)(2). Other examples include Wi-Fi access points operating in the 6 GHz band that must operate either under the control of an automated frequency coordination (AFC) system or only indoors at lower power to protect licensed incumbents from harmful interference. *See Unlicensed Use of the 6 GHz Band; Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3852, 3860, paras. 17-18 (2020). In addition, indoor access points must employ a contention-based protocol. *See* 47 CFR § 15.407(d)(6).

[263] *See* ITU Radio Regulation Nos. 0.4, 0.8, and 15.1 § 1.

Commission determines that it should deauthorize contraband wireless device satellite communications currently authorized under part 25, we seek comment on the appropriate approach to authorizing jamming solutions in the relevant bands.

3. Transmitters Used to Enable Jamming Solutions

a. Part 2 Equipment Authorization

120. The Commission carries out its responsibilities under section 302 of the Communications Act with respect to RF equipment through two principal means.[264] First, the Commission establishes technical rules for RF equipment to address specific regulatory objectives, e.g., to prevent harmful interference. Second, to ensure compliance with the technical rules, the Commission's rules generally require RF equipment to be authorized under part 2 prior to marketing or importation into the United States.[265] Commission rules generally provide three means for authorizing equipment: (1) Certification; (2) Supplier's Declaration of Conformity; and (3) Exemption.[266] Certification, the most rigorous approval process, is required for RF devices with the greatest potential to cause harmful interference to radio services.[267] Under the certification process, an FCC-recognized accredited testing laboratory[268] performs testing and an FCC-recognized telecommunication certification body (TCB) grants the equipment authorization based on an evaluation of the supporting documentation and test data submitted by the responsible party (e.g., the manufacturer or importer). Information, including the authorized technical parameters and descriptive information, for all certified equipment, is posted on a Commission-maintained public database.[269]

121. To achieve regulatory harmonization and administrative efficiency, we propose in this *Third Further Notice* to apply our current procedures to eligible entities for equipment certification regarding equipment to be used as part of a jamming solution in correctional facilities. We note that base stations employed as part of existing CISs in correctional facilities throughout the United States are required to comply with current part 2 equipment authorization rules.[270] Specifically, we propose to require entities to comply with existing part 2, subpart J, equipment authorization procedures for certification of equipment used as part of a jamming solution that would be authorized for operation pursuant to our part 1 leasing rules, a part 90 overlay license, or a combination thereof. Among other things, this would require that RF equipment associated with jamming solutions must be shown to comply with a variety of, and possibly differing, technical rules that are set forth under various parts of the Commission's rules governing spectrum typically used in commercial wireless networks, including, for

---

[264] 47 U.S.C. § 302a. This section authorizes the Commission, consistent with the public interest, convenience, and necessity, to make reasonable regulations governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications.

[265] 47 CFR pt. 2. The Office of Engineering and Technology (OET) administers the equipment authorization program under the authority delegated to it by the Commission. As part of its administration of the equipment authorization rules, OET has developed a substantial body of supplemental guidance that is available via public notices, which can be found at https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization, and in the Commission's Knowledge Database (KDB), which can be found at https://apps.fcc.gov/oetcf/kdb/index.cfm.

[266] *See* 47 CFR pt. 2, subpt. J, pt. 15.

[267] *Id.* §§ 2.906, 2.1031 et seq.

[268] For a list of currently FCC-recognized accredited testing laboratory, *see* FCC Office of Engineering and Technology, *Test Firm Search*, https://apps.fcc.gov/oetcf/eas/reports/TestFirmSearch.cfm.

[269] *See* FCC Office of Engineering and Technology, *Equipment Authorization Search*, https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm.

[270] *See Contraband Second R&O*, 36 FCC Rcd at 11822, para. 23; 47 CFR § 20.23(b)(1)(i).

example, parts 22, 24, 27, 30, and 96. Under current rules, measurement data used to document compliance with the pertinent rule requirements must be obtained in accordance with the procedures set forth in part 2 and provided to a TCB along with the application for certification.[271] Because equipment certifications must generally note the services under which the certification applies, jamming solutions would require certification for the rule parts consistent with the equipment it is intended to prevent from communicating. However, because the equipment could also potentially be used under a part 90 overlay license, it would necessarily require a part 90 equipment certification. Importantly, although we propose to permit the certification of transmitters intended for use as part of a jamming solution under various rule parts governing spectrum typically used in commercial wireless networks, we further propose that the Commission will not certify such transmitters under part 15 of the rules.[272] We believe that this proposed prohibition is necessary to ensure the authorization of jamming solutions does not result in the production, marketing, and sale of unlicensed low-power, hand-held jamming solution devices. We seek comment on this proposal.

122. We seek comment on whether the application requirements of current Commission rule sections 2.911 and 2.1033 are appropriate in this case or whether specific requirements should be added, modified, or considered inapplicable.[273] We believe that a transmitter used for jamming solutions would fall within section 2.1033(e), which applies to a "composite system that incorporates devices subject to certification under multiple rule parts."[274] Would this rule or any other rules prohibit or make it difficult to certify a jamming solution that can operate under both spectrum leasing and non-exclusive overlay licensing authorizations? In this regard, we note that section 2.947(f) requires that the individual devices in a composite system must comply with its specific standards.[275] To enable jamming solutions to be approved, does this rule need to be modified, and if so, how? Commenters should target any proposals regarding this rule to the specific issues associated with approving jamming solutions and not generally comment on equipment authorization procedures that could apply to any device. Further, should the testing of equipment used to provide jamming solutions include a method to ensure that it does not operate in any unauthorized bands (not just the bands adjacent to those for which it seeks authorization)? Finally, in light of the sensitive use and unique technology involved in jamming solutions, we propose to include jamming solutions equipment on the "Pre-approval Guidance List," thus requiring a TCB to process the application in coordination with the Commission in accordance with the procedures as set forth in the Commission's rules.[276]

123. Are any additional procedures necessary to ensure the equipment's ability to comply with our technical rules? We seek comment on the costs and benefits of applying our existing procedures to certifying equipment to transmitters that can be deployed as part of a jamming solution in a correctional facility. What other information should be required to make sure equipment used for jamming solutions complies with the appropriate technical standards and other applicable requirements? Should we take an alternative approach to certifying transmitters in this specific context? Commenters supporting alternative methods should describe and provide details regarding what process is needed to ensure that jamming solutions transmitters function properly, consistent with applicable Commission technical rules developed in this context. We also seek comment on ways the Commission can facilitate, encourage, or

[271] *See* 47 CFR § 2.1033(c)(17).

[272] *See supra* para. 114.

[273] 47 CFR §§ 2.911, 2.1033. We note that certain service rule requirements must be specifically addressed in documentation provided with certification applications. For example, part 90 public safety interoperability requirements and part 20 hearing aid-compatibility requirements. *See id.* §§ 2.1033(c)(23) and 2.1033(d), respectively.

[274] *Id.* § 2.1033(e).

[275] *Id.* § 2.947(f).

[276] *Id.* § 2.964.

require the production of these devices within the United States or United States allied countries. Are there specific actions we should take to mitigate any national security risks posed by jamming solutions that use equipment produced by foreign adversaries or other entities that have been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons?[277]

124. *Operation of Equipment Used for Jamming Solutions Prior to Equipment Authorization*. Commission rule section 2.805 provides that a radio frequency device may not be operated prior to equipment authorization unless certain conditions are met.[278] One exception for operating a device prior to equipment authorization is through grant of an experimental radio service license issued under part 5 of the Commission's rules.[279] We recognize that an entity seeking to implement a jamming solution that might ultimately be authorized through our proposed framework, either through a lease arrangement or an overlay license, may initially be interested in obtaining authorization to test, on a temporary basis, the system in a particular correctional facility. Such a test might be needed, for example, in responding to a DOC's request for proposal; to be eligible to enter into a contract with a DOC; and/or as part of a lease negotiation with a wireless provider. Given the importance, however, of facilitating effective jamming solutions in correctional facilities that are carefully deployed so as to avoid harmful interference to authorized users, we seek comment on whether we should amend section 2.805 to specify that jamming solutions may not be operated for testing purposes, unless and until equipment authorization is obtained. Alternatively, should we adopt more flexible rules to permit testing of jamming solutions prior to equipment authorization, but only through one of two methods: (1) special temporary authority granted by the Bureau;[280] or (2) experimental license granted by OET pursuant to part 5 of the Commission's rules?[281] What are the costs and benefits of either of these approaches or any suggested alternatives?

b. Marketing, Labeling, and Importation of Equipment Used for Jamming Solutions

125. The wireless industry has expressed concerns regarding the potential that equipment specifically intended for use as a jamming solution, if ever authorized for use in the United States—even in a limited correctional facility capacity—could be deployed in unauthorized contexts, such as in a business context (e.g. theaters, restaurants) or in the furtherance of criminal activity.[282] We share industry concerns that transmitters capable of being deployed as part of a jamming solution in correctional facilities might be misappropriated for other uses, and we therefore seek comment on whether we should limit the marketing[283] of such transmitters directly to DOCs and solutions providers that contract to

[277] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, Report and Order and Further Notice of Proposed Rulemaking, 37 FCC Rcd 13493 (2022).

[278] *See* 47 CFR § 2.805(a).

[279] *Id.* § 2.805(b).

[280] *See id.* § 1.931.

[281] *See id.* pt. 5. We note that, although operation of an experimental radio station is permitted only on the condition that harmful interference is not caused to any station (*see, e.g.*, *id.* § 5.84, 5.111(a)), we interpret that to mean any "authorized station," and therefore if we were to adopt our proposed deauthorization rule and a licensee obtained authorization to test a jamming solution under part 5, contraband wireless devices would not be protected against harmful interference under these part 5 rules or section 333 of the Act.

[282] *See, e.g.*, CTIA – The Wireless Association, Comments, Docket No. 100504212-0212-01, *Preventing Contraband Cell Phone Use In Prisons*, Dept of Commerce, NTIA, at 23-24 (June 11, 2010) (arguing that the use of jamming in prisons will lead to an increase in unauthorized jammer use, for example, in schools).

[283] *See generally* 47 CFR pt. 2, subpt. I (Marketing of Radio-frequency Devices). As used in this subpart, "marketing" includes "sale or lease, or offering for sale or lease, including advertising for sale or lease, or importation, shipment, or distribution for the purpose of selling or leasing or offering for sale or lease." *Id.* § 2.803(a). RF equipment generally must receive an equipment authorization prior to marketing. *Id.* § 2.803(b)(1).

provide jamming solutions within a correctional facility. If so, what rule changes would be required to limit the marketing of transmitters in this way? What are stakeholders' concerns, challenges, or cost considerations associated with limiting the marketing of transmitters to these entities? Have marketing restrictions been effective in other contexts? Should we also consider allowing the marketing of such equipment directly to wireless providers, in the event they provide record support for engaging with DOCs to offer a more direct solution to this issue? Further, in light of our concerns, and given that our rules do not provide restrictions on the marketing of "routinely" authorized equipment, should we implement this limitation by adopting a specific rule in our part 2 RF device marketing rules (subpart I)?[284] Such a rule could set forth the compliance requirements that apply to the responsible party associated with the part 2 equipment certification. If we adopt such a rule, in order to ensure that equipment distributors, equipment dealers, or others in the supply and distribution chains associated with marketing or sale of such equipment are aware of this restriction, should applicants be required to address compliance with the rule requirements by including a compliance plan in any certification application submitted to a TCB? Should all marketing include clear disclosures that such equipment can only be sold to DOC or solutions provider lessees or overlay licensees for the provision of jamming solutions in correctional facilities? Should specific language be required for the disclosure? Should the marketer be required to verify and retain documentation that any sale is only to a DOC or solutions provider lessee or licensee?

126. To ensure compliance with any marketing restriction that the Commission might adopt, we seek comment on the need for any or all of the following requirements. First, we could require transmitter manufacturers to have a unique stock keeping unit (SKU) identifier for each transmitter sold in the United States that is intended for use as part of a jamming solution in correctional facilities. Second, we could require that a manufacturer maintain a record of any such transmitter from manufacturing to deployment, including the location where they were shipped and installed. Should there be a reporting requirement for such records? Should the report be submitted to the Commission on an annual basis or other periodic basis? Would these types of records help with transmitter tracking and traceability in the event enforcement action is necessary due to possible unauthorized use or potential harmful interference to authorized users? Are manufacturers the best repository of this information, and are they able to effectively control who operates their equipment once sold? Third, given the likelihood that the jamming equipment would support more frequency bands than a prison facility may need, we could require manufacturers to: (1) ensure that the registered transmitters used for jamming solutions are installed and provisioned by a qualified professional trained by the manufacturers; (2) develop transmitters that contain security features sufficient to protect against software and firmware modifications by any unauthorized parties; and (3) maintain a U.S. point of contact or Responsible Party located in the United States to address and resolve, as appropriate, any issues regarding the installation and use of such a transmitter at a correctional facility. Should equipment authorizations for this type of device have an expiration date? Would an expiration date prevent the marketing of a used device if it is removed from an authorized correctional facility location, or are there other measures that would achieve this goal? Should we develop rules regarding the decommissioning or destruction of equipment used in jamming solutions at the end of its operational life? Should DOCs or solutions providers maintain a registry or otherwise retain a record that lists jamming solutions that have been deployed in correctional facilities? Should there be a reporting requirement for such records? Should the report be submitted to the Commission on an annual basis or other periodic basis? Are there any other requirements or recommendations that the Commission should consider to ensure compliance if it were to adopt a marketing restriction?

127. We also seek comment on whether to require a label on any transmitter intended for use in a jamming solution deployment in a correctional facility to warn users that the equipment can only be used by a DOC or solutions provider that has contracted to provide a jamming solution in a correctional

[284] *See generally id.* pt. 2, subpt. I.

facility as a Commission lessee or licensee. What language would sufficiently warn users in this regard? We note that RF equipment is generally allowed to satisfy Commission labeling requirements via electronic means ("e-labeling"). However, in certain instances our rules provide specific requirements for printed warnings. Given our concerns regarding the misuse of equipment for jamming solutions, should we prohibit use of e-labeling for any warning information requirements?

128. In addition, we recognize that certain Commission rules provide exceptions for importing and marketing radio frequency devices prior to equipment authorization.[285] Should we exclude equipment used to provide jamming solutions from these exceptions, or should we apply significantly more restrictive limits, while permitting such pre-equipment authorization importation? If required in any of these scenarios, what are the appropriate conditions or restrictions? What information would be needed by port authorities to ensure that any incoming equipment intended for use as part of a jamming solution is only being imported by or shipped to authorized recipients? Alternatively, rather than restricting importation, should we require that equipment intended for use in a jamming solution be manufactured or assembled in the United States to simplify efforts by our federal partners to interdict equipment imported into the United States intended for use outside of the correctional facility context? Should we restrict distribution of equipment intended for use in a jamming solution, such that the equipment may only be shipped directly from the manufacturer to a DOC or solutions provider lessee or licensee?

129. Finally, we seek comment on whether it is in the public interest to require manufacturers to employ some type of locking mechanism, if technically feasible, that would prevent any non-eligible entities from using such a transmitter outside of the correctional facilities context described herein. If so, we seek detailed comment on how to accomplish this goal. For example, would it be possible to limit the activation of a transmitter deployed as part of a jamming solution via a cloud-based operating system, perhaps controlled by geo-location, such that the device would de-activate when it is no longer used by the specific authorized operator at the relevant correctional facility? Would such a mechanism make the equipment cost-prohibitive? Are there other ways to ensure that only eligible entities are able to use the equipment for the intended public-safety related purpose? Should we require these devices to have embedded unique RF identifiers in their transmissions to facilitate their identification and location if used outside an authorized location? We seek comment on these issues and whether there are other conditions that might be appropriate to prevent transmitters authorized for correctional facility use from being diverted to uses outside of the intended locations and purposes. Commenters should discuss the costs and benefits of any proposed restrictions, requirements, or conditions in the areas of importation, marketing, and labeling, and discuss any other requirements or approaches that would further our goal of restricting the use of equipment required for jamming solutions to the limited context of correctional facilities.

D. Facilitating Other Handset-Centric Technologies

130. In the extensive effort to address the problem of contraband wireless devices in correctional facilities, the Commission has continually sought input from stakeholders on any and all viable technical solutions beyond MAS and other CIS technologies, and what regulatory steps the Commission could take to support the development and deployment of new technologies.[286] The record in this proceeding reflects comment on a variety of technologies and their relative effectiveness, viability, and challenges in their implementation. With the goal of ensuring that correctional facilities have the choice to utilize any legally permissible tool for combatting contraband wireless device use, we seek comment on whether there are other device-based solutions that should be considered for inclusion in the proposed deauthorization framework in addition to jamming solutions. We also seek comment on the best mechanism for facilitating those technologies. In the context of the proposed deauthorization

[285] *See, e.g., id.* §§ 2.1204(a)(3), (a)(4), (a)(11), and 2.803(c).

[286] *See Contraband First FNPRM*, 32 FCC Rcd at 2380-83, paras. 122-31; *Contraband Refresh PN*, 35 FCC Rcd 7910; *Contraband Second FNPRM*, 36 FCC Rcd at 11843-47, paras. 75-85.

framework proposed herein, we invite commenters to refresh the record specifically on the feasibility of geofencing, or geolocation-based denial, and beacon technology, as described in more detail below, including whether there have been technological, economic, or policy developments affecting the deployment of these technologies, and whether the Commission can play a role in promoting these tools.

131. *Geolocation-Based Denial or Geofencing Technology*. In the *Contraband Second FNPRM*, the Commission sought comment on geolocation-based denial, also known as geofencing, whereby mobile device software and/or hardware is used to disable contraband wireless devices that violate a perimeter surrounding a correctional facility.[287] Stakeholders in this proceeding expressed concerns about the technical feasibility of geofencing.[288] For example, some wireless providers maintain that they are technically incapable of employing geofencing or other network-based solutions because they do not actively track the precise geolocation of their subscribers, and moreover, a contraband device user can disable device location capabilities.[289]

132. Today, we seek to refresh the record on whether there have been technological advancements in the wireless carriers' network engineering that might make it more feasible to implement network-based geofencing around the borders of correctional facilities. A further developed record will help the Commission determine whether it is necessary to adopt rules to aid stakeholders in the deployment of geofencing technology. Are there stakeholders with real-world experience with respect to the viability of geofencing in the contraband cellphone context? We seek comment generally on whether there are any solutions providers that are developing or have developed a geolocation-based technology that could be used in correctional facilities. What network modifications would be required for wireless providers to be able to track and identify contraband wireless devices on their networks to a sufficient degree of location accuracy, and at what cost? Have there been advances in location technology that now enable wireless providers to accurately locate contraband devices in correctional facilities? Are there new device applications that enable the identification of the location of the device through GPS or other location technology located in the device? Are there novel ways to prevent the device user from disabling the location capabilities in the contraband device? Should we require wireless providers to use their own network capabilities to geolocate and disable contraband devices, and would that violate section 222 or any other statute, rule, or policy? What are the costs to wireless providers of complying with a Commission mandate in this regard? Are there other technical, privacy, legal, or other considerations relevant to this approach? We seek comment on specific rules that the Commission should amend or adopt, if any, to promote the use of geofencing as a tool available to combat contraband wireless devices in correctional facilities.

133. *Beacon Technology*. In the *Contraband Second FNPRM*, the Commission sought 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.[290] We seek comment generally on whether the Commission should facilitate beacon technology. In this proceeding, stakeholders opposing the use of beacon technology have argued that it is an infeasible solution because it would require device manufacturers to install the necessary hardware and software on every mobile device, which would take years to implement, would be exceptionally costly, and could be circumvented with legacy devices.[291] We seek

[287] *See Contraband Second FNPRM*, 36 FCC Rcd at 11844-46, paras. 80-83.

[288] Most recently, parties filed comments generally opposing geofencing in response to our *Contraband Second FNPRM*. *See, e.g.*, CTIA 2021 Comments at 9-10; T-Mobile 2021 Comments at 3; AT&T 2021 Comments at 5; OmniProphis 2021 Comments at 4.

[289] *See, e.g.*, T-Mobile 2021 Comments at 3; AT&T 2021 Comments at 5-6; CTIA 2021 Comments at 9-10.

[290] *See Contraband Second FNPRM*, 36 FCC Rcd at 11846-47, paras. 84-85.

[291] *See, e.g.*, T-Mobile 2021 Comments at 5; ShawnTech 2021 Comments at 1-2; CTIA 2021 Comments at 10.

comment on whether there have been any advancements in beacon technology that make it possible to install beacon software on mobile wireless devices remotely, e.g., through a software update. Stakeholders also maintain that, even if a software update could be used for some devices, this solution would not address legacy devices that are incapable of software updates and that could not realistically be retrofitted.[292] Further, some stakeholders have contended that beacon technologies pose a cybersecurity threat.[293]

134. We invite comment on ways in which the Commission could help overcome these potential deficiencies in beacon technology and on any updated real-world experience in using beacon technology. We note that Cell Command has claimed that its beacon technology is relatively inexpensive, highly efficient, and could be implemented quickly, but that the technology will not work without carrier participation.[294] Some stakeholders argue that a beacon solution would require the Commission to mandate software or hardware design in a way that would violate its policy of technological neutrality.[295] What authority does the Commission have to require installation of software in wireless devices and how is such an approach consistent with our policy of technological neutrality? We seek comment on what would be required in order to support beacon technology in a manner that places it on a level playing field with other technologies. What would the cost and implementation timeline be for beacon technology, and which stakeholders should bear this cost?

E. Further Facilitating and Streamlining the Authorization of Current CIS Technology

135. In the *Contraband Second FNPRM*, the Commission sought 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.[296] We seek further comment to refresh the record on this topic. What is the current status of the development and deployment of E-MAS? What further steps could the Commission take to facilitate MAS deployments? Are there new specific outreach or educational opportunities that the Commission could be engaging in to further promote stakeholder cooperation and the effectiveness of MAS and E-MAS?

136. There is substantial agreement in the current record in this proceeding that the Commission should continue to support MAS and E-MAS as tools to combat contraband wireless devices in correctional facilities.[297] The record reflects a difference of opinion, however, as to whether the Commission should mandate roaming agreements.[298] We invite updated comment on whether the Commission should mandate roaming agreements between wireless carriers and solutions providers in the correctional facility context given the vital public safety concerns. If so, using what parameters and under

[292] *See, e.g.*, T-Mobile 2021 Comments at 5 (also arguing that the solution would not address foreign devices brought into the United States); AT&T 2021 Comments at 7 (noting its skepticism that beacon software would be backwards-compatible with every handset in the United States).

[293] *See, e.g.*, CTIA 2021 Comments at 10-11.

[294] *See generally* Cell Command 2021 Comments.

[295] *See, e.g.*, T-Mobile 2021 Comments at 5; AT&T 2021 Comments at 7; CTIA 2021 Comments at 11.

[296] *Contraband Second FNPRM*, 36 FCC Rcd at 11847, para. 86.

[297] *See, e.g.*, T-Mobile 2021 Comments at 6; AT&T 2021 Comments at 2; CTIA 2021 Comments at 3-8; OmniProphis 2021 Comments at 5-6.

[298] *See, e.g.*, ShawnTech 2021 Comments at 2 (supporting a mandate for MAS Evolved where a CIS operator is FCC compliant and the carrier approves the equipment); OmniProphis 2021 Comments at 5-6 (contending that a standard contract that includes only MAS-relevant information would be helpful, as well as addressing the lack of monetary exchange); T-Mobile 2021 Comments at 6-7 (advocating against a mandate because they already freely enter into agreements with the providers, it would be contrary to Commission precedent, and regulatory guardrails would take time to implement); CTIA 2021 Comments at 6-7 (stating that the current roaming agreement process is efficient).

what timeframe? Have these agreements become more standardized? Is there still a need to mandate these types of agreements between wireless carriers and MAS providers?

137. In the *Contraband Second FNPRM*, the Commission also asked whether it should review the previously streamlined leasing rules in the correctional facility context to facilitate additional CIS deployments nationwide.[299] In response, Shawntech suggested that a process that would permit a wireless carrier to lease all call signs to a solutions provider in designated geographic areas would greatly reduce the time and effort required to expeditiously secure leases and deploy CIS systems.[300] T-Mobile advocated for a number of changes to the leasing rules, including that the Commission should modify its rules to permit qualifying leases to be subject to immediate processing notwithstanding overlap or any unjust enrichment concerns, and eliminating the lease requirement altogether for portable CIS solutions.[301] We invite stakeholders to refresh the record on the question of whether we should make any changes to our parts 1 and 20 rules to further streamline the current CIS leasing process. How can the Commission better accommodate the deployment of mobile solutions and any newer solutions that may not fit within the existing leasing framework?

138. We also seek comment on whether we should amend any other regulatory procedures in section 20.23 of the Commission's rules. In particular, we seek comment on whether we should consider making any changes to further streamline the CIS Phase 1 authorization and Phase 2 self-certification process.[302] Similarly, we seek comment on whether we should consider making changes to our disabling process.[303] In particular, should we consider extending the time period associated with the sending of qualifying requests to wireless providers for the disabling of contraband devices? Under current Commission rule section 20.23(c), a DCFO may send a qualifying request to a CMRS licensee on the sixth business day following the date of the filing of a Phase 2 self-certification, provided no objections from CMRS licensees are received.[304] Since the Bureau began receiving certifications under this process over two years ago, the Bureau has found that, despite a lack of wireless provider objection, certain filings from solutions providers have necessitated discussion with Bureau staff and the filing of amended certifications.[305] This has resulted in a delay in the posting of a correctional facility as approved for disabling on the CIS status tracker located on the Commission's website.[306] We therefore seek comment on extending the time period necessary for receipt of wireless provider objections *and* Commission staff review of the certification filing. In the alternative, to account for the potential necessary back and forth discussion with stakeholders, the filing of required amendments and staff review of same, should we clarify by rule that a DCFO can submit a qualifying request, provided there are no wireless provider objections received within five business days, on the date the Bureau updates the Commission's website to reflect certification of a specific facility?

---

[299] *Contraband Second FNPRM*, 36 FCC Rcd at 11848, para. 88.

[300] ShawnTech 2021 Comments at 3.

[301] *See* T-Mobile 2021 Comments at 8-9.

[302] 47 CFR § 20.23(b).

[303] *Id.* § 20.23(c).

[304] *See id.*

[305] *See, e.g.*, *Promoting Technological Solutions to Combat Contraband Wireless Devices Use In Correctional Facilities*, Supplement to SOC LLC – Contraband Interdiction System Site Based Testing and Self-Certification under Section 20.23(b)(3)(ii) of the Commission's rules, GN Docket No. 13-111 (July 5, 2024) (supplementing SOC LLC's initial self-certification filing for this particular facility dated February 29, 2024).

[306] *See* FCC, *Disabling Process: CIS/Correctional Facility Approval Status Tracker*, https://www.fcc.gov/wireless/bureau-divisions/mobility-division/contraband-wireless-devices/disabling-process (last visited Sept. 3, 2025).

139. We note that in the *Contraband Second R&O*, the Commission created obligations that required a licensee, upon receipt of a qualifying request, to (1) disable the contraband wireless device from using the wireless provider's network at both the device and subscriber level, and (2) take reasonable and practical steps to prevent the contraband wireless device from being used on another wireless provider's network.[307] As it specifically pertains to the latter obligation, the Commission did not specifically state how the wireless provider should meet this obligation.[308] Instead, it provided an example that the wireless provider could meet this obligation "by adding the equipment identifier to the Stolen Phone Database."[309] We seek comment on whether stakeholders believe that we should revisit this requirement to further clarify the wireless provider's obligations in any way. Commenters should provide specific information and describe how the process has worked thus far.

F. Other Technological Solutions

140. We seek comment generally on whether there are other technologies currently available or under development, beyond those identified above as "handset-centric" technologies, that could be used in correctional facilities to combat contraband devices. If so, what steps could the Commission take to facilitate deployment of those technologies? We also seek comment on whether there are other studies, standards, efforts, or analyses regarding the effectiveness of CISs or other related solutions that we should consider in this proceeding. If so, we ask that commenters identify them and explain why they should be considered. Finally, we invite comment on other possible approaches to resolving this issue, and the costs and benefits of such approaches, that we should consider in addition to those discussed in this *Third Further Notice*.

G. Costs and Benefits

141. Overall, the goal of this *Third Further Notice* is to consider expansion of technological options for combating contraband wireless device use in correctional facilities. The benefits of the proposed rule amendments include reduced criminal activity resulting from inmates' use of contraband wireless devices, which can impact the safety of prison officials and employees, the prison population, and members of the general public. The costs of the proposed rule amendments include the need for considerable stakeholder cooperation and a commitment, particularly from DOCs, to make the expenditures necessary to ensure that jamming solutions are installed, deployed, and maintained in such a manner as to avoid harmful interference to non-contraband devices located outside a correctional facility, as well as non-contraband devices that might be permitted within a particular correctional facility, depending on state or local law or policies (e.g., devices used by vendors, attorneys, or medical personnel). We seek comment on all costs and benefits associated with adopting the proposals set forth in this *Third Further Notice*. Comments should be accompanied by specific data and analysis supporting claimed costs and benefits.

IV. PROCEDURAL MATTERS

142. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA),[310] requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemaking proceedings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[311] Accordingly, the Commission

[307] *Contraband Second R&O*, 36 FCC Rcd at 11833-34, paras. 51-52; 47 CFR § 20.23(c)(3)(i).

[308] *Contraband Second R&O*, 36 FCC Rcd at 11833-34, para. 52.

[309] *Id.*; *see also id.* at 11833-34, para. 52 n.117 (stating "CellBlox suggests that the devices be disabled and entered into the Stolen Phone Database so that they are permanently disabled.").

[310] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[311] *Id.* § 605(b).

has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning potential rule and policy changes contained in this *Third Further Notice of Proposed Rulemaking* (*Third Further Notice*). The IRFA is set forth in Appendix B. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the *Third Further Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

143. *Initial Paperwork Reduction Act Analysis*. This *Third Further Notice of Proposed Rulemaking* may contain potential new or revised information collection requirements. Therefore, we seek comment on potential new or revised information collections subject to the Paperwork Reduction Act of 1995.[312] If the Commission adopts any new or revised information collection requirements, the Commission will publish a notice in the Federal Register inviting the general public and the Office of Management and Budget to comment on the information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

144. *Providing Accountability Through Transparency Act*. Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document is available on https://www.fcc.gov/proposed-rulemakings.

145. *Ex Parte Presentations.* The proceeding this *Third Further Notice* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[313] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in the proceeding should familiarize themselves with the Commission's *ex parte* rules.

146. *Comment Period and Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). Commenters should refer to GN Docket No. 13-111 when filing in response to this *Third Further Notice of Proposed Rulemaking*.

- *Electronic filers*: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs.

[312] Paperwork Reduction Act of 1995, Pub. L. No. 104-13, 109 Stat. 163 (1995).

[313] 47 CFR § 1.1200 *et seq.*

- *Paper filers*: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. **All filings must be addressed to the Secretary, Federal Communications Commission.**
    - Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.

147. *Availability of Documents*. Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS.

148. *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the FCC's Consumer and Governmental Affairs Bureau at 202-418-0530 (voice).

149. *Additional Information.* For additional information on this proceeding, contact combatcontraband@fcc.gov.

V. ORDERING CLAUSES

150. IT IS ORDERED, pursuant to the authority found in sections 1, 2, 4(i), 4(j), 301, 302, 303, 307–310, 319, 324, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 301, 302a, 303, 307–310, 319, 324, and 332, and section 1.411 of the Commission's rules, 47 CFR § 1.411, that this *Third Further Notice of Proposed Rulemaking* IS HEREBY ADOPTED.[314]

151. IT IS FURTHER ORDERED that the Commission's Office of the Secretary SHALL SEND a copy of this *Third Further Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch

Secretary

[314] Pursuant to Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 20, 2025), this regulatory action has been determined to be not significant under Executive Order 12866, 58 Fed. Reg. 68708 (Dec. 28, 1993).

APPENDIX A

Proposed Rules

The Federal Communications Commission proposes to amend 47 CFR parts 1, 15, and 90 as follows:

Part 1 – Practice and Procedure

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

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. § 2461 note; 47 U.S.C. 1754, unless otherwise noted.

2. Section 1.903 is amended by revising paragraph (c) to read as follows:

§ 1.903 Authorization required.

* * * * *

(c) Subscribers. Authority for subscribers to operate mobile or fixed stations in the Wireless Radio Services, except for certain stations in the Rural Radiotelephone Service and except for any fixed or mobile station that is considered a contraband wireless device, as defined in § 1.9003 of this chapter, is included in the authorization held by the licensee providing service to them. Subscribers are not required to apply for, and the Commission does not accept, applications from subscribers for individual mobile or fixed station authorizations in the Wireless Radio Services, and individual authorizations for contraband wireless devices are not permitted. Individual authorizations are required to operate rural subscriber stations in the Rural Radiotelephone Service, except as provided in § 22.703 of this chapter. Individual authorizations are required for end users of certain Specialized Mobile Radio Systems as provided in § 90.655 of this chapter. In addition, certain ships and aircraft are required to be individually licensed under parts 80 and 87 of this chapter. See §§ 80.13, 87.18 of this chapter.

3. Section 1.9003 is amended by revising the definition of "Contraband Interdiction System" and adding the definition of "Jamming Solution" in alphabetical order to read as follows:

Contraband Interdiction System. A Contraband Interdiction System is a system that transmits radio communication signals comprised of one or more stations used only in a correctional facility to: (1) provide a jamming solution, subject to the special provisions of § 1.9041 of this chapter; (2) prevent transmissions to or from contraband wireless devices within the boundary of the facility, while being capable of distinguishing transmissions from contraband and non-contraband wireless devices; and/or (3) obtain identifying information from a contraband wireless device.

* * * * *

Jamming Solution. A Jamming Solution is the deployment of RF transmitter(s) within a correctional facility to prevent contraband wireless devices from establishing or maintaining a connection with a network.

* * * * *

4. Section 1.9041 is added to read as follows:

§ 1.9041 Special provisions relating to spectrum leasing arrangements for a jamming solution in correctional facilities.

(a) ***Eligibility criteria.*** An entity seeking to engage in spectrum leasing as a lessee under this section may do so if it is a department of corrections with authority over the correctional facility for which the lease is sought, or a solutions provider that has entered into a contract with a department of corrections with authority over the correctional facility for which the lease is sought.

(b) ***Application requirements.*** An entity seeking to engage in spectrum leasing as a lessee under this section must provide a certification as an attachment to FCC Form 608 stating that the entity: (1) meets the eligibility criteria; and (2) seeks to deploy equipment with a valid equipment authorization under part 2 of this chapter.

(c) ***Subleasing.*** Notwithstanding the provisions of §§ 1.9020(l) and 1.9030(k), a spectrum lessee authorized to provide a jamming solution may not sublease spectrum usage rights.

(d) ***Construction/performance requirements.*** Notwithstanding the provisions of §§ 1.9020(d)(5)(i) and 1.9030(d)(5)(i), a licensee may not attribute to itself the build-out or performance activities of its spectrum lessee(s) providing a jamming solution for purposes of complying with any applicable performance or build-out requirement.

(e) ***Good faith negotiations.*** CMRS licensees must negotiate in good faith with entities seeking to deploy a jamming solution in a correctional facility. Upon receipt of a good faith request by such an entity, a CMRS licensee must negotiate toward a lease agreement. If, after a 45-day period, there is no agreement, the entity seeking to operate a jamming solution in the absence of CMRS licensee consent may file an application for a part 90 non-exclusive overlay license for a jamming solution on FCC Form 601, as described in § 90.1403 of this chapter, accompanied by evidence demonstrating its good faith, and the lack of good faith on the part of the CMRS licensee(s), in negotiating a lease arrangement.

Part 15 – Radio Frequency Devices

3. The authority citation for part 15 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, 304, 307, 336, 544a, and 549.

4. Section 15.5 is amended by adding paragraph (e) to read as follows:

§ 15.5 General conditions of operation.

* * * * *

(e) Operation of devices as part of a jamming solution, as defined in § 1.9003 of this chapter, is prohibited under this part, even under power levels that comply with the limits set forth in this part. Any jamming solution must be authorized pursuant to §§ 1.9041 or 90.1401, or a combination thereof, of this chapter.

5. Section 15.201 is amended by adding paragraph (e) to read as follows:

§ 15.201 Equipment authorization requirement.

* * * * *

(e) An intentional radiator intended for use as part of a jamming solution, as defined in § 1.9003 of this chapter, is not eligible for certification under part 15 pursuant to the Commission's part 2, subpart J Equipment Authorization Procedures.

Part 90 – Private Land Mobile Radio Services

5. The authority citation for part 90 continues to read as follows:

Authority: 47 U.S.C. 154(i), 161, 303(g), 303(r), 332(c)(7), 1401–1473.

6. A new subpart AA is added to read as follows:

Subpart AA Regulations Governing the Licensing of Jamming Solutions.

§ 90.1401 Eligibility.

An entity is eligible to apply for an overlay license for the provision of a jamming solution (as defined in § 1.9003 of this chapter) under this subpart if it:

(1) Is a department of corrections with authority over the correctional facility for which authority to implement a jamming solution therein is sought, or is a solutions provider that has entered into a contract with a department of corrections with authority over a correctional facility for which authority to implement a jamming solution therein is sought; and

(2) Meets the good faith negotiation requirements specified in § 1.9041(d) of this chapter.

§ 90.1403 Application requirements.

(a) ***Jamming overlay license application requirements.*** An overlay license applicant seeking authority to provide a jamming solution in a correctional facility must apply using FCC Form 601in the Commission's Universal Licensing System (ULS) in accordance with part 1, subpart F of this chapter. All modifications or renewals of licenses and associated waiver requests must also be filed on FCC Form 601 in the Commission's Universal Licensing System (ULS) in accordance with part 1, subpart F. The entity seeking an overlay license under this section must provide with its FCC Form 601 the following information:

(1) A certification regarding its eligibility as specified in § 90.1401;

(2) A certification that it seeks to deploy equipment as part of a jamming solution with a valid equipment authorization under part 2 of this chapter;

(3) A description of the jamming solution to be deployed at the correctional facility demonstrating that the applicant is prepared to deploy a solution that does not interfere with authorized devices, including technical parameters, and the service area associated with the proposed operations; and

(4) A declaration in accordance with § 1.16 of this chapter.

(b) ***Authorization of jamming solutions.*** An overlay license for a jamming solution in a correctional facility is deemed effective only after the following actions are completed:

(1) Conditional grant of an overlay license application for the specified geographic area;

(2) Satisfaction of the condition(s) of the overlay license following on-site testing at the correctional facility demonstrating to the Commission, through the filing of a certification, that the system functions as expected and within the licensed area, protecting authorized users within and outside the correctional facility from harmful interference; and

(3) Grant of final Commission authority to provide a jamming solution at the correctional facility following successful on-site testing.

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Third Further Notice of Proposed Rulemaking* (*Third Further Notice*) assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *Third Further Notice*. The Commission will send a copy of the *Third Further Notice*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *Third 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 the *Third Further Notice*, the Commission aims to strengthen public safety through the removal of regulatory barriers to the deployment and viability of existing and developing technologies that can assist the ability of correctional facilities to stem the use of contraband wireless devices in correctional facilities, which can be used to engage in criminal activity. The proposals contained in the *Third Further Notice* build upon prior Commission actions and seek to meet our objectives of expanding the scope of technical options available to corrections officials, while simultaneously fostering a collaborative environment among key stakeholders, including departments of correction (DOCs), solutions providers, and wireless providers. To achieve these goals, the Commission seeks comment on a broad range of potential actions intended to help eliminate a continuing public safety threat, reduce regulatory burdens, and also continue the growth of currently deployed technologies, commonly known as contraband interdiction systems (CISs), while ensuring that the Commission's rules evolve to afford consistent regulatory treatment across technologies, some of which are operated by small entities.

3. As a first step, the *Third Further Notice* proposes to deauthorize subscriber operation of contraband wireless devices in correctional facilities. The proposed deauthorization rule is intended to facilitate the use of jamming solutions consistent with section 333 of the Communications Act of 1934, as amended (the Act),[4] and is a key step towards permitting corrections officials to engage with wireless providers to use jamming solutions or other technologies in the limited context of combatting contraband wireless devices in correctional facilities. The Commission's lead licensing proposal would involve the participation of wireless providers, so as to help prevent harmful interference to legitimate users, a long-standing wireless industry concern.

4. In addition, the proposed approach ensures that a contraband wireless device located in a correctional facility would not be considered, for purposes of section 301 of the Act,[5] a "station licensed or authorized by or under [the] Act"[6] and, therefore, would not be afforded protection against willful or malicious interference by other technologies, such as jamming solutions, that have been approved under our proposed process. The *Third Further Notice* proposes to apply the deauthorization rule to subscriber

[1] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *Id.* § 603(a).

[3] *Id*.

[4] 47 U.S.C. § 333.

[5] *Id*. § 301.

[6] *Id.* § 333.

operation of a contraband wireless device that is used in a correctional facility in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy, consistent with the approach that the Commission took in prior decisions to facilitate CISs. The *Third Further Notice* also seeks comment on only applying a jamming solutions approach to a narrower group of correctional facilities (e.g., only those located in jurisdictions that impose criminal penalties for possessing or using contraband wireless devices, or for delivering or attempting to deliver those devices to prison inmates).

5. Recognizing that the proposed deauthorization rule would make operation of any contraband wireless device a violation of section 301 of the Act and revised section 1.903(a) of the Commission's rules, the *Third Further Notice* also proposes to create a "safe harbor" wherein the Commission would take no enforcement action against a wireless provider, to the extent it might be liable, for unauthorized operation of contraband wireless devices in a correctional facility if certain conditions exist. Specifically, the proposed safe harbor would apply to (1) wireless providers licensed in a geographic area where no DOC is actively seeking to implement a technology solution, including jamming, to combat contraband devices; and (2) any wireless provider that is (a) actively participating in good faith negotiations (or has successfully completed such negotiations) with the DOC/solutions provider that is seeking to lease spectrum to authorize operation of a CIS solution, including jamming.

6. The *Third Further Notice* also seeks to establish the framework whereby correctional facilities or solution providers that contract with them can become authorized to deploy an expanded range of technological solutions to combat contraband wireless devices. The Commission's lead proposal in the *Third Further Notice* is to authorize jamming solutions in correctional facilities by applying its existing secondary markets framework. The Commission's goal and expectation is that wireless providers will reach agreement with DOCs and solutions providers on lease terms for authorized jamming solutions, in the same way that parties have, to date, successfully negotiated in good faith for CIS deployments. The *Third Further Notice* seeks comment on, among other things, the types of leases parties may wish to utilize, eligibility criteria, and a requirement for good faith negotiations.

7. As a method of last resort, in cases where parties fail to reach a good faith leasing arrangement, the Commission proposes to permit eligible entities to directly apply for a non-exclusive overlay license to deploy a jamming solution in a correctional facility provided certain conditions are met. The *Third Further Notice* seeks comment on a variety of issues related to the framework for issuing a last resort overlay license, including licensing and operating rules, license term and renewal, application procedures, and technical parameters of the overlay licenses. The *Third Further Notice* also seeks comment on other issues related to the deployment of jamming solutions. For example, the Commission seeks comment on authorizing jamming solutions on Wi-Fi spectrum and part 25 satellite spectrum, in order to ensure that that the proposed authorization framework is broad enough to include all spectrum that may be used to communicate with contraband wireless devices.

8. In addition, the Commission seeks comment on possible measures to ensure that jamming solutions are limited solely to correctional facilities. For example, the *Third Further Notice* proposes an express prohibition against certifying any transmitter utilizing jamming solutions pursuant to part 15 of the Commission's rules and against the operation of such equipment under part 15 to ensure that the proposed deauthorization framework does not result in low-power, hand-held jamming devices being produced, marketed, and sold in the United States for use on a part 15 unlicensed basis. The Commission also seeks comment on the appropriate procedures for the certification of equipment used to provide jamming solutions in correctional facilities, and on the extent to which it is necessary to specifically limit the marketing and sale of such transmitters directly to DOCs and solutions providers that contract with them to provide jamming solutions.

9. Finally, the Commission seeks comment on whether there are other device-based solutions that should be considered for inclusion in the proposed deauthorization framework in addition to jamming solutions. In the context of the proposed deauthorization framework, the *Third Further Notice* invites commenters to refresh the record specifically on the feasibility of geofencing, or geolocation-

based denial, and beacon technology, whether there have been technological, economic, or policy developments affecting the deployment of these technologies, and whether the Commission can play a role in promoting these tools.

B. Legal Basis

10. The proposed action is authorized pursuant to sections 1, 2, 4(i), 4(j), 301, 302, 303, 307–310, 319, 324, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 301, 302a, 303, 307–310, 319, 324, and 332, and section 1.411 of the Commission's rules, 47 CFR § 1.411.

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

11. 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.[7] The RFA generally defines the term "small entity" as having the same meaning as under the Small Business Act.[8] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act."[9] 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 SBA.[10]

12. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[11] In general, a small business is an independent business having fewer than 500 employees.[12] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[13] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant their field.[14] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[15] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[16] Based on the 2022 U.S.

---

[7] 5 U.S.C. § 604 (a)(4).

[8] *Id.* § 601(6).

[9] *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."

[10] 15 U.S.C. § 632.

[11] 5 U.S.C. § 601(3)-(6).

[12] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[13] *Id*.

[14] 5 U.S.C. § 601(4).

[15] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[16] 5 U.S.C. § 601(5).

Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[17]

13. The actions taken in the *Third Further Notice* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[18] codes and corresponding SBA size standard.[19]

Regulated Industry (NAICS Classification)	NAICS Code	SBA Size Standard	Total Firms[20]	Small Firms[21]	% Small Firms in Industry
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	656	624	95.12
Other Communications Equipment Manufacturing	334290	750 employees	321	310	96.57
Wireless Telecommunications Carriers (except Satellite)[22]	517112	1,500 employees	2,893	2,837	98.06
Telecommunications Resellers[23]	517121	1,500 employees	1,386	1,375	99.21
Satellite Telecommunications	517410	$47 million	275	242	88.00
All Other Telecommunications	517810	$40 million	1,079	1,039	96.29
Engineering Services	541330	$34 million	37,462	34,803	92.90

[17] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[18] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[19] The size standards in this chart are set forth in 13 CFR 121.201 by six digit NAICS code.

[20] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, *and 2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM.

[21] *Id.*

[22] Affected Entities in this industry include 3650-3700 MHz Band, 600 MHz Band, Advanced Wireless Services - AWS Services, Broadband Personal Communications Service, Cellular Radiotelephone Service, Lower 700 MHz Band Licenses, Specialized Mobile Radio Licenses, Upper 700 MHz Band Licenses, and Wireless Communications Services.

[23] Affected Entities in this industry include 800 and 800-Like Service Subscribers, IMTS Resale Carriers, Local Resellers, Payphone Service Providers, Prepaid Calling Card Providers, Toll Resellers, and Wireless Resellers.

Regulated Industry (NAICS Classification)	NAICS Code	SBA Size Standard	Total Firms[20]	Small Firms[21]	% Small Firms in Industry
Facilities Support Service	561210	$47 million	1,922	1,783	92.77
Security Guards and Patrol Services	561612	$47 million	76	76	100.00
All Other Support Services	561990	$16.5 million	9,615	9,350	97.24
Correctional Institutions	922140	No SBA Size Standard	1,677[24]	813	48.48

14. Based on currently available U.S. Census data regarding the estimated number of small firms in each identified industry, we conclude that the adopted rules will impact a substantial number of small entities. Where available, we provide additional information regarding the number of potentially affected entities in the above identified industries, and information for other affected entities, as follows.

2024 Universal Service Monitoring Report Telecommunications Service Provider Data[25] (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Toll Resellers	411	398	96.84
Wireless Telecommunications Carriers (except Satellite)[26]	585	498	85.13

15. *Experimental Radio Service (Other Than Broadcast).* Neither the SBA nor the Commission have developed a size standard for this industry. Experimental Radio Service is a service in which radio waves are employed for purposes of experimentation in the radio art or for purposes of providing essential communications for research projects that could not be conducted without the benefit of such communications.[27] The majority of experimental licenses are issued to companies such as Motorola and Department of Defense contractors such as Northrop Grumman and Lockheed Martin. Large businesses such as these are the primary applicants for such licenses and may have as many as 200 licenses at one time. For the purposes of this regulatory flexibility analysis, using the SBA's Office of Advocacy's general definition that a small business is an independent business having fewer than 500 employees,[28] the Commission estimates that 30 percent of applications, will be awarded to small entities.

[24] *See* U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, *Census of State and Federal Adult Correctional Facilities, 2019 - Statistical Tables* (NCJ 301366, BJS) (Nov. 2021) (*2019 CCF*), https://bjs.ojp.gov/content/pub/pdf/csfacf19st.pdf.

[25] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[26] Affected Entities in this industry include all reporting wireless carriers and service providers.

[27] 47 CFR § 5.5.

[28] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* 1 (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

(continued….)

The Commission processes approximately 1,000 applications a year for experimental radio operations. About half, or 500 of these are renewals and the other half are for new licenses. We do not have adequate information to predict precisely how many of these are from small entities. However, based on the above figures we estimate that as many as 300 of these applications could be from small entities and could potentially be impacted.

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

16. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.[29]

17. In the *Third Further Notice*, the Commission seeks public comment on a potential framework that would increase the radio frequency (RF) options that DOCs could utilize to combat contraband wireless device use in correctional facilities. There are three classes of small entities that might be impacted: correctional facilities, solutions providers, and providers of wireless services. For all of these entities, the Commission first proposes to leverage its existing leasing rules applicable to CISs as much as possible to reduce regulatory burdens and continue expedited processing for these important solutions. With this intent in mind, the *Third Further Notice* seeks comment on the extent to which the Commission's rules require amendment to effectuate authorization through lease arrangements of transmitters operating on wireless provider licensed commercial spectrum to deploy jamming solutions in correctional facilities. Small and other entities are encouraged to comment on any potential regulatory burdens or costs incurred in connection with these proposals, if adopted. We also encourage suggestions from small and other entities on ways in which the Commission may minimize any required information collections, while ensuring that all parties meet the desired goals of providing an additional tool toward combating contraband wireless device use, and that only non-authorized devices are impacted.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

18. The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities.[30] The discussion is required to include alternatives such as: "(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 such 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 such small entities."[31]

19. As discussed above, in the *Third Further Notice*, the Commission seeks public comment on a proposed framework that seeks to increase the RF options that DOCs could utilize to better combat contraband wireless device use. Additionally, the Commission seeks comment on several regulatory alternatives that might reduce impacts on small entities. For example, the Commission seeks to leverage its current licensing process and existing leasing rules applicable to CISs, which small and other correctional facilities and/or solution providers that contract with correctional facilities have successfully

(Continued from previous page)

[29] 5 U.S.C. § 603(b)(4).

[30] *Id.* § 603(c).

[31] *Id.* § 603(c)(1)-(4).

used for more than a decade, rather than creating a completely new paradigm. Many entities that may be interested in participating in the framework proposed in the *Third Further Notice* may already be engaged in the process of combatting contraband wireless devices by the processes currently available, specifically for CISs. By leveraging the Commission's current spectrum leasing rules, small entities – be they solutions providers, or even the DOCs, as well as wireless providers – will already be familiar with the processes, thereby decreasing any new regulatory burdens and, by extension, minimizing significant economic impact to such entities.

20. The *Third Further Notice* also proposes a safe harbor for wireless providers to avoid potential liability for unauthorized operation of subscriber devices that fall within the proposed deauthorization rule, as well as direct jamming solution authorization mechanisms. The safe harbor will provide wireless providers with assurance that they will not be subject to enforcement action, provided they either: have not received a specific request to lease their spectrum to support the authorization of a jamming solution or, if they have received such a request, they negotiated a good faith leasing arrangement with a DOC or its contracted solutions provider.

21. The Commission invites comment on its proposed deauthorization rule and framework for facilitating the authorization of jamming solutions. Through these comments, the Commission seeks to develop final rules that combat the exigent public safety concerns of contraband wireless device use in correctional facilities, while also minimizing economic and other compliance burdens on small and other entities to the greatest extent possible.

22. To clarify and simplify compliance and reporting requirements for impacted small and other entities, the *Third Further Notice* also invites comment regarding the prospective needs of the entities and the various approaches that can be taken to accommodate those needs in both a leasing arrangement and in a direct overlay licensing approach. In so doing, 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. 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.

23. 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 *Third 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 *Third Further Notice* to combat wireless contraband use in correctional facilities. Importantly, the *Third Further Notice* gives small entities the ability to submit cost-benefit analyses, 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 it may adopt.

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

24. None.