October 29, 2026

FCC FACT SHEET*

Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities

Third Report and Order and Fourth Further Notice of Proposed Rulemaking - GN Docket No. 13-111

Background: The Commission has acted for more than a decade to combat the scourge of contraband wireless device use in correctional facilities, but the problem persists. This Third Report and Order (Order) would authorize non-federal operation of radio frequency jamming solutions in the limited context of correctional facilities, in compliance with applicable congressional statutes. This Fourth Further Notice of Proposed Rulemaking (FNPRM) would seek comment on a proposed framework to authorize jamming solutions on unlicensed spectrum, the application of jamming solutions to satellite communications, and potential additional safeguards.

What the Order Would Do:

- Deauthorize wireless devices in correctional facilities that are deemed contraband through a federal, state, or local statute, or a correctional facility rule, regulation, or policy, so that the deployment of jamming solutions in correctional facilities will comply with the statutory prohibition against willful or malicious interference to authorized stations.
- Apply the deauthorization rule to contraband wireless devices operating on traditional commercial wireless bands, as well as FirstNet (Band 14) in this limited context, to prevent spectrum gaps for inmates to exploit.
- Enable the authorization of jamming solutions through non-exclusive overlay licensing, while permitting leasing as an available option where parties reach mutual agreement.
- Require both a one-time proof-of-concept test at a correctional facility pursuant to an experimental license and pre-operational testing at facilities where jamming solutions will be deployed, to decrease the risk of harmful interference to authorized users.
- Require an annual certification to ensure the ongoing accuracy and reliability of a jamming solution.
- Adopt technical parameters and safety features for jamming solutions, including a network monitoring requirement, a locking mechanism requirement, and interference resolution procedures that include the cessation of jamming operations pending the resolution of credible complaints of harmful interference, as well as marketing, labeling, and importation rules.
- Require compliance with existing equipment authorization procedures for certification and prohibit certification for equipment used under our unlicensed rules.
- Revise our rules to increase flexibility for the authorization of CIS technologies.

* 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. 26-74 and WT Docket No. 24-629, 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*.

What the FNPRM Would Do:

- Propose and seek comment on a framework to deauthorize unlicensed part 15 operations in correctional facilities and ways to authorize deployment of jamming solutions on unlicensed spectrum.
- Seek comment on the application of jamming solutions to satellite communications.
- Seek comment on additional safeguards for jamming solutions, including potential adjustments to wireless provider networks, and compliance or monitoring obligations to protect authorized users, including vital public safety operations.
- Seek comment on the establishment of "quiet zones" in and around certain correctional facilities.

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 REPORT AND ORDER AND FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING*

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

Comment Date: 60 days after date of publication in the Federal Register
Reply Comment Date: 90 days after date of publication in the Federal Register

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND AND OVERVIEW 2
III. THIRD REPORT AND ORDER 7
A. Definition of Jamming Solution, Jamming Device, and Jamming Containment Area 8
B. Deauthorizing Contraband Wireless Devices in Correctional Facilities 13
1. Deauthorization Mechanism and Amendment to Section 1.903 14
2. Safe Harbor 24
3. Commission Authority to Deauthorize Contraband Wireless Devices and to Authorize Jamming Solutions Under Section 301 29
a. Arguments that Permitting Jamming Violates the Communications Act 31
b. Arguments that Permitting Jamming Violates the Administrative Procedure Act 48
C. Authorization of Jamming Solutions in the Public Interest 63
1. Table of Allocations 67
2. Proof of Concept Test 69
3. Non-Exclusive Overlay Licensing 76
a. Regulatory Matters 79
b. Application Process and Procedures 110
4. Leasing Arrangements 122

* This document has been circulated for tentative consideration by the Commission at its November 19, 2026 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.

a. Regulatory Matters 127
5. Technical Parameters 154
6. Part 15 Prohibition 194
7. Part 2 Equipment Authorization 196
8. Marketing, Labeling, and Importation of Jamming Devices 204
D. Facilitating Other Interdiction Technologies 212
E. Further Facilitating and Streamlining the Authorization of CIS Technology 215
F. Costs and Benefits 218
IV. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING 222
A. Unlicensed Operations Under Part 15 224
B. Satellite Operations Under Part 100 252
C. Additional Safeguards for Jamming Solutions 261
D. Quiet Zones 264
V. PROCEDURAL MATTERS 267
VI. ORDERING CLAUSES 277
APPENDIX A: FINAL RULES
APPENDIX B: PROPOSED RULES
APPENDIX C: FINAL REGULATORY FLEXIBILITY ANALYSIS
APPENDIX D: INITIAL REGULATORY FLEXIBILITY ANALYSIS

I. INTRODUCTION

1. Today, we take an unprecedented step toward making the United States of America a safer place. For more than a decade, the Commission has acted to combat the scourge of contraband wireless device use in correctional facilities, from streamlining the process of deploying contraband interdiction systems, to adopting a framework requiring wireless providers to disable these devices. Despite these efforts, the problem persists and the corrections community seeks further Commission action authorizing non-federal jamming technologies. For far too long, the Commission has cited statutory constraints as a bar to authorizing any form of jamming. But today, we increase the availability of technical options for corrections officials by legalizing non-federal operation of radio frequency jamming solutions in the narrow context of correctional facilities, in compliance with applicable congressional statutes. Our groundbreaking action takes a cue from congressional leaders, such as Senator Tom Cotton and Representative David Kustoff, who proposed key legislation and who, along with a multitude of bipartisan state attorneys general, continue to highlight the critical need for alternatives to meet this public safety challenge. In a clear win for the American people, we facilitate corrections officials' efforts to protect innocent individuals from the ever-growing criminal activity perpetrated by inmates' use of contraband wireless devices. We stress that our action does not require the corrections community to adopt a jamming solution, but makes available another potential tool to combat this ongoing threat where doing so makes sense.

II. BACKGROUND AND OVERVIEW

2. As the Commission has acknowledged throughout this proceeding, the use of contraband wireless devices by inmates in correctional facilities is unrelenting and continues to threaten the safety of prison officials and employees, the prison population, and members of the general public.[1] The problem remains notwithstanding Commission action facilitating the deployment of technological solutions, including: (1) authorizing and streamlining the leasing process to deploy contraband interdiction systems

[1] The Commission first initiated a proceeding on this important public safety issue in 2013. *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Notice of Proposed Rulemaking, 28 FCC Rcd 6603 (2013).

(CISs), typically managed access systems (MAS) and MAS Evolved (E-MAS),[2] and (2) establishing a regulatory framework whereby wireless providers are required to disable contraband wireless devices upon the submission of a qualifying request by a designated correctional facility official (DCFO).[3] These Commission actions are consistent with section 333 of the Communications Act as amended (Act), which prohibits any person from willfully or maliciously interfering with or causing interference to the radio communications of any station licensed or authorized by or under the Act, or operated by the U.S. Government.[4] In the past, the Commission has stated that, because jamming solutions use transmitters to willfully interfere with stations authorized by the Commission, non-federal entities are prohibited from using jamming technology to interfere with contraband wireless devices in correctional facilities.[5]

3. In September 2025, the Commission adopted a *Third Further Notice of Proposed Rulemaking* (*Third FNPRM*) proposing to authorize non-federal operation of radio frequency (RF) jamming in correctional facilities in response to continued calls by congressional leaders, state attorneys general, and state corrections officials to leverage additional tools in their ongoing efforts to combat contraband cellphones.[6] Specifically, to comply with section 333, the Commission proposed to deauthorize subscriber operation of contraband wireless devices in correctional facilities.[7] The Commission proposed to leverage its existing leasing process as a preferred approach to licensing jamming solutions,[8] while also proposing and seeking comment on an overlay licensing mechanism where parties fail to reach a leasing arrangement negotiated in good faith.[9] The Commission also proposed and sought comment on restrictions that might be necessary to ensure that jamming solutions are limited to correctional facility use, and to mitigate the risk that these solutions could be deployed in other contexts.[10] Finally, the Commission sought further comment on other technological solutions, and

[2] *See Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2236 (2017) (*First R&O* and *First FNPRM*, respectively). For an explanation of these CIS technologies, including detection systems, *see Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Third Further Notice of Proposed Rulemaking (2025) (*Third FNPRM*), 40 FCC Rcd 8001, 8004, para. 5, n.11, n.12, and n.13.

[3] *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) (*Second R&O* and *Second FNPRM*, respectively). *See also* 47 CFR § 20.23.

[4] *See* 47 U.S.C. § 333.

[5] *See Third FNPRM*, 40 FCC Rcd at 8008, para. 13, n.44 ("[N]on-federal entities currently are prohibited from using jamming technology to interfere with contraband wireless devices in correctional facilities."). We note that in a recent Declaratory Ruling, the Wireless Telecommunications Bureau stated, in the context of counter-unmanned aircraft systems, that the federal government is exempt from the application of section 333 of the Act. The Bureau clarified the conditions under which non-federal entities acting on behalf of or under the oversight of the federal government may receive the benefit of the federal government's exemption. *See Application of Section 333 of the Communications Act to Development of Operations of Counter-Unmanned Aircraft Systems for the Federal Government and under the SAFER SKIES Act, Unleashing Drone Dominance*, GN Docket No. 26-74, Declaratory Ruling, DA 26-655 (WTB July 2, 2026); Petition for Reconsideration and/or Clarification of CTIA (filed Aug. 3, 2026).

[6] *See generally Third FNPRM*.

[7] *Third FNPRM*, 40 FCC Rcd at 8013-18, paras. 23-34.

[8] *Id*. at 8019-35, paras. 36-71.

[9] *Id.* at 8035-48, paras. 72-108.

[10] *Id*. at 8053-58, paras. 120-29.

whether it is necessary for us to take regulatory steps to support their development and deployment, and on whether we should further streamline the authorization of current CIS technology.[11]

4. In response to the *Third FNPRM*, the Commission received over 100 filings during the comment and reply comment period from a wide variety of stakeholders, including departments of corrections (DOCs), solutions providers, wireless providers, public safety entities, public interest and advocacy groups, and trade associations. There is universal agreement that there are significant public safety concerns raised by contraband wireless device use in correctional facilities.[12] The Correctional Leaders Association (CLA) affirms that the contraband threat is "pervasive and growing."[13] Members of the South Carolina corrections and law enforcement community describe the ongoing criminal activity stemming from contraband cell phones in prisons and the urgent need for the Commission to authorize jamming.[14] Commenters in support of the authorization of jamming solutions, including the DOCs,

[11] *Id.* at 8059-63, paras. 134-143.

[12] *See infra* notes 13, 14. *See also* Letter from Wendy Kelley, former Secretary of Arkansas DOC, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 23, 2026) (describing the contraband problem and risk to staff, the public, and other inmates); Vortezon, Inc. Comments at 1 (Vortezon Comments) (describing the proliferation of contraband wireless devices as an "epidemic" and that use of such devices "has reached a crisis level"); National District Attorneys Association Comments at 1 (NDAA Comments) (noting recent illicit activities perpetrated by using contraband wireless devices, including a drug trafficking operation across the state of Georgia); Letter from Jeff Zmuda, Secretary, Kansas Department of Corrections, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111, at 1 (filed Oct. 26, 2026) (describing how contraband wireless devices directly contribute to violence and the introduction of other contraband in correctional facilities); Letter from Colby Braun, Director, North Dakota Department of Corrections and Rehabilitation, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026) (noting major drug trafficking operations enabled by contraband wireless devices); Letter from Nick Lamb, Secretary, South Dakota Department of Corrections, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026) (stating specific instances of contraband wireless device possession); Letter from Bobby Lumpkin, Executive Director, Texas Department of Criminal Justice, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026) (describing the role of contraband wireless device use in criminal activity and violence).

[13] Correctional Leaders Association Comments at 2 (CLA Comments). More recently, CLA reports on the multitude of examples across the country of contraband cell phones used for criminal activity and the urgent need for additional help to combat this problem. *See* Letter from Kevin Kempf, Executive Director, CLA, to Marlene H. Dortch, Secretary, FCC, GN Docket Nos. 13-111 and 26-74, Attach. at 1 (filed Oct. 21, 2026) (attaching CLA handout, "Support Contraband Cell Phone Interdiction Efforts to Safeguard America's Prisons"); *see also* Letter from Kevin Kempf, Executive Director, CLA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026) (providing summaries of several publicly reported cases involving contraband wireless device use). CLA urges the Commission to authorize jamming and details crimes facilitated by inmates using contraband cell phones in a South Carolina facility. *See* Letter from Kevin Kempf, Executive Director, CLA, to Marlene H. Dortch, Secretary, FCC, GN Docket Nos. 13-111 and 26-74, at 2 (filed Oct. 21, 2026) (CLA *Ex Parte* Letter).

[14] *See* Letter from Alan Wilson, South Carolina Attorney General, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 23, 2026) (reiterating support for allowing the authorization of jamming solutions in state correctional facilities and attaching previous letters calling for congressional action on the issue of contraband wireless device use); Letter from Shane Martin, South Carolina State Senator and Chairman, Senate Corrections and Penology Committee, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 23, 2026); Letter from John E. "JJ" Jones, Executive Director, South Carolina Police Chiefs Association, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026); Letter from D. Max Dorsey, II, Sheriff of Chester County, South Carolina, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026); Letter from Leon Lott, Sheriff of Richard County, South Carolina, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026); Letter from Mark A. Keel, Chief of the State Law Enforcement Division (SLED), to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026); Letter from Sally Foster, Executive Director, South Carolina Sheriffs' Association, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026); Letter from Michael L. Crenshaw, Sheriff, Oconee County, South Carolina, to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 23, 2026). *See also* Letter from Kevin Johns et al. to Marlene H. Dortch,

(continued….)

corrections community, and various solutions providers, argue that jamming can be an effective tool for certain correctional facilities when deployed with safeguards in place.[15] There is a clear recognition among many commenters that authorized jamming would provide an additional tool for the corrections community, but may not be appropriate in all correctional facility settings.[16] Commenters opposing the authorization of non-federal jamming solutions raise a range of legal and policy concerns regarding our proposed authorization framework, including the claim that jamming poses a risk to legitimate communications both inside and outside of prisons, and that other safer interdiction solutions are available.[17] In addition to the wireless industry, commenters expressing opposition to our proposals include groups representing public safety, unlicensed operations, and the public interest generally, among others.[18] Below, we address legal and policy arguments against correctional facility jamming raised in the record that are within the scope of this proceeding.[19]

5. More recently, CTIA engaged the Virginia Tech Applied Research Corporation (VT-ARC) to conduct a test of a micro-jamming system at the Broad River Correctional Institution in South Carolina.[20] VT-ARC coordinated with CTIA and its members, the South Carolina DOC, and the jamming vendor TalkTelio.[21] The test occurred in July 2026, and VT-ARC filed the results in this docket in

(Continued from previous page)
Secretary, FCC, GN Docket No. 13-111 (filed Oct. 22, 2026) (describing the dangers and consequences of inmate use of contraband cell phones).

[15] State DOCs supporting the authorization of jamming solutions for state and local agencies include South Carolina, Arkansas, Florida, Oklahoma, Texas, New York, West Virginia, and Kansas. *See, e.g.*, CLA Comments; NDAA Comments; CellAntenna International Inc (DBA Stealth RF) Comments (Stealth RF Comments); Detection Innovation Group Comments (DI Group Comments); Global Tel*Link Corporation d/b/a ViaPath Technologies Reply Comments (ViaPath Reply); Letter from Lindsay Wallace, Secretary, Arkansas DOC, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026); Letter from Bob McMahan, Executive Director, Arkansas Prosecuting Attorneys Association, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026); Letter from William J. Johnson, Executive Director, National Association of Police Organizations (NAPO), to Brendan Carr, Chairman, FCC, GN Docket No. 13-111 (filed Oct. 26, 2026).

[16] *See, e.g.*, StealthRF Comments at 3, 6-7 (noting that different tools are appropriate in different facilities depending on the location of the facility, i.e., rural or urban, and budget, among other factors); Las Vegas Metropolitan Police Department Clark County Detention Center Comments (noting that it will take technical expertise and increase costs if jammers are used in dense urban areas); GSMA Comments at 3 (noting that deployment of jamming solutions is highly site-dependent).

[17] *See generally, e.g.*, Verizon Comments; AT&T Services, Inc. Comments (AT&T Comments); CTIA Comments; Competitive Carriers Association Comments (CCA Comments).

[18] *See generally, e.g.*, Wi-Fi Alliance Comments; GPS Innovation Alliance Comments (GPSIA Comments); Alarm Industry Communications Committee Comments (AICC Comments); Worth Rises Reply; Multicultural Media, Telecom and Internet Council Reply (MMTC Reply); Public Knowledge Reply.

[19] We acknowledge comments from groups discussing institutional issues in correctional facilities related to the use of contraband phones. We find, however, that these arguments are outside the scope of this proceeding, which is focused on facilitating the legal use of jamming solutions by the corrections community to promote public safety by addressing the well-documented use of contraband wireless devices to facilitate criminal activity. *See, e.g.,* Worth Rises Reply (arguing that the demand for contraband phones is driven by systemic barriers to lawful communications); Andrew Jarecki, Charlotte Kaufman, and Beth Shelburne, Directors and Producers, *The Alabama Solution* Reply (arguing that contraband phones are important for incarcerated people to communicate and expose system failures).

[20] *See* Letter from Charles E. Cockrell, Jr., Director, Engineering Test and Evaluation Division, VT-ARC, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed Sept. 15, 2026). OET granted TalkTelio an experimental license to conduct the test. *See* ELS File No. 1221-EX-ST-2026 (granted July 13, 2026).

[21] *Id*.

September 2026 (VT-ARC Report).[22] VT-ARC states that the test was designed as a proof-of-concept assessment in a real-world environment, limited to a single vendor, a limited number of indoor and outdoor jamming devices, a portion of one building, operation on certain spectrum bands, and was intended to provide useful context for evaluating additional jamming deployments in other environments.[23] MITRE Corporation (MITRE) also participated in the test and produced a report, retained by the South Carolina DOC as independent advisor.[24] The participants filed responses in the docket regarding the test, as discussed below.[25]

6. In this *Third Report and Order (Third R&O)*, we deauthorize subscriber operation of contraband wireless devices in correctional facilities that are deemed contraband through a federal, state, or local statute, or a correctional facility rule, regulation, or policy that prohibits the possession or operation of contraband wireless devices. In the interest of creating a comprehensive regulatory framework that does not leave spectrum gaps for inmates to exploit, we apply our deauthorization approach to traditional commercial wireless bands, as well as spectrum licensed to the First Responder Network Authority (FirstNet),[26] specifically "Band 14," in this limited context. We adopt rules to enable the authorization of jamming solutions through non-exclusive overlay licensing, while retaining leasing as an available option where parties reach mutual agreement. We adopt testing requirements and technical parameters for jamming solutions, additional safety features for jamming devices, and marketing, labeling, and importation rules for jamming devices, to ensure that this solution is limited to targeted use in correctional facilities. We also adopt a rule amendment to increase flexibility for the authorization of CIS technologies. In the *Fourth Further Notice of Proposed Rulemaking (Fourth FNPRM)*, we seek comment on a proposed framework to deauthorize unlicensed part 15 operations in the correctional facility context and on mechanisms to authorize the deployment of jamming solutions on unlicensed spectrum. To further develop the record, we seek comment on application of jamming solutions to satellite communications. Finally, we seek comment on potential adjustments to wireless provider networks to provide additional safeguards for the implementation of jamming solutions, possible additional solutions provider compliance or monitoring obligations to protect authorized users, including public safety users, as well as an approach whereby the Commission would establish "quiet zones" in and around certain correctional facilities.

---

[22] Virginia Tech Applied Research Corporation (VT-ARC), Jamming Pilot Testing Analysis & Report – Broad River Correctional Institution (2026), https://www.fcc.gov/ecfs/document/26110076669/2 (VT-ARC Report).

[23] *See id*. at 5-6.

[24] *See* Letter from Joel Anderson, Director, South Carolina Department of Corrections, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 1 (filed Oct. 21, 2026) (SC DOC *Ex Parte* Letter); Cameron W. Patterson, The MITRE Corporation, Public Release Case No. 26-2240, Performance and Impact of a Contraband Wireless Device Jammer at Broad River Correctional Institution (2026), https://www.fcc.gov/ecfs/document/26110082733/1 (MITRE Report).

[25] *See* SC DOC *Ex Parte* Letter; MITRE Report; Letter from Michael Mullinix, Vice President, Regulatory Affairs, CTIA, *et al*., to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 2, 8 (filed Oct. 1, 2026) (CTIA Oct. 1 *Ex Parte* Letter); Letter from Abbie Forrest, President/CEO, TalkTelio, LLC (TalkTelio), to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111, at 5 (filed Oct. 14, 2026) (TalkTelio *Ex Parte* Letter).

[26] In 2012, Congress created FirstNet pursuant to the Spectrum Act, which called for the deployment of a National Public Safety Broadband Network (NPSBN). *See* Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, §§ 6001-6303, 6413, 126 Stat. 156, 201-22, 235-36 (codified at 47 U.S.C. §§ 1401-1433, 1457) (Spectrum Act). To that end, the Spectrum Act established FirstNet as an independent authority within the National Telecommunications and Information Administration (NTIA). 47 U.S.C. § 1424(a). In 2012, the Commission issued a license to FirstNet under call sign WQQE234 for the 758-769/788-799 MHz band (sometimes referred to as "Band 14"), which was renewed in May 2023. *See First Responder Network Authority, Nationwide Public Safety Broadband Network, Renewal of SP-700 MHz Public Safety Broadband Nationwide License Radio Service, Call Sign WQQE234, ULS File No. 0010176495*, Order, 38 FCC Rcd 4989 (PSHSB 2023) (*FirstNet Renewal Order*).

III. THIRD REPORT AND ORDER

7. In this *Third R&O*, we adopt rules to allow for the non-federal operation of RF jamming solutions in correctional facilities. As we take this historic step to improve public safety, we reassure stakeholders that eligible entities pursuing either of the two licensing paths discussed below will be subject to strict technical standards and testing requirements. This includes initial testing pursuant to an experimental license to prove that the jamming solution can be contained within designated geographic areas, as well as post-license grant testing at the subject correctional facility prior to the commencement of operations. We view the adopted technical rules and testing requirements as safeguards that render unnecessary the establishment of a formal pilot program or other type of phased implementation of this important public safety solution. We strongly emphasize, however, that although today's action expands the options available to the corrections community to combat contraband wireless devices in correctional facilities, we do not sanction jamming solutions that cause harmful interference to authorized users in violation of section 333 of the Act. Given this constraint, and the clear limits of our authorization framework, DOCs are cautioned that deployment of a jamming solution may not be technically feasible or cost-effective in every correctional facility environment. A jamming solution must be deployed in a way that causes harmful interference solely to deauthorized contraband wireless devices located in the intended contained area of the correctional facility, consistent with the scope of Commission approval to operate and the Act.

A. Definition of Jamming Solution, Jamming Device, and Jamming Containment Area

8. Given the legal and technical ramifications of today's action, we define at the outset relevant terms related to jamming in correctional facilities, specifically "jamming solution," "jamming device," and "jamming containment area." We adopt these definitions in a new part 90 subpart governing the overlay licensing of jamming solutions and providing technical requirements for all jamming solutions, however licensed.[27] In the *Third FNPRM*, the Commission proposed 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."[28] The Commission explained that, in contrast to currently deployed CISs (i.e., MAS and detection systems) that, where applicable, permit authorized wireless devices and emergency communications to connect to the wireless network, a jamming solution blocks all communications in the intended geographic location from connecting to the wireless network.[29] This functional difference is reflected in the Commission's proposed definition of "jamming solution," which focuses on preventing a network connection in the first instance, whereas a CIS typically either captures a call from a contraband device and drops it, or transmits an RF signal to acquire contraband phone identifying information from a contraband wireless device for later wireless provider disabling.[30]

9. In the *Third FNPRM*, the Commission sought comment on incorporating a definition of "jamming solution" as another type of CIS where appropriate to increase administrative efficiency and to achieve regulatory harmony across technologies.[31] Some commenters agree that a jamming solution

[27] *See* Appx. A, section 90.1401 (to be codified at 47 CFR § 90.1401). We incorporate cross-references to part 90 definitions relevant to jamming solutions in part 1, subpart X of the Commission's rules for jamming solutions authorized through lease arrangements. 47 CFR part 1, subpart X.

[28] *Third FNPRM*, 40 FCC Rcd at 8013, para. 20.

[29] *Id*. at para. 21.

[30] *See* 47 CFR § 1.9003 defining CIS 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."

[31] *See Third FNPRM*, 40 FCC Rcd at 8013, para. 22, at 8019, para. 36.

should be categorized as another type of CIS.[32] The South Carolina DOC suggests, however, that the proposed definition is too broad and believes that jamming solutions should be distinguished from other CISs.[33] Conversely, CTIA argues that the proposed definition is "overly broad" because it would encompass MAS.[34]

10. CISs currently are authorized solely pursuant to leasing, which affords "streamlined processing." Our approach to the authorization of jamming solutions is distinguishable from CIS in that it does not rely solely on leasing, but also allows for jamming solutions to be deployed through an overlay license. We adopt specific technical and application requirements for jamming solutions, whether licensed through overlay or leasing, that include testing at an initial, one-time proof-of-concept stage to demonstrate a given technology, application evaluation and, following application grant, separate on-site testing prior to operation. Accordingly, we do not find it appropriate to amend our existing CIS definition to include jamming solutions as a type of CIS. Rather, we adopt a definition of jamming solution that clearly distinguishes it from a CIS as a separate type of technological solution with distinct rules, where appropriate, to acknowledge stakeholder concerns of the risk of harmful interference to authorized wireless devices, particularly if a jamming solution is not carefully engineered and deployed.

11. We conclude that adopting a definition of "jamming device" in addition to "jamming solution" increases precision, more accurately describes the equipment regulated as a component(s) of an overall deployed jamming solution, and best captures the difference between an RF transmitter used in a jamming solution and one used in a CIS. We therefore adopt the following definition of "jamming device": "A transmitter within a correctional facility that prevents a contraband wireless device from establishing or maintaining a radio link by overwhelming the contraband wireless device with RF energy. A jamming device does not provide information to or communicate with a contraband wireless device." Having established this definition, we adopt the following definition of "jamming solution": "A system comprised of one or more jamming device(s) and associated elements used only at a correctional facility." We believe that these definitions combine to accurately capture the key differences in functionality between a jamming solution and types of CISs, rendering it unnecessary to further narrow the proposed definition of jamming solution in other ways suggested by some commenters.[35] We also find it appropriate to define "jamming containment area" as the "geographic area(s) of a correctional facility within which possession of a contraband wireless devices is a violation of federal, state, or local law, or a correctional facility rule, regulation, or policy; where a jamming solution is authorized; and outside of which the jamming solution must not cause harmful interference to authorized devices." We emphasize to all stakeholders that "harmful interference" is currently defined in our rules as "[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with [the ITU] Radio Regulations."[36]

12. In defining relevant terms, we make clear that our authorization of jamming solutions in correctional facilities applies to systems using transmitters that do not communicate with a contraband wireless device, and that prevent the device from establishing or maintaining a connection in the affected area by overwhelming the device with RF energy and blocking all communications. This contrasts with the functioning of CIS transmitters that can permit authorized wireless devices and emergency

[32] *See, e.g.*, Tecore, Inc. d/b/a Tecore Networks Comments (Tecore Comments) at 5.

[33] South Carolina DOC Comments at 2.

[34] CTIA Comments at 31.

[35] *See, e.g.*, South Carolina DOC Comments at 2 (proposing to add ". . . in a manner that does not involve using a cell site simulator"); J3 Technology LLC Comments (J3 Tech Comments) at 6 (recommending that the Commission add ". . . RF transmitter(s) that transmit non-CMRS signal(s) . . .").

[36] 47 CFR § 2.1.

communications ultimately to connect to the wireless network. To avoid any potential confusion, we also amend our current definition of CIS to specifically clarify that CIS does not include a "jamming solution."[37] These definitional changes set the foundation for a regulatory framework that enables the authorization of jamming solutions through both overlay licensing and leasing, but with licensing procedures and required safeguards that are distinct from CIS.[38]

B. Deauthorizing Contraband Wireless Devices in Correctional Facilities

13. After careful consideration of the record, we adopt the Commission's proposal to deauthorize subscriber operation of contraband wireless devices located within a correctional facility. As discussed below, we find that this approach is essential to allowing DOCs to employ jamming solutions consistent with section 333 of the Act. In this section, we rebut the legal and policy arguments of some commenters opposing jamming solutions and affirm our authority to deauthorize subscriber operation of contraband wireless devices and thereby authorize jamming solutions consistent with the Communications Act. We also decline to adopt our proposed safe harbor, finding it unnecessary.

1. Deauthorization Mechanism and Amendment to Section 1.903

14. The Commission's interpretation of section 333 of the Communications Act to date has stood as a barrier to non-federal use of jamming technology in correctional facilities in the United States. Section 333 prohibits any person from willfully or maliciously interfering with or causing interference to the radio communications of any station licensed or authorized by or under the Act or operated by the U.S. Government.[39] Because jamming devices are used to willfully interfere with licensed or authorized stations, the Commission currently prohibits non-federal entities (state, local, tribal, and territorial agencies) from deploying jamming devices to interfere with contraband wireless devices in correctional facilities.[40] Currently, contraband wireless devices in correctional facilities are authorized by the Commission under the wireless providers' licenses operating on commercial wireless networks, and, with respect to Band 14, operating under FirstNet's license, pursuant to section 1.903(c) of our rules.[41] By changing the licensing status of subscriber operations of contraband wireless devices in the limited context of correctional facilities to render such operations no longer licensed or authorized, we are able to authorize non-federal jamming consistent with section 333 and enhance public safety by further aiding DOC efforts to rid correctional facilities of a key means of perpetuating criminal activity.

---

[37] *See* Appx. A, section 90.1401 (to be codified at 47 CFR § 90.1401).

[38] Stakeholders interested in deploying CISs in correctional facilities for the purpose of disabling contraband wireless devices may continue to use our CIS certification and disabling process set forth in section 20.23 of the Commission's rules. *See* 47 CFR § 20.23. The Commission's website includes a list of all the accepted DCFOs and a chart that tracks the solutions providers that have approved CISs for use in the submission of qualifying requests for disabling and the specific correctional facilities where the CISs have been tested and approved. 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.

[39] *See* 47 U.S.C. § 333.

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

[41] 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."). FirstNet is authorized and governed under part 90 of the Commission's rules and is therefore deemed a WRS pursuant to Commission rule section 1.907. *See* 47 CFR § 1.907 (defining Wireless Radio Services as "[a]ll radio services authorized in parts 13, 20, 22, 24, 26, 27, 30, 74, 80, 87, 88, 90, 95, 96, 97, and 101 of this chapter, whether commercial or private in nature").

15. In the *Third FNPRM*, the Commission proposed to amend its rules to address the prohibition set forth in section 333 of the Act.[42] Specifically, the Commission proposed to amend section 1.903(c) so that subscriber operation of contraband devices in the Wireless Radio Services (WRS) would not be authorized.[43] As section 1.903 only applies to fixed and mobile stations in the WRS, the Commission sought comment on deauthorizing end-user subscriber operations on WRS spectrum bands (i.e., those traditionally used by wireless providers in commercial network deployments).[44] Commenters supporting jamming solutions agree that deauthorization is a viable way to permit non-federal jamming without violating section 333 of the Act and that the final rule should include, at a minimum, commercial wireless service bands.[45]

16. We adopt our proposal and amend section 1.903(c) of our rules to create an exception with regard to subscriber operation of a "contraband wireless device" as defined in section 1.9003.[46] Through this rule amendment, operation of any fixed or mobile station in the WRS considered a "contraband wireless device" will no longer be licensed or authorized by the Commission and, therefore, there is no section 333 statutory protection against willful or malicious interference by a jamming solution licensed by the Commission pursuant to our processes. We refer to this rule change as the "deauthorization approach" or the "deauthorization rule." Although we in large part limit our newly adopted regulatory framework to jamming solutions operating on traditional commercial wireless bands, we find it in the public interest to include Band 14, as AT&T end user customers can access that spectrum on a commercial basis through agreement with FirstNet, so as to remove an important spectrum loophole that could be exploited by inmates to circumvent jamming solutions.

17. To more comprehensively address potential spectrum loopholes, in the accompanying *Fourth FNPRM*, we propose and seek further comment on an approach to expand our adopted framework to unlicensed part 15 operations consistent with section 333 of the Act. We also seek additional comment on the scope of inmate use of contraband wireless devices communicating via satellite networks, and the appropriate means to authorize jamming operations on this separately licensed spectrum consistent with statutory constraints.

18. *Contraband Wireless Device*. As proposed, we apply our deauthorization rule expansively to operation of a contraband wireless device as defined in section 1.9003 of the Commission rules, i.e., any wireless device, including the physical hardware or part of a physical device, such as a subscriber identification module (SIM), that is within a correctional facility in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy, so that a jamming solution will be an available option and potential tool for correctional facilities where feasible.[47] This approach aligns with our CIS leasing framework.[48] We believe this broad, flexible approach to defining a contraband wireless device will best serve our goal of facilitating effective deployment of jamming solutions where desirable.

---

[42] *Third FNPRM*, 40 FCC Rcd at 8013-17, paras. 23-29; 47 U.S.C. § 333. As noted, section 301 requires Commission authorization to transmit RF energy. 47 U.S.C. § 301.

[43] *Third FNPRM*, 40 FCC Rcd at 8014-15, paras. 24-25.

[44] *Id*. at 8021, para. 39.

[45] *See* Vortezon Comments at 4; Tecore Comments at 14; Trace-Tek LLC Comments (Trace-Tek Comments) at 2-3; DI Group Comments at 6. We address commenters opposing our deauthorization proposal *infra*.

[46] 47 CFR § 1.903(c). Our rules define "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." *See* 47 CFR § 1.9003.

[47] *Third FNPRM*, 40 FCC Rcd at 8015, para. 26.

[48] *See* 47 CFR § 1.9003.

19. We received no comments suggesting that, for the purpose of applying our deauthorization rule, we should take a narrower view of the definition of "contraband wireless device" consistent with the Commission's approach to the disabling of contraband devices.[49] Some commenters agree that the proposed deauthorization rule should not be limited to states that criminalize the possession of contraband wireless devices in correctional facilities.[50] Dedrone assumes that our definition of "contraband wireless device" includes drones operated within a correctional facility in violation of law or policy, but may not include drone operations over a correctional facility, and seeks clarification on this point.[51]

20. We believe that the public safety goal of thwarting inmate criminal activity conducted using contraband wireless devices is best served by deauthorizing contraband wireless devices at correctional facilities where the use or possession of such devices violates federal, state, or local law, or a correctional facility rule, regulation, or policy, and we therefore adopt our proposed definition. With respect to drones, or unmanned aircraft systems (UAS), the *Third R&O* does not authorize jamming of devices operating on part 15 of the Commission rules, under which the majority of UAS control links operate.[52] Today's action also does not specifically address UAS in the correctional facility context, as Congress previously has acted in this particular area through the SAFER SKIES Act of 2025, which became law in December 2025.[53] The SAFER SKIES Act permits state, local, tribal, and territorial (SLTT) law enforcement and correctional agencies to conduct certain counter-UAS (C-UAS) operations pursuant to specific statutory criteria, and subject to federal training and certification requirements.[54] We also note that multiple Bureaus and Offices of the Commission issued an order on delegated authority on July 2, 2026, specifically granting special temporary authority to SLTT correctional agencies to conduct C-UAS operations that comply with the SAFER SKIES Act.[55] We therefore anticipate that a DOC will conduct any RF-based C-UAS activities in and around a correctional facility pursuant to the SAFER SKIES Act requirements, the SLTT C-UAS Spectrum Order, and the interim final rule required by the SAFER SKIES Act, which was jointly issued by the Department of Homeland Security (DHS) and the Department of Justice (DOJ) on July 1, 2026, as well as any future orders issued, or rules promulgated by, the Commission, DHS, and/or DOJ.[56]

---

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

[50] *See, e.g.*, J3 Tech Comments at 6; CLA Comments at 3; Vortezon Comments at 5.

[51] Dedrone Comments at 2 (seeking clarification that wireless devices entering low airspace (<400 ft) within the footprint of a correctional facility have functionally entered the facility and are therefore considered contraband wireless devices).

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

[53] SAFER SKIES Act of 2025, Pub. L. No. 119-213, § 2, 139 Stat. 1582 (2025) (SAFER SKIES Act) (codified as amended at 6 U.S.C. § 124n); *see also Unleashing American Drone Dominance*, Exec. Order 14307, 90 Fed. Reg. 24727 (June 6, 2025), https://www.whitehouse.gov/presidentialactions/2025/06/unleashing-american-drone-dominance/.

[54] *Id.*

[55] *See* Counter-UAS Spectrum Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies under the SAFER SKIES Act; Unleashing American Drone Dominance, GN Docket No. 26-74, Order, DA 26-656 (WTB/OET/PSHSB/SB/MB rel. July 2, 2026) (SLTT C-UAS Spectrum Order). CLA requests that the grant of special temporary authority be renewed prior to its expiration on December 29, 2026. *See* CLA *Ex Parte* Letter at 2.

[56] *See* U.S. Dept. of Homeland Security & U.S. Dept. of Justice, Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies, Interim Final Rule, Fed. Reg. Doc. No. 2026-13609 (continued….)

21. *Correctional Facility*. In the *Third FNPRM*, the Commission proposed that the deauthorization rule would apply broadly to contraband wireless devices located in "correctional facilities," currently defined in the CIS context 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."[57] The Commission sought comment on the appropriateness of applying to jamming solutions this definition of "correctional facility," which would include local facilities in close proximity to government facilities or residential areas, and thus present an increased risk of interference to authorized devices if a jamming solution is not properly deployed and maintained.[58] Specifically, the Commission asked whether it is necessary to restrict the application of the deauthorization rule to a specific type of correctional facility or to consider factors such as the security level of the facility.[59] The commenters addressing this issue contend that the Commission should use the proposed broad definition of "correctional facility," and that consideration of other factors is unnecessary.[60] For example, the South Carolina DOC argues that jamming deployments should not be restricted based on facility type, security level, location, or other characteristics that may differ across jurisdictions or locations.[61]

22. We seek regulatory consistency where possible and adopt our proposal to align the deauthorization approach in the jamming solutions context with the definition of "correctional facility" applied in current rule section 1.9003.[62] We agree with commenters that applying a definition of correctional facility that is restricted based on security level of the facility could lead to stakeholder confusion. We also find that limiting the definition of correctional facility in other ways, such as the average length of time of inmate incarceration, could prevent the availability of jamming solutions in a facility where such a solution is particularly needed. We remind stakeholders that all eligible solutions providers seeking to deploy a jamming solution in correctional facilities will be required to adhere to the strict testing requirements adopted herein to ensure that the solution is properly engineered, deployed, and maintained so as not to cause harmful interference to authorized communications.

23. In a similar vein, many commenters argue that the Commission should not limit the deauthorization approach to specific categories of correctional facility geographic locations.[63] For example, Trace-Tek states that strict and enforceable technical requirements will ensure that jamming solutions do not cause harmful interference, irrespective of geographic location.[64] Tecore believes that there is no need to restrict jamming to facilities in certain geographic areas, such as rural locations, because the safeguards put in place would guard against harmful interference.[65] We agree with these authorized CIS providers and note that, if a jamming solution is properly engineered, deployed, and maintained, the risk of harmful interference can be comparable to an RF-based MAS solution deployed at the same location. As stated, we find that imposing strict testing requirements on jamming solutions will

(Continued from previous page)
(July 1, 2026) (*DHS/DOJ Interim Final Rule*), *available at* https://www.federalregister.gov/public-inspection/2026-13609/counter-unmanned-aircraft-system-authority-for-state-local-tribal-and-territorial-law-enforcement.

[57] *Third FNPRM*, 40 FCC Rcd at 8016, para. 27; 47 CFR § 1.9003.

[58] *Third FNPRM*, 40 FCC Rcd at 8016, para. 28.

[59] *Id*.

[60] *See, e.g.*, J3 Tech Comments at 6; Vortezon Comments at 5-6; South Carolina DOC Comments at 3-4.

[61] *See* South Carolina DOC Comments at 3-4.

[62] 47 CFR § 1.9003.

[63] *See, e.g.*, South Carolina DOC Comments at 3-4; Vortezon Comments at 5-6.

[64] *See* Trace-Tek Comments at 5.

[65] *See* Tecore Comments at 11-13.

help ensure that harmful interference does not occur to authorized devices, regardless of the correctional facility locale.

2. Safe Harbor

24. In proposing the deauthorization rule, the Commission recognized that wireless providers might have concerns that they could be held liable for violations of section 301 of the Act for the unauthorized operation on their networks of contraband wireless devices in correctional facilities.[66] To address concerns about potential liability for deauthorized operations, the Commission proposed 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.[67] The Commission explained that wireless providers might be liable for continuing to authenticate and provide service to such devices following deauthorization.[68] The Commission detailed potential circumstances under which it would not take enforcement action against a wireless provider, and when the proposed safe harbor would not be available.[69] Importantly, the Commission explained that the safe harbor was intended to incentivize wireless providers to participate in good faith negotiations under the proposed leasing approach to authorizing jamming solutions.[70]

25. Some commenters contend that the proposal is unclear and overly complex with respect to the sufficiency of the proposed safe harbor in providing liability protection from potential section 301 violations. CTIA contends that the safe harbor is problematic, in that it is tied to undefined "good faith negotiations," which it argues is too vague and fails to provide guidance such that providers would be able to reliably qualify for it.[71] Proponents of jamming and our deauthorization approach also point out the difficulty of determining what "unreasonable risk of interference" and "technical infeasibility" mean in the context of the Commission's determination of whether a wireless provider potentially qualifies for the safe harbor in the absence of a good faith lease arrangement.[72]

26. Moreover, opponents of the Commission's deauthorization approach argue that the proposed safe harbor's protection against potential liability for violations of section 301 is insufficient because it does not protect the wireless providers against other sources of liability. AT&T suggests that, in addition to section 301, the wireless providers would not be protected from Commission enforcement under section 333, tort liability, or other liability resulting from the incidental blocking of authorized communications.[73] Therefore, AT&T states that the Commission must immunize the wireless providers

---

[66] *Third FNPRM*, 40 FCC Rcd at 8017-18, para. 31.

[67] *Id*. at paras. 31-34.

[68] *Id*. at para. 31.

[69] *Id.* at 8018, paras. 32-33. The *Third FNPRM* proposed that the safe harbor would apply to: (1) 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; and (2) 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. *Id*. at para. 32. A wireless provider would not qualify for the safe harbor where a party actively seeks authority as lessee for a jamming solution to combat contraband wireless devices and negotiates in good faith, but the wireless provider fails to negotiate in good faith. And, 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. *Id*. at para. 33.

[70] *Id*. at para. 31.

[71] CTIA Comments at 25.

[72] CLA Comments at 4.

[73] AT&T Comments at 14-15.

from all provisions of the Act, its rules, and other federal and state laws that could be attributable to jammer-related violations.[74] In the same vein, CTIA asks the Commission to act affirmatively to protect wireless providers from liability when a jamming solution blocks legitimate calls, including preempting state liability.[75]

27. After considering the record, we find it unnecessary to adopt the proposed safe harbor rule as an incentive to engage in leasing. Our action today provides for the direct path of overlay licensing to authorize non-federal jamming solutions in correctional facilities, and we decline to mandate good faith negotiations in lease arrangements as initially contemplated in the *Third FNPRM*, though we authorize leasing for jamming solutions as a purely voluntary option for stakeholders. We thereby reduce regulatory complexity and avoid adoption of a standard that commenters find vague.[76] As explained below, the record in this proceeding reflects wireless provider opposition to the concept of authorizing jamming solutions in correctional facilities,[77] and therefore we anticipate that voluntary leasing arrangements will present a substantial minority of applications filed in this context.

28. Our adopted regulatory framework is designed to promote efficiency and accuracy in the deployment of jamming solutions that must be engineered to not cause harmful interference to authorized, non-contraband wireless devices. Although we acknowledge wireless providers' concerns about liability not only for violations of section 301 of the Act, but for other potential violations, we require jamming solutions to be contained to areas of correctional facilities where the operation of wireless devices is prohibited. We find that our required safeguards—more stringent than those applicable in the CIS disabling context—will work to prevent harmful interference to authorized communications.[78] Moreover, as discussed below, we adopt a "stop-buzzer" type requirement that a jamming solutions operator immediately cease operation to address credible complaints of harmful interference.[79]

3. Commission Authority to Deauthorize Contraband Wireless Devices and to Authorize Jamming Solutions Under Section 301

29. In the *Third FNPRM*, the Commission tentatively concluded that it has the authority to deauthorize contraband wireless devices pursuant to section 303 of the Act, which provides the Commission with expansive powers and duties to make rules governing wireless operations required by the public convenience, interest, or necessity.[80] In particular, relevant 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]."[81]

---

[74] *Id*. at 15.

[75] CTIA Comments at 29-30 (suggesting that the Commission should preempt state liability, including tort liability, for wireless providers when the jamming system blocks calls from non-contraband devices).

[76] *Third FNPRM*, 40 FCC Rcd at 8017-18, paras. 31, 34.

[77] *See infra* paras. 31-62.

[78] In the context of CIS disabling, the Commission preempted state tort liability for wireless provider disabling actions. *See Second R&O*, 36 FCC Rcd at 118019, para. 15. In contrast to the CIS disabling context, we adopt for the authorization of jamming solutions core technical rules, equipment authorization rules that require particular interference protection features, and specialized testing requirements, including POC testing and pre-operational testing, applicable to both overlay licensing and leasing.

[79] *See infra* paras. 186-191.

[80] *Third FNPRM*, 40 FCC at 8015, para. 25; 47 U.S.C. § 303.

[81] 47 U.S.C. § 303(b), (d), (h), (l)(1), (r).

30. We believe that section 333's plain language unambiguously prohibits willful or malicious interference to a specific class of stations, i.e., stations authorized or licensed by the Commission, and thus stations deemed deauthorized under the Act are not entitled to interference protection. We affirm our authority to authorize jamming solutions both under sections 301 and 303 of the Act,[82] either through non-exclusive overlay licensing or leasing.[83] Our rules require a license to operate a station in the WRS[84] and, in the correctional facility context, an effective jamming solution will deploy base stations transmitting on frequencies licensed to WRS licensees to provide commercial service. Therefore, the deployment of a jamming solution will require Commission authorization to transmit on wireless providers' licensed spectrum.[85] Through today's action, operators of jamming solutions can be licensed under section 301 of the Act through overlay licensing or leasing,[86] to address specifically the operations of contraband wireless devices that are no longer authorized under the wireless provider's license.[87] Below, we address commenters' challenges under the Communications Act and the Administrative Procedure Act (APA), both to our authority to deauthorize contraband wireless devices and to authorize jamming solutions.

a. Arguments that Permitting Jamming Violates the Communications Act

31. Section 333 of the Act provides that "[n]o person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government."[88] CTIA and other commenters argue that section 333 of the Act expressly and independently prevents the authorization of non-federal jamming, and thus, the adoption of rules authorizing jamming solutions is unlawful.[89] These commenters contend that jamming solutions will result in willful interference in violation of section 333, arguing that RF jamming signals cannot be cabined merely to block newly deauthorized communications, and will also block authorized communications located within and outside of a correctional facility. CTIA contends that deauthorizing contraband wireless devices will not solve the Commission's statutory problem, as jamming solutions will violate section 333 of the Act by impacting authorized devices.[90] In support, CTIA and AT&T focus in particular on the Commission's statements that jamming devices cannot distinguish between authorized and deauthorized devices.[91] CTIA also argues that section 333 prohibits the jamming of any station, even one's own signal.[92]

[82] *Id*. §§ 301, 303(b), (d), (h), (l)(1), (r).

[83] *Third FNPRM*, 40 FCC Rcd at 8019, para. 36; *id.* at 8036, para. 74.

[84] 47 CFR §§ 1.903, 1.9001 (authorization through lease arrangement with a licensee).

[85] 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).

[86] *See infra* paras. 76-153.

[87] As explained, this licensing approach also complies with section 333 of the Act. 47 U.S.C. § 333.

[88] *Id*.

[89] *See, e.g.*, CTIA Comments at 21-23; Public Knowledge Reply at 7; Letter from Joe Kane, Director of Broadband and Spectrum Policy, Information Technology and Innovation Foundation, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 11-113, at 2 (Jan. 29, 2026) (ITIF *Ex Parte* Letter).

[90] CTIA Comments at 10-15; 21-23.

[91] *Id*. at 10-11 (referencing Commission statements acknowledging that jamming solutions block all communications on affected frequencies); AT&T Comments at 12 (noting the Commission's past statement that jammers cannot differentiate between contraband devices and legitimate devices).

[92] *See* CTIA Comments at 22, citing *Johnson v. Am. Towers, LLC*, 781 F.3d 693, 708 (4th Cir. 2015).

32. The Commission acknowledged in the *Third FNPRM* that jamming devices cannot distinguish between authorized and deauthorized devices.[93] We clarify, however, that the referenced technical limitation applies to devices located *within a chosen targeted area*. Under our adopted framework, authorized jamming is limited to a specific containment area(s) within a correctional facility, which by definition can only include contraband wireless devices that are not permitted in the area(s) pursuant to federal, state, or local law, or a correctional facility rule, regulation, or policy and, therefore, are deauthorized.[94] To be clear, all devices located within the jamming containment area are deauthorized under our rules and the Act, and therefore are subject to being jammed.

33. We observe that the wireless industry's argument that jamming of authorized devices is inevitable due to the inherent nature of jamming technology relates solely to technical and policy determinations, and presents no legal challenge to our approach that results in a lack of section 333 protection against willful or malicious interference afforded to *deauthorized* contraband wireless devices. We find that a legal argument tied to an assumed impact to *authorized* devices clearly fails to appreciate the limited scope of the operations we authorize today. We do not sanction jamming solutions to cause willful or malicious interference to authorized wireless devices and agree that, under our regulatory framework, such devices located outside of the jamming containment area, whether within the correctional facility premises if permitted (e.g., medical personnel, vendors, attorneys), or outside of the perimeter, remain protected under section 333 of the Act.

34. With respect to CTIA's argument that the 4th Circuit's decision in *Johnson* bars any jamming, even self-jamming, we find that the court's ruling was in the context of a preemption analysis and addressed whether wireless providers could be required under state tort common law to implement jamming technology to address contraband phone use.[95] The court analyzed the language of section 333 in response to the contention that the statute barred interference with any radio communications, including his or her own.[96] The court agreed that section 333 prohibited self-interference with licensed communications, but had no reason to address the effect of section 333 regarding interference with communications that the Commission has affirmatively deauthorized.[97] Given this omission and our approach that deauthorizes contraband wireless devices, we find that the *Johnson* case does not bar the authorization of jamming solutions, including self-jamming, to address the issue of contraband wireless device use.

35. A review of section 333's legislative history also suggests that the statute does not bar Commission action to authorize jamming solutions, but rather provides a source of explicit authority to halt willful or malicious interference. In 1990, Congress granted this additional authority, as requested by the Commission, to more quickly and effectively address the issue of parties jamming authorized services. The Senate Report explains that, at the time, the Commission was using "the more limited prohibition" in section 303(m)(1)(E)—which gives the Commission discretionary authority to suspend a license—to attempt to halt jamming, and that with the enactment of section 333, Congress granted the Commission "explicit authority" to halt interference with more severe penalties.[98] In its filing in the record, Marcus Spectrum Solutions discusses the reason that the Commission requested additional authority from

[93] *See, e.g.*, *Third FNPRM*, 40 FCC Rcd at 8013, para. 21, at 8040, para. 87.

[94] *See supra* paras. 11 (defining jamming containment area), 18-20 (defining contraband wireless device).

[95] *See generally Johnson v. Am. Towers, LLC*, 781 F.3d 693 (4th Cir. 2015).

[96] *Id*. at 707-709.

[97] *Id*. at 708.

[98] S. Rep. 101-215 at 7 (1989), accompanying S. 1022 (Senate Report). The House Report also explained that without a statutory prohibition, the Commission had to rely on more limited penalties in the Act, but that section 333 made willful and malicious interference a criminal offense. H.R. Rep. No. 101-316 at 8 (1989), accompanying H.R. 3265 (House Report).

Congress, referencing Global Tel*Link Corporation's (GTL) 2011 petition for rulemaking, in which it addressed the legislative intent of section 333.[99] GTL argued that Congress intended to confer upon the Commission the discretion to exercise authority, not prohibit the Commission from exercising discretion, after the Commission requested legislation in response to a series of intentional jamming incidents in which a jammer used a *licensed* transmitter and thus could not be prosecuted for criminal violation of section 501 of the Act.[100] With the enactment of section 333, the Commission received explicit authority to halt jamming and apply more severe consequences under section 501.[101] We find that the legislative history of section 333 supports congressional intent to strengthen Commission enforcement efforts—not to bar Commission action regarding harmful interference in all instances.

36. Some commenters contend that the text, structure, and purpose of the Communications Act make clear and unambiguous that it does not authorize the Commission to permit jamming.[102] These commenters argue that Congress has not specifically granted the Commission authority to authorize jamming and, through various statutory provisions, has directed the Commission to prevent interference.[103] Specifically, CTIA and AT&T contend that because section 303(f) of the Act provides that the Commission "shall" take action "as it may deem necessary to *prevent* interference between stations," the Commission is barred from acting to *permit* interference absent an express statutory directive, and therefore cannot authorize jamming.[104] CTIA also argues that section 302a, addressing equipment authorization and permitting regulations governing the interference potential of devices the emit radio energy, further supports its claim that the Commission must act to reduce interference and must authorize devices accordingly.[105] CTIA interprets other subsections of 303 as being directed towards, and limited to, *mitigating* interference.[106]

37. We reject commenters' overly narrow view of section 303(f) as it relates to section 333, including the argument that the Act as a whole directs the Commission to prevent or mitigate interference in *all* circumstances, effectively barring the Commission from permitting interference in any RF context. We find that the Communications Act affords the Commission flexibility to pursue public safety goals that further the public interest and, accordingly, that we have the authority to authorize jamming solutions, particularly in the narrowly tailored context of correctional facility use. In interference-related matters, the Commission has been afforded substantial deference in determining whether the risk of harmful interference in a particular situation is significant, and what safeguards to apply to reduce that potential.[107] This includes the appropriateness of Commission-mandated mechanisms to remediate cases

[99] *See* Letter from Michael J. Marcus, Marcus Spectrum Solutions LLC, to Marlene H. Dortch, Secretary, FCC at 6-7 (MSS *Ex Parte* Letter), referencing Petition for Rulemaking of Global Tel*Link Corporation, Amendment of Sections 22.3(b), 1.931 and Subpart X of the Commission's Rules and Create of New Rule(s) to Authorize a Plurality of Technical Solutions to Eradicate the Unauthorized Use of Wireless Devices in Correctional Facilities, at 15 (filed July 20, 2011) (GTL Petition).

[100] GTL Petition at 15, citing the House Report and the Senate Report.

[101] *Id.*

[102] *See, e.g.*, CTIA Comments at 17-21; Verizon Comments at 5-8; ITIF *Ex Parte* Letter at 1-2.

[103] *Id*.

[104] 47 U.S.C. § 303(f) (emphasis added); CTIA Comments at 17-18; AT&T Comments at 10.

[105] CTIA Comments at 18-19. *See also* Verizon Comments at 5-6.

[106] CTIA Comments at 18-19.

[107] *See AT&T Servs., Inc. v. FCC*, 21 F.4th 841, 846 (D.C. Cir. 2021) (finding that the Commission acted reasonably in permitting unlicensed device use in the 6 GHz band following its determination that the potential for harmful interference to incumbent operations was insignificant.). The court found reasonable the Commission's adoption of industry requested safeguards intended to ensure detection and resolution of harmful interference, as well as the

(continued….)

of harmful interference. As discussed below, today we reasonably adopt strict technical parameters for jamming solutions, a network monitoring requirement, a locking mechanism requirement, and interference resolution procedures requiring the cessation of jamming operations if harmful interference occurs.[108]

38. It is well settled that Congress granted the Commission the authority to regulate radio frequencies to promote public safety, specifically establishing the Commission for the purpose of, *inter alia*, "promoting safety of life and property through the use of wire and radio communications."[109] Section 151 of the Act unquestionably makes public safety a central Commission objective.[110] With regard to our duty to promote public safety, Public Knowledge claims that the Commission's authorization of jamming contradicts Congress' command to obtain "maximum effectiveness" from the use of communications in connection with safety of life and property.[111] We find implausible the notion that Congress effectively compelled the Commission to maximize inmates' use of contraband wireless devices to perpetrate criminal activity in designated areas of correctional facilities; rather, we find it in the public interest to authorize jamming solutions to facilitate the elimination of contraband wireless device use, thereby maximizing the use of licensed spectrum to promote safety of life consistent with congressional intent. We find that fulfilling our statutory obligation to promote public safety through the use of RF is paramount and, therefore, the absence of statutory language expressly granting the Commission authority to "permit jamming" does not bar today's action.[112] In fact, throughout this *Third R&O*, we discuss at length our public safety rationale for not perpetuating the stasis of prior Commissions regarding jamming solutions, in favor of proactively providing an additional tool for DOCs to combat the daily scourge of contraband wireless device use by inmates in correctional facilities.

39. Today's decision builds on actions the Commission has previously taken. In the same correctional facility context, the Commission has authorized the use of CISs (MAS and detection systems), which are deployed, as the wireless providers' preferred solution, to address contraband wireless device use. MAS solutions, in particular, emit RF transmissions to mimic commercial wireless base stations and capture calls made from within the correctional facility. This solution ultimately results in call degradation or obstruction to the extent that a contraband device call is interrupted and dropped without being connected to the wireless provider network, thereby harmfully interfering with the subscriber's intended communication.[113] While balancing policy objectives, the Commission adopted streamlined leasing procedures over a decade ago to authorize CIS systems, including MAS, to achieve an important public safety purpose of preventing communications from contraband wireless devices within correctional facilities.[114] As reflected in the Commission's Universal Licensing System (ULS), the Wireless Telecommunications Bureau (WTB) to date has approved over 2,200 lease arrangements for CIS

(Continued from previous page)
Commission's explanation that its Enforcement Bureau could investigate and take appropriate action to resolve such cases. *Id*. at 846, 852.

[108] *See infra* paras. 154-191.

[109] 47 U.S.C. § 151.

[110] *Id*.

[111] Public Knowledge Reply at 5, n.5, citing 47 U.S.C. § 104(n) [*sic*]. Section 154(n) states: "For the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems." 47 U.S.C. § 154(n).

[112] 47 U.S.C. § 151.

[113] *See First R&O*, 32 FCC Rcd at 2339, para. 6; *see also* 47 CFR § 2.1.

[114] *See First R&O,* 32 FCC Rcd at 2345-51, paras. 21-35 (streamlining the leasing process by permitting overnight processing for qualifying lease applications), at 2351-52, paras. 36-39 (enabling CIS operators to be presumptively treated as PMRS).

solutions in 31 states. Commission approval of MAS demonstrates its ability to authorize RF transmissions for a public safety purpose through sections 301 and 303, the latter of which provides the Commission with broad authority to regulate the use of RF spectrum in the public interest. We find that this authority includes the ability to deauthorize subscribers and to authorize licensed RF transmissions that advance public safety in response to the threat of unlawful contraband device use.[115]

40. We interpret our section 303 authority in the context of Congress's adoption of section 333 and therefore interpret the statutory mandate as requiring the Commission to consider whether to adopt regulations, in the public interest, convenience, and necessity, that prevent interference between *authorized* stations. Today, we carry out our section 303 responsibilities by specifying the nature of services to be rendered in the WRS bands where jamming solutions may be authorized in correctional facilities, as well as the characteristics of authorized solutions, including the location of stations and other technical parameters and device requirements. We also act under our authority to prescribe qualifications of station operators and duties to be performed, specifying that approved jamming devices may be operated only by authorized DOCs or their contracted solutions providers in correctional facilities after having obtained appropriate licenses. In acting pursuant to section 303, we are not bound to prevent interference to deauthorized stations, and therefore we do not violate section 333 by permitting jamming, as an alternative to CIS, to interrupt deauthorized communications from contraband wireless devices in designated areas of correctional facilities. Importantly, Commission authorization of CIS, the acknowledged wireless provider preferred solution, is arguably not based on express statutory language that permits "willful interference" caused by such solutions, most typically in the form of dropped calls from contraband wireless devices. Clearly, the Commission has found that public safety considerations can outweigh interference concerns, stating in one instance relating to broadcast services "that while protection of the interference-free contours is an important function of the Commission's regulatory responsibility, it is not absolute when that protection conflicts with the need for safety."[116] The vital objective of protecting and promoting public safety forms a central basis for our action authorizing the use of jamming solutions in correctional facilities.

41. Further, rather than acting to bar harmful interference in every instance, the Commission has adopted rules in a range of contexts that acknowledge the existence of harmful interference between spectrum users. For example, sections 2.104 and 2.105 address spectrum allocation issues and establish the relationship between primary and secondary services.[117] These rules provide that stations of a secondary service "[c]annot claim protection from harmful interference from stations of a primary service to which frequencies are already assigned or may be assigned at a later date."[118] In situations where primary and secondary licensed services coexist, the Commission clearly permits stations operating under a primary allocation to cause harmful interference to devices operating under a secondary allocation. In the WRS, for example, our rules governing Medical Body Area Network (MBAN) devices,[119] and

[115] 47 U.S.C. § 303.

[116] *Request of WDNT/WNFM(FM), Dayton, Tennessee Reconsideration of the Staff's Ruling of July 13, 1980*, 87 F.C.C.2d 984, 986-87 (1981) (affirming decision to allow AM station to broadcast emergency information using full daytime power during nighttime hours, thus permitting interference with other radio broadcast operations).

[117] *See* 47 CFR §§ 2.104(d)(3)(iii), 2.105(c)(2)(ii).

[118] *Id*.

[119] *See* 47 CFR § 95.2525(b). *See also Amendment of the Commission's Rules to Provide Spectrum for the Operation of Medical Body Area Networks*, ET Docket No. 08-59, First Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6422, 6441, para. 38 (2012) ("Operators of MBAN systems and health care facilities are reminded that even the 'life-critical' operation permitted on a secondary basis must accept interference from the primary spectrum users in the 2360-2400 MHz band.").

Supplemental Coverage from Space (SCS),[120] provide that such devices must accept any interference from licensed and authorized stations operating under a primary allocation. The Commission also has adopted rules in other radio services emphasizing the secondary nature of a particular service, for example, the Low Power Television (LPTV) service licensed under part 74, and for wireless microphones also licensed under part 74, specifying that such services and devices must accept interference from operations with primary status.[121] As another example, the Commission's part 15 rules authorizing unlicensed device operation also permit interference, as operations are subject to the condition that ". . . no harmful interference is caused and that interference must be accepted that may be caused by the operation of an authorized radio station . . . ."[122]

42. *Section 303(m)*. Public Knowledge asserts that section 303(m)(1)(E) of the Act is essentially a barrier to the Commission authorizing jamming.[123] Section 303(m)(1)(E) states that the Commission has the authority in the public interest to suspend the license of any operator upon proof that the licensee has willfully or maliciously interfered with any other radio communications or signals.[124] Public Knowledge contends that this statutory provision, adopted in 1934, prohibits interference without reference to a station being licensed or authorized, and therefore prohibits Commission action authorizing jamming.[125] Public Knowledge concedes, however, that section 303(m)(1)(E) "simply makes malicious or willful interference a reason to suspend a license"[126] but nevertheless asserts that it is "axiomatic" that behavior that provides grounds for suspending a license, i.e. malicious or willful interference, is prohibited.[127]

---

[120] *See* 47 CFR § 2.106(d)(33)(i). *See also Single Network Future: Supplemental Coverage from Space, Space Innovation*, GN Docket No. 23-65, IB Docket 22-271, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 2622, 2623, 2635, 2642, paras. 4, 31, 47 (2024).

[121] *See, e.g.*, *Implementation of the Low Power Protection Act*, MB Docket No. 23-126, Report and Order, 38 FCC Rcd 12627, 12628, para. 2 & n.5 (2023) ("As a result of their secondary status, LPTV stations can also be displaced by full power stations that seek to expand their service area, or by new full power stations seeking to enter the same area as an LPTV station."); *Promoting Spectrum Access for Wireless Microphone Operations*, *Expanding the Economic and Innovation Opportunities of Spectrum through Incentive Auctions*, GN Docket Nos. 14-166, 12-268, Report and Order, 30 FCC Rcd 8739, 8784-85, paras. 116-118 (2015).

[122] *See* 47 CFR § 15.5(b); *Revision of Part 15 of the Rules regarding the Operation of Radio Frequency Devices without an Individual License*, GEN. Docket No. 87-389, First Report and Order, 4 FCC Rcd 3493, 3515, para. 123 (1989) (*Revision of Part 15 Rules Report and Order*). In adopting the part 15 rules, the Commission acted in the public interest to promote innovation and enable a variety of applications by permitting the operation of low-power devices, while purposely fostering a spectral environment in which a class of devices would be required to accept interference. *See Revision of Part 15 Rules Report and Order*, 4 FCC Rcd 3493, 3494-95, paras. 8, 13, 15; *see also Revision of Part 15 of the Rules regarding the Operation of Radio Frequency Devices without an Individual License*, GEN. Docket No. 87-389, First Report and Order, 4 FCC Rcd 3493 (1989) (*Revision of Part 15 Rules Report and Order*). The history of the part 15 rules indicate that unlicensed devices were authorized, in part, to serve growing communications needs and that section 302 of the Act provides the Commission with the basis to allow unlicensed devices to share spectrum with licensed services. *See Amendment of Part 15 of the Commission's Rules to Allow Certification of Equipment in the 24.05-24.25 GHz Band at Field Strengths up to 2500 mV/m*, ET Docket No. 98-156, Memorandum Opinion and Order, 18 FCC Rcd 15944, 15946, 15948-49, paras. 5, 13-14 (2003).

[123] Public Knowledge Reply at 6-9. *See also* Verizon Comments at 5; ITIF *Ex Parte* Letter at 2.

[124] *See* 47 U.S.C. § 303(m)(1)(E).

[125] Public Knowledge Reply at 6-9.

[126] *Id*. at 6, n.8.

[127] *Id*.

43. We disagree with Public Knowledge's approach to statutory construction. The argument that section 303(m)(1)(E) bars authorization of jamming solutions, even when applied to deauthorized stations, assumes that this provision implicitly overrides section 333's express language, adopted many decades later, that limits the prohibition against willful or malicious interference to *licensed or authorized* stations. We believe that the more recently adopted section 333 expresses Congress' clear intent to apply the prohibition against willful or malicious interference *only* to licensed or authorized stations. Section 303(m)(1)(E) merely grants the Commission discretionary authority to suspend a license whereas, in contrast, a violation of section 333 implicates section 501 of the Act.[128]

44. Here, we abide by the established rule of statutory construction that clear and unambiguous statutory language ends the analysis with regard to congressional intent.[129] As courts have made clear, "[w]here the language Congress chose to express its intent is clear and unambiguous, that is as far as we go to ascertain its intent because we must presume that Congress said what it meant and meant what it said."[130] Accordingly, as evident from the plain language of the statutes relevant to this proceeding, section 303(m)(1)(E) simply makes willful or malicious interference a reason for the Commission, in its discretion, to suspend a license.

45. *Section 303(r)*. Section 303(r) of the Act grants the Commission authority to "[m]ake such rules and regulations . . . not inconsistent with law, as may be necessary to carry out the provisions of [the Act]."[131] CTIA contends that, to rely on ancillary authority under section 303(r) of the Act to authorize jamming, the Commission would have to confront the limit that such authority may be exercised only where it is "reasonably ancillary to the . . . effective performance of its statutorily mandated responsibilities," citing to *Comcast Corp. v. FCC*.[132] CTIA argues that, because the Commission has no mandate to authorize jamming and in fact has a mandate to prevent jamming, the Commission cannot rely on ancillary authority.[133]

46. We disagree. The Commission has independent authority to take action in the interest of public safety and national security under the Communications Act.[134] Our actions today stem not only from ancillary authority provided in sections 4(i) and 303(r) of the Act, but also from our statutory obligation to promote the safety of life. The public interest standard permits consideration of public

[128] *See* 47 U.S.C. §§ 501, 333. We also disagree with Public Knowledge's contention that it is "axiomatic" that behavior that provides grounds for a penalty per se means the behavior is prohibited. *See supra* n.52. The existence of a penalty can act to discourage a behavior, without necessarily prohibiting it, for example, where a party pays liquidated damages for breach of contract. Moreover, the behavioral context matters, as conduct that is objectionable in one circumstance may not be in another. Thus, the fact that the Commission has discretion under section 303(m)(1)(E) to impose a penalty where warranted does not illustrate that interference is axiomatically prohibited in all circumstances.

[129] *See, e.g.*, *Food Mktg. Inst. v. Argus Leader Media*, 588 U.S. 427, 436 (2019); *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992); *United States v. Steele*, 147 F.3d 1316, 1318 (11th Cir. 1998).

[130] *United States v. Steele*, 147 F.3d 1316, 1318 (11th Cir. 1998). *See also Food Mktg. Inst. v. Argus Leader Media*, 588 U.S. 427, 436 (2019); *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992).

[131] 47 U.S.C. § 303(r). The legislative history of § 303(r) indicates that this ancillary authority was established in part to promote safety of life and property at sea through the use of wire and radio communication. *See* Act of May 20, 1937, ch. 229, 50 Stat. 189, 191.

[132] CTIA Comments at 21, n.69, citing *Comcast Corp. v. FCC*, 600 F.3d 642, 644 (D.C. Cir. 2010) (confirming that the Commission may exercise ancillary authority in section 4(i) of the Act, 47 U.S.C. § 154(i), only when paired with other statutorily mandated responsibilities).

[133] CTIA Comments at 21.

[134] *See Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232, Third Report and Order and Third Further Notice of Proposed Rulemaking, FCC 26-50, at 9, para. 19 (July 23, 2026) (*Supply Chain Third R&O*).

safety and national security risks, and the Commission has repeatedly, and very recently, relied on its authority granted in the Communications Act to establish rules to address such risks.[135] Our approach represents a natural extension of our current public safety rules, and we adopt rules to allow for the non-federal operation of RF jamming solutions in correctional facilities to serve "the purpose of promoting safety of life and property."[136] Congress authorized the Commission to promulgate rules to carry out statutory provisions and strike a balance among overlapping or conflicting policies, which include the promotion of safety of life and property.[137] Here, we balance the competing policies of promoting public safety by combatting contraband wireless device use in correctional facilities, while preventing harmful interference with licensed or authorized communications. We find that, based on the extensive record, communications originating from contraband wireless devices in correctional facilities are a threat to the safety of prison officials and employees, other inmates, and the general public.[138] Although some stakeholders express concern that the authorization of jamming will lead to interference with authorized communications, we have carefully balanced our statutory responsibilities and determine that the public interest is best served through adoption of a narrowly tailored regulatory regime that authorizes jamming of deauthorized devices, limited to a contained geographic area within a correctional facility, to thwart the orchestration of criminal activity.

47. *Section 303(y)*. Section 303(y) of the Act grants the Commission authority to "allocate electromagnetic spectrum so as to provide flexibility of use" if certain conditions are met.[139] CTIA argues

[135] 47 U.S.C. § 302a(a). *See, e.g.*, *Supply Chain Third R&O* at 9, para. 19 (adopting rules that prohibit the authorization of devices that include logic-bearing hardware components produced by Covered List entities, finding that such action promotes the national defense and safety of life and property); *Facilitating Implementation of Next Generation 911 (NG911), Improving 911 Reliability*, PS Docket Nos. 21-479, 13-75, Second Report and Order and Second Further Notice of Proposed Rulemaking, FCC 26-39, at 62, para. 158 (June 26, 2026) (indicating that the Commission's authority to act in the interest of public safety is "among its most important responsibilities").

[136] 47 U.S.C. § 151.

[137] *Cohen v. Apple Inc.*, 46 F.4th 1012, 1017 (9th Cir. 2022) ("The Act, as amended, authorized the FCC 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 [statutory] provisions." 47 U.S.C. § 303(r); *see also id.* § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."); *Farina v. Nokia, Inc.*, 625 F.3d 97, 123 (3d Cir. 2010) ("When Congress charges an agency with balancing competing objectives, it intends the agency to use its reasoned judgment to weigh the relevant considerations and determine how best to prioritize between these objectives.").

[138] Commenters cited the public safety risks of contraband wireless devices and indicated that targeted jamming solutions would provide another useful tool to combat the widespread use of such devices. *See* Arkansas Attorney General Comments at 1-2 (joined by attorneys general from 22 states, expressing that "[t]he proliferation of contraband cellphones in prisons and jails poses a serious threat to public safety, undermines institutional security, and facilitates ongoing criminal activity from behind bars"); CLA Comments at 6, 12 (contraband wireless devices "have repeatedly been used to orchestrate assaults, intimidate witnesses, extort families, and victimize both staff and incarcerated individuals," and jamming solutions could serve as a tool to "directly prevent the victimization" of the public, correctional institution staff, and incarcerated individuals); CLA Reply at 1-3; Florida Department of Corrections Comments at 2; Kansas Department of Corrections Comments at 1 (contraband wireless devices are used to conduct activities that "compromise the safety of correctional staff, others in the prison population, and the general public"); Daniel F. Martuscello III Comments; MSS *Ex Parte* Letter; NDAA Comments at 1 ("expanding the technological tools available to corrections officials" will promote public safety by "disrupt[ing] incarcerated criminal enterprises from operating"); North Carolina Department of Adult Correction Comments at 1-2; Oklahoma Department of Corrections Comments at 1-2 (contraband wireless devices "are tools of criminal enterprise," "enable incarcerated individuals to direct drug trafficking operations, order assaults, intimidate witnesses, and coordinate escapes," and create risk for correctional staff, "undermining both institutional safety and rehabilitation efforts"); Texas Department of Criminal Justice Comments at 1; West Virginia Division of Corrections and Rehabilitation Comments at 1.

[139] 47 U.S.C. § 303(y).

that section 303(y) prohibits the Commission from allocating electromagnetic spectrum for flexible use if that use would result in harmful interference among users.[140] We find no statutory violation here because we require that authorized jamming solutions, limited to licensed jamming containment areas, not cause harmful interference to licensed or authorized users. Furthermore, we do not interpret section 303(y) as requiring the Commission to afford protection from harmful interference to deauthorized users.

b. Arguments that Permitting Jamming Violates the Administrative Procedure Act

48. Some commenters point to the *Loper Bright* decision[141] as support for the argument that the Commission has no authority to permit jamming and that a Commission decision to authorize jamming will not receive court deference.[142] We find that the plain language of section 333's prohibition against willful or malicious interference unambiguously applies only to authorized or licensed stations. We therefore believe that, under a "best reading"[143] of the Act, deauthorized contraband wireless devices receive no protection from section 333, and that the Commission has the discretion to authorize jamming solutions to combat use in the limited context of correctional facilities in furtherance of its mandate to act in the public interest, convenience, and necessity, and to promote the safety of life.

49. CTIA argues that adoption of our regulatory framework would be arbitrary and capricious in violation of the APA.[144] It is well established that agency action must be "reasonable and reasonably explained" to survive the APA's arbitrary and capricious standard of review.[145] CTIA claims that our framework could not satisfy this standard of review primarily because it relies on the premise that jamming devices will block only "deauthorized" contraband wireless devices and not other authorized devices which, CTIA argues, is not technologically possible and runs counter to the evidence before the agency.[146] Accordingly, CTIA concludes, adopting our framework notwithstanding evidence that jamming will also block authorized communications is arbitrary and capricious.[147]

50. As we have explained, we agree that, as a technical matter, jammers cannot distinguish between authorized and deauthorized devices located *in the same geographic area*.[148] That said, our framework limits jamming to a containment area in which the use of contraband wireless devices is deauthorized by the Commission, and requires that a jamming solution not cause harmful interference outside of the containment area. We also impose rigorous testing requirements, technical parameters, and safety features that require the cessation of jamming operations upon a credible complaint of harmful interference. With these safeguards in place, we believe it is in the public interest to authorize jamming contained within a specific geographic area of a correctional facility. Any harmful interference to authorized wireless devices outside of the jamming area remains a section 333 violation. CTIA's

[140] CTIA Comments at 18, citing section 303(y)(2)(C) of the Act.

[141] *Loper Bright Enters. v. Raimondo*, 603 U.S. 369 (2024).

[142] *See* ITIF *Ex Parte* at 2 (asserting that the Commission cannot expect deference to substitute its reinterpretation of the statute); Public Knowledge Reply at 6, 9 (contending that the authorization of jamming fails under both standard statutory analysis and the Major Question Doctrine); CTIA Comments at 17 (noting that the Commission would not receive deference in interpreting even an ambiguous statute).

[143] *Loper Bright Enters*., 603 U.S. at 395, 400 (holding that only the "best reading" of a statute is permissible).

[144] CTIA Comments at 23-25; CTIA Reply at 12.

[145] *Ohio v. EPA*, 603 U.S. 279, 292 (2024) (citation omitted); *see also* 5 U.S.C. § 706(2)(A).

[146] CTIA Comments at 24, citing *Motor Vehicle Mfrs. Ass'n of the United States, Inc. v. State Farm Mut. Auto. Ins. Co*., 463 U.S. 29, 43 (1983) (agency rule is arbitrary and capricious if decision runs counter to the evidence before the agency or is so implausible that it cannot be ascribed to a difference in view or the agency's expertise).

[147] CTIA Comments at 24.

[148] *See supra* para. 32.

contention regarding the industry's apparent collective inability to contain the impact of jamming solutions appears to be irrespective of any proper engineering or network management techniques. We disagree that such speculation relegates a Commission determination to authorize, for public safety purposes, targeted jamming solutions in the limited context of correctional facilities, to the status of an arbitrary and capricious APA violation.[149]

51. CTIA also contends that the Commission would violate the APA through its failure to consider an important aspect of the problem, particularly, in its view, the likely proliferation of jamming devices.[150] We disagree with CTIA's argument that we have not considered this potential issue. In the *Third FNPRM*, the Commission repeatedly stated its concern that jamming devices might be misappropriated for unintended uses and therefore sought comment on specific ways to guard against proliferation.[151] In reliance on the record developed in response, we adopt a regulatory authorization framework, technical rules, and marketing and labeling restrictions for jamming equipment intended to ensure that only eligible entities will deploy jamming solutions.[152]

52. CTIA also contends that the deauthorization rule imposes a requirement on the wireless providers—facing potential liability for providing service to contraband devices that they have no means of identifying as unauthorized—that cannot be satisfied and thus is inherently arbitrary and capricious.[153] Relatedly, CTIA claims that any Commission action to bring an enforcement action against a wireless provider for failing to connect authorized devices that are blocked by a jamming solution would violate due process requirements because any such action could not satisfy the "ascertainable certainty" standard for imposing liability.[154] CTIA cites to the *Trinity* case for the proposition that the regulated party must be able to determine with "ascertainable certainty" what the agency expects it to do.[155] We believe that wireless providers can easily discover and definitively establish the location of correctional facilities, and whether the operation of contraband wireless devices in a particular correctional facility is in violation of a federal, state, or local law, or a correctional facility rule, regulation, or policy, which is the case in the vast majority of correctional facilities in the country. As jamming solutions are only authorized in those areas where wireless device operation is deauthorized, we do not find that our approach is arbitrary and capricious.[156]

---

[149] CTIA claims that "interference outside correctional facility walls is not a theoretical risk but a predictable outcome" and concludes that any implementation of a jamming solution would therefore violate section 333 of the Act. CTIA Comments at 12-15.

[150] *Id*., also citing *Cap. Power Corp. v. FERC*, 156 F.4th 644, 653 (D.C. Cir. 2025) (holding that a FERC order was arbitrary because the agency "failed to consider important aspects of the problem before it").

[151] *See, e.g.*, *Third FNPRM*, 40 FCC Rcd at 8021, para. 41 (regarding eligibility criteria); *Third FNPRM*, 40 FCC Rcd at 8014 (regarding the deauthorization rule); *Third FNPRM*, 40 FCC Rcd at 8056-58, paras. 125-129 (regarding marketing, labeling, and importation of equipment used for jamming solutions).

[152] In the context of correctional facilities, we are unaware of complaints regarding the proliferation of MAS base stations used outside the correctional facility environment, even without having imposed the types of restrictions we adopt today for jamming devices.

[153] CTIA Comments at 25.

[154] *Id.*, citing *Trinity Broad. of Fla., Inc. v. FCC*, 211 F.3d 618, 628 (D.C. Cir. 2000) (regulated party must be able to determine with ascertainable certainty what the agency expects it to do) (citing Gen. Elec. Co. v. EPA, 53 F.3d 1324, 1329 (D.C. Cir. 1995); *see also AT&T Corp. v. FCC*, 323 F.3d 1081, 1086 (D.C. Cir. 2003) (Court noting that FCC slamming rules charged carriers with "a virtually impossible task").

[155] CTIA Comments at 25, n.89.

[156] We note that the wireless carriers have not raised an arbitrary and capricious argument in the more than a decade of involvement as lessors in the deployment of MASs in correctional facilities, which similarly hinge on preventing the use of contraband wireless devices that are in violation of federal, state, or local law, or correctional facility rule, regulation, or policy. *See* 47 CFR §1.9003.

53. *Martha Wright-Reed Act*. Public Knowledge contends that the adoption of rules to authorize jamming solutions is inherently arbitrary and capricious because the Commission failed to implement the Martha Wright-Reed Act (MWRA), which required the Commission to ensure that wireline rates charged to incarcerated persons were just and reasonable.[157] As background, the Cell Phone Contraband Act of 2010 (Contraband Act of 2010), which prohibits the possession or use of cell phones and similar devices in federal prisons, also required that the Comptroller General submit a report to Congress within one year of enactment with the results of studies on cell phone use in prisons, efforts to prevent their use, and telephone rates within prisons to include costs, how revenue from inmate telephone services is used, and options for lowering costs.[158]

54. As an initial matter, we disagree with Public Knowledge that, in the Contraband Act of 2010, Congress established a "clear link" between the proliferation of contraband cell phones and the unjust and unreasonable rates charged to incarcerated people in the Contraband Act of 2010.[159] Requiring studies of telephone rates in federal prisons and cell phone use by inmates is not a Congressional determination that the use of contraband wireless devices is per se the result of unjust and unreasonable telephone rates in prisons. In 2022, Congress passed the MWRA, which expanded the Commission's jurisdiction over incarcerated people's communications services (ICPS) and directed the Commission to establish a plan to ensure just and reasonable charges for telephone and advanced communications services in correctional facilities.[160] Contrary to Public Knowledge's assertion, there is no MWRA provision establishing a nexus between unjust and unreasonable ICPS rates and the proliferation of contraband wireless devices in prisons. Not only has Congress not directly linked the issue of contraband wireless device use in correctional facilities with unjust and unreasonable ICPS rates, but the Commission has affirmatively separated the issues. In its 2024 order implementing the MWRA, the Commission stated that the issue of contraband devices in correctional facilities is "unrelated to our implementation of the Martha Wright-Reed Act or the consideration of the costs of necessary safety and security measures for inclusion in just and reasonable rates for IPCS."[161] Further, in discussing the purpose and scope of the MWRA in that proceeding, the Commission does not once mention contraband wireless devices.[162]

55. Public Knowledge cites to *National Lifeline Ass'n v. FCC* for the premise that an agency acts in an arbitrary and capricious manner when "it fails to grapple with an important element of the problem."[163] Public Knowledge argues that because the Commission did not seek comment on what it characterizes as an important element of the contraband phones in prison problem, i.e., its connection to unjust and unreasonable ICPS rates, adopting rules to authorize jamming solutions is automatically arbitrary and capricious.[164] We disagree, finding that we have clear authority in the public interest to facilitate solutions to combat unsecure, unmonitored, contraband device use by those seeking to

[157] Public Knowledge Reply at 12-13; *see generally* Pub. L. 117-338 (Martha Wright-Reed Act). MSS also argues that there is an interaction between prison phone pricing and contraband wireless devices in prisons, and that the Commission should consider this interaction when making decisions with respect to the public interest analysis. MSS *Ex Parte* Letter at 2-3.

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

[159] Public Knowledge Reply at 12.

[160] Martha Wright-Reed Act.

[161] *Incarcerated People's Communications Services; Implementation of the Martha Wright-Reed Act Rates for Interstate Inmate Calling Services*, Report and Order, Order on Reconsideration, Clarification and Waiver, and Further Notice of Proposed Rulemaking, 39 FCC Rcd 7647, 7839, n.1313 (2024) (*IPCS Order*).

[162] *See IPCS Order*, 39 FCC Rcd at 7666-67, paras. 31-32.

[163] Public Knowledge Reply at 13, citing *Nat'l Lifeline Ass'n v. FCC*, 921 F.3d 1102, 1110 (D.C. Cir. 2019).

[164] *Id*.

perpetuate criminal activity, irrespective of the Commission's separate consideration of the state of ICPS rates.

56. *Subdelegation*. Verizon argues that the Commission may not delegate its function of determining the location of classes of stations or individual stations to state or local governments or to other federal agencies.[165] By applying the deauthorization rule to areas where state or local authorities prohibit the use of contraband wireless devices, Verizon argues, the Commission is unlawfully delegating the authorization status of mobile stations to state or local governments or individual correctional facilities.[166] CTIA contends that the deauthorization rule we adopt today—which applies to subscribers that operate contraband wireless devices where a federal, state, or local law, or a correctional facility rule, regulation, or policy make such operation unlawful—is an unlawful subdelegation of the Commission's responsibility to make licensing and authorization decisions to states, localities, and private entities.[167] CTIA cites to *U.S. Telecom Ass'n v. FCC* for the proposition that subdelegations to outside parties, both state and private, "are assumed to be improper absent an affirmative showing of congressional authorization."[168] In *U.S. Telecom Ass'n v. FCC*, however, the court discussed specific types of legitimate outside party input into agency decision-making processes, one of which is establishing a reasonable condition for granting federal approval.[169] The court stated that a federal agency may condition its grant of permission on the decision of another entity, such as a state, local, or tribal government, provided that there is a reasonable connection between the outside entity's decision and the federal agency's determination, citing cases in which an agency had adopted an "obviously relevant local concern" as an element of its decision process.[170]

57. Here, the Commission establishes by rulemaking the class of devices to be deauthorized, and fully retains decision-making authority regarding whether or not to grant authority to an applicant seeking to deploy a jamming solution in a correctional facility based on technical demonstrations and successful testing results. The Commission requires that the licensed area be no larger than the area(s) where operation of a contraband wireless device within a correctional facility is in violation of federal, state, or local law, or a correctional facility rule, regulation, or policy, tantamount to a "condition" contemplated in *U.S. Telecom Ass'n v. FCC*. Further, we recognize that the severity of contraband wireless device use at a particular correctional facility and the ability to fund a jamming solution is a local consideration, and therefore we permit DOCs, through applicable laws and policies, to inform the number of wireless devices ultimately deemed contraband by establishing the jamming containment area. We find, however, that there is no improper subdelegation regarding the Commission's establishment of the overall class of devices warranting deauthorization, as well as our decision-making authority to authorize jamming solutions.

58. We note that, in the *Second R&O*, the Commission took a similar approach by establishing the CIS disabling process and imposing mandatory obligations on the wireless providers to

[165] Verizon Comments at 8, citing to 47 U.S.C. §§ 301, 303(d), 316.

[166] *Id*.

[167] CTIA Comments at 25-26, citing 47 U.S.C. §§ 301, 303(d), and 303(h).

[168] *U.S. Telecom Ass'n v. FCC*, 359 F.3d 554, 565–66 (D.C. Cir. 2004). CTIA explains that, applying that presumption, the D.C. Circuit has vacated, as an unlawful subdelegation, those portions of an order that "delegate[d] to state commissions the authority to" make decisions that Congress vested with the FCC. *Id.* at 568.

[169] *Id*. at 567.

[170] *Id*., citing *United States v. Matherson*, 367 F.Supp 779, 782-83 (E.D.N.Y. 1973), aff'd 493 F.2d 1339 (2d Cir. 1974) (the court upheld the decision of the Fire Island National Seashore Superintendent to condition issuance of federal seashore motor vehicle permits on the applicant's acquisition of an analogous permit from an adjacent town) and *South Pacific Transp. Co. v. Watt*, 700 F.2d 550, 556 (9th Cir. 1983) (citing *Matherson,* sustained the Secretary of Interior's conditioning of right-of-way permits across tribal lands on the tribal government's approval).

comply with qualifying requests to disable contraband devices based on a federal or state law criminal statute prohibiting the possession or operation of contraband wireless devices in a correctional facility.[171] And in the 2017 FNPRM, when first proposing the disabling rules, the Commission clarified that a disabling request would be pursuant to an adopted Commission rule where certain criteria are met, and that the Commission would not be delegating decision-making authority regarding the disabling of contraband wireless devices.[172] We similarly maintain decision-making authority in applying a detailed regulatory framework for authorizing jamming solutions. We also observe that, during more than a decade of CIS deployments preferred by wireless providers, none have argued that the Commission unlawfully subdelegated its section 301 responsibilities by permitting leasing for the sole purpose of capturing and terminating transmissions that are licensed by the Commission, but are nonetheless "illegal" based solely on federal, state, or local law, or correctional facility policy determinations.

59. As additional support for its position, CTIA argues that the delegation to private correctional facilities would raise constitutional questions under the private nondelegation doctrine.[173] In *Consumers' Research*, the Court ruled that the Commission did not violate the doctrine because it retained all decision-making authority within the universal-service contribution scheme.[174] The Court held that there was "no impermissible transfer of authority" when the USAC Administrator submitted recommendations to the Commission, but did not govern or make decisions.[175] Again, in this proceeding, we are permitting jamming only when eligible entities satisfy certain criteria, including that the jamming containment area, as licensed by the Commission, is no larger than the area where the use of contraband wireless devices is in violation of federal, state, or local law or correctional facility regulation or policy. We therefore find without merit CTIA's position that there is an unlawful delegation of authority to private parties.

60. *Major Question Doctrine*. Public Knowledge asserts that the Commission's proposal violates the Supreme Court's "Major Question Doctrine" (MQD) and that the Commission has no authority to adopt rules to authorize jamming solutions.[176] As the Court explained in *West Virginia v. EPA*, the major questions doctrine was developed over a series of significant Court cases addressing circumstances in which agencies have asserted "highly consequential power beyond what Congress could reasonably be understood to have granted."[177] These cases involved "extravagant statutory power over the national economy" or were otherwise "extraordinary" cases that required decisions of "magnitude and consequence."[178] In his concurrence to *West Virginia v. EPA*, Justice Gorsuch described this doctrine as applying to cases involving agencies claiming the power to make decisions of "vast" economic and political significance.[179] Under the facts of *West Virginia v. EPA*, the Court concluded that it was a major questions case that involved a statute that the agency argued gave it the power to "substantially restructure

[171] *See Second R&O*, 36 FCC Rcd at 11825-26, para. 31.

[172] *See First FNPRM*, 32 FCC Rcd at 2369, para. 86, citing *U.S. Telecom Ass'n v. FCC*, 359 F.3d 554, 566 (D.C. Cir. 2004).

[173] CTIA Comments at 26, arguing that, unlike in the Consumers' Research decision, the delegation to private correctional facilities is to entities that are not "broadly subordinate to the Commission" and are not governed by a backend review process by the Commission. *FCC v. Consumers' Rsch*., 145 S. Ct. 2482, 2508–09 (2025).

[174] *FCC v. Consumers' Rsch*., 145 S.Ct. 2482, 2492 (2025).

[175] *Id.*

[176] Public Knowledge Reply at 9-11.

[177] *West Virginia v. EPA*, 597 U.S. 697, 724 (2022).

[178] *Id.* at 735.

[179] *Id*.

the American energy market."[180] Other instances where the major questions doctrine was applied include those involving an agency's assertion of power to regulate tobacco products, ban drugs used in physician-assisted suicide, and enforce a vaccine mandate.[181] In such cases, the agency must have clear congressional authorization for the authority claimed by the agency.

61. Public Knowledge's position is conclusory at best, stating with no support that "unleashing jammers on the wireless world constitutes a question of economic importance" and the authorization of jamming solutions would be the Commission acting in a "dramatic manner."[182] We disagree that authorizing non-federal jamming solutions in the limited context of correctional facilities is a major question requiring application of Justice Gorsuch's "several telling clues" as to what courts look at to determine what qualifies as clear congressional authorization.[183] In his concurrence, Justice Gorsuch first lists three triggers for when the MQD should apply: (1) when an agency claims the power to resolve a matter of great "political significance"; (2) when an agency seeks to regulate "a significant portion of the American economy"; and (3) when an agency seeks to intrude into an area that is the particular domain of state law."[184] The Court applied this list to the facts of *West Virginia v. EPA* to find a major question, because the question of whether coal and gas-fired power plants should be allowed to operate "is a question everyone can agree is vitally important."[185]

62. In contrast to *West Virginia v. EPA* and other MQD case law, a proceeding authorizing jamming solutions in the context of correctional facilities does not in our view rise to the level of extreme economic or political sensitivity mandating application of the major questions doctrine. Adopting a narrowly tailored regulatory construct with strict rules to prevent jamming devices from proliferating outside of the correctional facility context runs counter to a narrative that our action is one of "political significance" or that it affects a "significant portion" of the American economy. Because our adoption of a regulatory framework to authorize jamming solutions is not, in our view, a major questions case, we need not reach, as a legal matter, Public Knowledge's application of Justice Gorsuch's "checklist" to measure whether Congress has granted us the authority to create rules in this area.[186]

C. Authorization of Jamming Solutions in the Public Interest

63. Throughout this proceeding, the Commission has pursued the vital public safety goal of combatting the use of contraband wireless devices in correctional facilities, while recognizing statutory limitations and the potential impact that any RF-based solutions, if not properly deployed, might have on authorized communications. To balance these competing concerns, the Commission in the *Third FNPRM* proposed and sought comment on a narrowly tailored authorization mechanism for the non-federal operation of RF jamming solutions, limited to the context of correctional facilities, that complies with section 333 of the Act and contains safeguards to protect authorized wireless network operations from harmful interference.[187] Drawing on its experience with CIS deployments pursuant to the secondary markets framework, whereby stakeholders are required to collaborate in good faith to execute spectrum leasing arrangements, the Commission proposed a leasing model to substantially leverage this market-

[180] *Id.*

[181] *Id*. at 741.

[182] Public Knowledge Reply at 9.

[183] *West Virginia v. EPA*, 597 U.S. at 746.

[184] *Id.* at 743-44.

[185] *Id*. at 745. Other factors weighing in favor of the case being a major question case included that the electric power sector is among the largest in the U.S. economy, the proposed rule would eliminate jobs, and consumers' electric costs would rise dramatically. *Id*. at 745-46.

[186] Public Knowledge Reply at 9-11.

[187] *See Third FNPRM*, 40 FCC Rcd at 8019, para. 35; 47 U.S.C. § 333.

based approach and apply it to the authorization of jamming solutions.[188] The Commission reasoned that a leasing approach for the authorization of jamming solutions would promote stakeholder engagement on this issue,[189] and would reduce complexity and regulatory burdens.[190] As another option, the Commission proposed a non-exclusive overlay licensing path whereby eligible entities would apply directly for an overlay jamming license, provided certain conditions were met.[191] At the time the Commission sought comment, however, the record addressing necessary technical restrictions on jamming solutions, as distinct from CIS, was not yet developed.

64. As discussed, the record reflects opposition from some stakeholders to the overall concept of the Commission authorizing jamming solutions, based on legal, policy, and technical considerations. CTIA argues that the Commission's proposed framework is unlawful, and that jamming solutions will block legitimate communications and negatively impact public safety because jamming cannot be adequately limited to targeted areas.[192] Similarly, AT&T opposes any authorization of jamming not only because it would exceed the Commission's legal authority, but also because jammers would threaten public safety connectivity and other lawful communications and, in fact, would be potentially "catastrophic."[193] AT&T argues that the proposed authorization framework will inevitably violate section 333 so is unworkable.[194] Neither CTIA nor AT&T submitted any comment regarding the specifics of the Commission's proposed leasing framework (e.g., eligibility, immediate approval procedures, notification requirements) or the part 2 equipment authorization process. T-Mobile did not file comments or a reply in response to the *Third FNPRM*.

65. Verizon offers an alternative "leasing" framework, but makes clear that it does not believe that the Commission's proposed authorization framework is permitted under the Communications Act.[195] Verizon's suggested alternative leasing process includes the possibility of the Commission imposing an "involuntary lease" and holding a jamming solutions provider solely liable for the jamming system's effectiveness.[196] These components of Verizon's proposed "leasing" framework are inconsistent with the Commission's envisioned approach when it proposed in the *Third FNPRM* to largely apply existing leasing rules for jamming solutions to reduce regulatory burdens and encourage stakeholder participation.[197] Although we appreciate Verizon's effort to submit a proposed jamming authorization framework involving stakeholder collaboration, we decline to incorporate Verizon's suggestion into our adopted framework. We find that its alternative version of leasing presents regulatory challenges as a significant departure from the fundamental principles of our existing secondary markets rules that address control of spectrum and related rights and responsibilities of the parties, and will result in unnecessary delay in DOC efforts to solve a pressing public safety issue.[198]

---

[188] *See Third FNPRM*, 40 FCC Rcd at 8019-35, paras. 36-71.

[189] *Id*. at 8019, para. 36.

[190] *Id.*

[191] *Id*. at 8035-48, paras. 72-108.

[192] CTIA Comments at 17-26, 10-14; CTIA Reply at 3-13.

[193] AT&T Reply at 2, Comments at 6-14.

[194] AT&T Comments at 13.

[195] Verizon Comments at 4-8.

[196] *See* Verizon Reply at 7-8 (describing the process whereby an involuntary lease is imposed); Verizon Reply at 9-10 (agreeing with AT&T and CTIA on the need for federal preemption of state law liability for impact on authorized communications and stating that the vendor should bear any applicable liability for the system's effectiveness).

[197] *Third FNPRM*, 40 FCC Rcd at 8019-30, paras. 36, 38.

[198] *See infra* para. 124.

66. In sum, we conclude that, at least in the near term, widespread leasing arrangements in this context are unlikely, given the wireless providers' opposition to the Commission's proposed deauthorization framework and accompanying authorization proposals for jamming solutions, coupled with a DOC preference for overlay licensing.[199] In the *Third FNPRM*, the Commission stated, in connection with several components of the proposed framework, a clear goal of incentivizing wireless provider participation in deploying jamming solutions in correctional facilities, in the first instance by leveraging, where appropriate, the existing leasing process.[200] Based on the record, and our overarching goal of enhancing public safety by facilitating the deployment of new technologies to combat contraband wireless devices in correctional facilities, we believe that the most direct and efficient route to achieving this goal is by adopting a non-exclusive overlay licensing framework. We agree with CLA that the overlay framework is an "essential safeguard against delay."[201] Below, we describe this approach in detail, including the guardrails necessary to limit jamming operations only to the correctional facility environment. We adopt an overlay licensing framework as a direct path that we anticipate will result in timely jamming solution deployments in the public interest. To reiterate a key concept underpinning today's action, we do not mandate the implementation of jamming solutions, nor the authorization mechanism. Stakeholders are afforded the flexibility, if seeking this technological alternative for a particular correctional facility, to pursue either direct overlay licensing or to enter into an arms-length leasing arrangement. We recognize that, although the authorization processes that we adopt today are straightforward, DOCs and vendors seeking jamming solutions may not be familiar with our licensing and leasing processes. Therefore, to assist stakeholders, we direct WTB to issue a public notice and related materials as necessary to guide compliance with our requirements. We also note that staff, including the Contraband Ombudsperson, will be available to help explain and clarify concepts and requirements.

1. Table of Allocations

67. The Commission sought comment in the *Third FNPRM* on whether the authorization of jamming solutions through issuance of overlay licenses in bands currently licensed to wireless providers would require an amendment to the U.S. Table of Allocations (U.S. Table), including potentially the addition of a footnote applicable to relevant bands.[202] We received no comments on this issue. We find that it would serve the public interest to create a US footnote to establish a primary fixed and land mobile service allocation for jamming solution operations, indicating that such use is limited to the context of correctional facilities addressing contraband wireless device use. Specifically, we place the following footnote in bands where jamming solutions are permitted: "USXXX A jamming solution may be authorized subject to part 90, subpart Z of this chapter to prevent the operation of wireless devices in correctional facilities deemed contraband through a federal, state or local law, or a correctional facility rule, regulation, or policy. Jamming solution operation is permitted under a primary allocation in the fixed and land mobile services, limited to a jamming containment area within a correctional facility. Beyond the authorized jamming containment area, RF signals generated by a jamming solution are on a non-interference basis and shall not cause harmful interference to authorized services or devices."

[199] *See* CLA Comments at 8.

[200] *See Third FNPRM*, 40 FCC Rcd at 8014, para. 23 (anticipating that the deauthorization approach would facilitate jamming to increase public safety, while incentivizing wireless provide participation); *id.* at 8018, para. 34 (indicating that the proposed safe harbor would address liability concerns, while encouraging wireless providers to work with correctional facilities to combat the problem); *id.* at 8019, para. 36 (noting that a leasing approach would promote stakeholder engagement on this important issue).

[201] CLA Comments at 8. Other commenters also generally support the adoption of an overlay licensing framework. *See* Vortezon Comments at 16; DI Group Comments at 7; SOC LLC and Hawks Ear Communications LLC (CIS Providers) Comments (CIS Providers Comments) at 6.

[202] *Third FNPRM*, 40 FCC Rcd at 8038, para. 80.

68. We clarify that our addition of US footnote XXX, providing for a co-primary allocation in bands where jamming solutions are authorized to operate in jamming containment areas within a correctional facility, affords previously deployed primary wireless operations within the containment area on the referenced bands no co-primary "first-in-time" priority rights. We find this approach warranted given the vital public safety purpose jamming solutions serve to prevent any communications in the authorized jamming containment area, and particularly where the operations of such contraband wireless devices are no longer in accordance with the U.S. Table, or authorized under section 301 of the Act and section 1.903(c) of the Commission's rules. We note that our change to the U.S. Table implicates spectrum bands deployed for jamming solutions under either overlay licensing or through a *de facto* transfer spectrum leasing arrangement.

2. Proof of Concept Test

69. An essential part of the regulatory framework we adopt today, and the necessary first step in the process, is requiring a one-time proof of concept (POC) test for each proposed jamming solution that supplants the need for a Commission established pilot program and ultimately will expedite authorization of jamming solutions. Real-world POC testing of a jamming solution at a correctional facility chosen by the proponent, pursuant to a part 5 experimental license granted by the Commission, will enable solutions providers to demonstrate that the jamming system works as intended to contain harmful interference to a targeted area, addressing a primary stakeholder concern. A one-time, representative POC test for a given jamming device technology will then be used to support applications for jamming licenses or leases for the deployment of the jamming solution at multiple correctional facilities. As the Commission noted in the *Third FNPRM*, a party seeking to implement a jamming solution at a correctional facility is likely to be interested in testing the system, for example, in response to a DOC's request for proposal or to be eligible to enter into a contract with a DOC.[203] The Commission sought comment on when to permit the operation of jamming solutions vis-a-vis the equipment authorization process.[204] The Commission explained that the operation of an RF device prior to equipment authorization is permitted through grant of an experimental radio service license issued by the Office of Engineering and Technology (OET) under part 5 of the Commission's rules.[205]

70. After a thorough review of the record, we find that requiring an up-front, initial POC test will best serve the public interest by ensuring that the jamming device technology can function as intended at an actual correctional facility under real-world conditions, not merely through theoretical calculations based solely on engineering models. The one-time POC test for each jamming device technology will ensure the application and authorization process is properly data-driven and efficient, enabling the expeditious deployment of jamming solutions. To streamline the process, although we require the POC test as the first step in the licensing process for a jamming solution, we do not require the results to be filed until a party submits a license or lease application. To streamline and simplify the process for carrying out the POC test, we direct WTB and OET to issue a Public Notice outlining a fast-track process for submitting a lean experimental license application. The Public Notice will expedite the process by describing minimal filing information (e.g., spectrum bands, location, date) and directing applicants to certify to a set of operating limitations that will be common to all such testing (e.g., non-

[203] *Id*. at 8055, para. 124.

[204] *Id*.

[205] 47 CFR § 2.805(b). In the *Third FNPRM*, the Commission noted 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)), it interpreted that to mean any "authorized station," and therefore under the 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. *See Third FNPRM*, 40 FCC Rcd at 8056, para. 124, n.282.

interference operation, stop buzzer, wireless carrier notification, prison designation of appropriate testing area).

71. In the *Third FNPRM*, the Commission sought comment on whether to adopt a phased implementation of jamming solutions, which might include such a pilot program.[206] The record includes support for a phased implementation of jamming solutions, such as through a pilot program, intended to help stakeholders assess the impact of jamming solutions prior to the adoption and implementation of a full authorization framework.[207] In fact, the VT-ARC Report reflects that the recent jamming test conducted in South Carolina was "intentionally designed as a proof-of-concept assessment rather than a full-scale operational deployment evaluation . . . and provided the first controlled, real world field test on how a modern micro-jamming system performs in a correctional facility environment and interacts with commercial and public safety spectrum."[208] The VT-ARC Report cautions that findings from the test are specific to the particular deployment as tested at the Broad River Correctional Institution, and that "[s]ite specific results should not be generalized or directly applied to other facilities or jamming products without further testing . . . ."[209] MITRE, an entity sponsored by the SC DOC that collected data during the VT-ARC test in South Carolina, also warns that test results are not directly applicable to other locations with different RF environments and that location-specific evaluations would be needed to determine the impact of a jamming deployment.[210] The SC DOC, in its own assessment of the test, stresses that each deployment of a jamming solution must be specifically designed, calibrated, and tested at each facility "before a system is placed in service."[211] Several commenters suggest that pilots could be useful to test technology prior to adopting technical safeguards.[212] For example, CTIA argues that the VT-ARC test demonstrates that further testing is required to address questions as to the effectiveness of jamming solutions.[213] CTIA also contends that the Commission must start with pilots to gather information to inform technical requirements for jamming solutions and mandate testing "to assess real-

[206] *Third FNPRM*, 40 FCC Rcd at 8058, paras. 130-32.

[207] *See, e.g.*, Oklahoma DOC at 2 (arguing that a pilot would allow for practical evaluation of jamming systems while gathering real-world data for national deployment standards); CCA Comments at 6 (suggesting narrow, site-specific pilot programs); Industry Council for Emergency Response Technologies, Inc. Comments (iCERT Comments) at 8-9 (supports pilots to gather insights on technical feasibility and challenges of jamming); GSMA comments at 2 (supporting a pilot program with Commission action deferred until testing is complete).

[208] VT-ARC Report at 5. In 2018 and 2019, the Bureau of Prisons (BOP), in collaboration with the Commission and the National Telecommunications and Information Administration (NTIA), tested micro-jamming technology at correctional facilities in Maryland and South Carolina, respectively, to determine whether the technology could block inmate calls from a contraband device in a housing unit. *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. NTIA subsequently released a report on the results of the testing in South Carolina, which some characterize as demonstrating that the targeted use of the technology could be effective in fighting contraband cell phone use in correctional facilities. 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. *See* South Carolina DOC Comments at 3 (claiming that the trial showed effective containment of a jamming solution); J3 Tech Comments at 2.

[209] VT-ARC Report at 6.

[210] MITRE Report at 5-4.

[211] *See* SC DOC *Ex Parte* Letter at 4-6.

[212] *See, e.g.*, AICC Reply at 5; Association of Public-Safety Communications Officials-International, Inc. Reply (APCO Reply) at 2-3.

[213] CTIA Oct. 1 *Ex Parte* Letter at 2, 8.

word consequences."[214] AT&T concurs, stating that no jamming technology should be authorized unless specifically tested in a pilot program and verified as demonstrating no risk to authorized communications.[215] APCO recommends comprehensive testing "under real-world conditions" to ensure jamming does not compromise public safety.[216] In addition to pilots, CTIA argues that jamming vendors must demonstrate that they can implement a solution without interrupting lawful communications and that every jamming deployment, whether authorized by lease or overlay license, should be subject to site-specific testing coordinated with affected wireless providers.[217] The common thread in the overall support for a pilot program is the desire to prove under real-world conditions at a correctional facility that a jamming solution can be contained to the area in a facility where it is authorized to conduct jamming operations, and not impact legitimate communications outside of that area.

72. Some parties oppose the imposition of a pilot program as unnecessary or the source of undue delay. For example, CLA argues that a pilot program "would not be responsive to the urgent pleas for assistance from the corrections field, other law enforcement, state Attorneys Generals, and governors."[218] CLA states that it is most likely that jamming solution authorization requests will not be widespread due to the practicalities and costs, and that the Commission's rules will serve as sufficient safeguards against harmful interference.[219] The SC DOC references past testing and the VT-ARC test results, arguing that a pilot program is unnecessary.[220] The SC DOC explains that "every month of delay [resulting from additional general testing] carriers real consequences for staff, inmates, and the public," instead favoring site-specific testing prior to deployment and safeguards, aligned with the requirements described in this *Third R&O*.[221] J3 Tech highlights past field tests of jamming technologies and contends that the "time for delay is over—it is time for action."[222]

73. After considering the record, we find that implementing a formal pilot program at this time would cause undue delay in bringing this valuable tool to aid the corrections community in combatting this problem. Rather, requiring a POC test at a correctional facility of choice at the outset of the authorization process, coupled with subsequent post-license grant on-site testing at the specific correctional facility where a jamming solution overlay or lease authorization is sought, will serve the same public interest purpose of ensuring the accuracy and precision of jamming solutions. Indeed, the required POC test is designed to achieve the same purpose as a pilot to test in real-world circumstances, but is more expeditious. We believe that a POC test allows a range of jamming solutions manufacturers and providers to demonstrate the capabilities of jamming equipment, along with the ability to competently install that equipment to ensure that emissions outside jamming containment areas do not cause harmful

[214] CTIA Comments at 5.

[215] AT&T Comments at 16.

[216] APCO Reply at 2.

[217] CTIA Comments at 28.

[218] CLA Comments at 10. CLA argues that jamming testing has already occurred, and "slow-rolling jamming solutions in the form of a pilot program would only further delay" the use of this interdiction tool. CLA Comments at 11 (noting that there was testing in 2018 at a federal facility in Maryland that demonstrated the feasibility of jamming). Vortezon also argues that a phased implementation would result in delay to deploying solutions that are urgently needed in correctional facilities. Vortezon Comments at 22.

[219] CLA Comments at 10.

[220] South Carolina DOC Comments at 6 (noting the NTIA jamming trials in Maryland in 2018 and South Carolina in 2019); SC DOC *Ex Parte* Letter at 5.

[221] SC DOC *Ex Parte* Letter at 5-6.

[222] Letter from J3 Technology LLC to Marlene H. Dortch, FCC, GN Docket No. 13-111, at 8 (filed Oct. 5, 2026) (J3 Tech *Ex Parte* Letter).

interference to authorized users. Further, a POC test provides for significantly shorter deployment times than requiring a pilot test program prior to adopting rules, while accomplishing the same goals.

74. We find that any benefit that might arise from conducting a lengthy pilot program prior to adoption of rules, or pursuing a phased implementation approach, is outweighed by the cost of delayed deployment of jamming solutions.[223] Here, any roll-out of jamming solutions will necessarily be on a case-by-case basis at particular correctional facilities with different configurations, construction materials, security needs, geographic locations, and proximity to wireless provider base stations and the associated authorized end users. As such, following POC testing, we anticipate that targeted post-license grant pre-operational testing will enable accurate assessment of the impact of a jamming solution on a given RF environment. As stated in the VT-ARC Report, assessing the operation of a jamming solution in the context of the specific local jamming deployment is essential, where the local RF environment, commercial network conditions, and facility architecture, etc., can be considered.[224] The MITRE Report also concludes that a jamming solution deployment would require local, site-specific design and evaluation.[225] We agree with stakeholders that a jamming system is not a "turnkey" or "plug-and-play" system, but rather a solution that requires engineering and deployment of resources tailored to the specific correctional facility environment.[226] CTIA concludes from the VT-ARC test results that a full-scale deployment of a jamming solution in a correctional facility would inevitably result in a significant increase the risk to authorized communications, apparently rejecting VT-ARC Report's express caveat that the test results not be generalized and should be interpreted within the limited parameters of the test.[227] Such a sweeping extrapolation appears misplaced, as we anticipate that an experimental test of this nature would inevitably result in harmful interference to test devices located outside the proposed jamming containment area, so that necessary technical adjustments can be made to maximize efficiencies and ultimately achieve the desired RF footprint that does not cause harmful interference outside the designated area. We find that adopting an authorization framework that mandates two levels of testing obviates the need for a lengthy pilot program prior to adoption of an authorization framework, is more efficient, will better address the RF environment at each specific correctional facility location, and will enhance public safety.

75. To conduct the required POC test as an initial step in either the overlay or leasing approach, an eligible solutions provider seeking to deploy a jamming solution at a correctional facility must obtain an experimental radio service license from OET under part 5 of the Commission's rules.[228] We will not require an applicant to have equipment authorizations in place at the time it files an application for an experimental license.[229] Rather, equipment authorizations will be required no later than site-specific testing that follows grant of a WTB overlay license or approval of a lease arrangement.[230] We require that experimental licensees provide at least seven days advance notification of the POC test to all relevant wireless providers, as well as FirstNet, to allow them the opportunity to attend and participate.

---

[223] *See* Richard Bennett Reply at 5 (suggesting that the FCC convene a panel and conducts trials over the course of two or three years).

[224] *See* VT-ARC Report at 9, 127-28.

[225] *See* MITRE Report at 4-2 – 4-3.

[226] *See, e.g.*, CTIA Oct. 1 *Ex Parte* Letter at 8-9. *See also* TalkTelio *Ex Parte* Letter at 5 (explaining that an effective jamming solution contained to a targeted area requires engineering the solution specific to the local facility environment).

[227] *See* CTIA Oct. 1 *Ex Parte* Letter at 5; VT-ARC Report at 6.

[228] 47 CFR § 2.805(b). We note that applications for part 5 experimental licenses that include bands with shared federal/non-federal allocations are coordinated with NTIA.

[229] *See* 47 CFR § 2.805(1).

[230] *See infra* paras. 120, 143.

We define "relevant wireless providers" in a similar manner as defined in the CIS disabling context.[231] As discussed below, eligible entities seeking to apply for an overlay license or a lease for a jamming solution will be required to submit, along with their application, POC test results demonstrating that the jamming solution does not cause harmful interference to authorized devices located outside the jamming containment area, and that the POC test was representative of, and scalable to, the jamming solution that will be deployed pursuant to the lease or overlay license. WTB will evaluate the results of the POC test as part of the application review process of a solutions provider seeking authority to operate a jamming solution at a specific correctional facility.[232] We believe that requiring a successful POC test at the outset of the jamming solution authorization process will serve as a foundation for stakeholders to build confidence that authorized users can be protected when a jamming solution is ultimately deployed.

3. Non-Exclusive Overlay Licensing

76. In this section, we establish a non-exclusive overlay licensing path for authorizing jamming solutions, available to eligible entities, including application, licensing, operating, and technical rules. We also explain the timing of testing requirements adopted as part of the application process. We believe that this approach strikes the appropriate balance between expediting the availability of jamming as a technical solution to combat contraband wireless devices in correctional facilities and the need to prevent harmful interference to authorized wireless devices consistent with section 333 of the Act and the public interest.

77. Because we find that a non-exclusive, eligibility-based licensing scheme serves the public interest, we will not be accepting mutually exclusive applications, and we will not conduct a system of competitive bidding for such licenses pursuant to section 309(j) of the Act.[233] 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.[234] As discussed below, our overlay licensing approach allows more than one applicant to provide jamming solutions at a specific facility at a DOCs option, and any such application will be processed on a first come-first served basis. As a result, mutual exclusivity is not created that otherwise would require resolution through competitive bidding under section 309(j).

78. In the *Third FNPRM*, the Commission sought comment on the appropriate Commission rule section(s) to house the service and technical rules applicable to jamming solutions in a non-exclusive overlay licensing approach. As noted, wireless providers currently serving correctional facilities across multiple spectrum bands are regulated under various rule parts, including parts 22, 24, 27, 30, 90, and 96.[235] Future jamming solution providers will also be transmitting on these same bands. The Commission proposed to adopt a new, standalone part 90 subpart to govern the use of overlay licenses for jamming solutions.[236] Alternatively, we sought comment on authorizing jamming solutions licensees by spectrum band through each of these many rule parts. After a review of the record, we find that creating a new part 90 subpart for rules applicable only to jamming solutions in the correctional facility context will best serve the public interest as the most clear and administratively efficient approach. Part 90 will include not only the service rules for jamming solution overlay licensees, but also the core technical rules

[231] *See* 47 CFR § 20.23(b)(3)(i).

[232] *Id*.

[233] *Third FNPRM*, 40 FCC Rcd at 8036, para. 74; 47 U.S.C. § 309(j)(2)(A).

[234] 47 U.S.C. § 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.").

[235] *Third FNPRM*, 40 FCC Rcd at 8037, para. 76.

[236] *Id*.

for all jamming devices, whether authorized for deployment through an overlay license or a spectrum lease arrangement as discussed below.

a. Regulatory Matters

79. *Eligibility Restrictions*. To ensure that jamming solutions are permitted only in the limited context of correctional facilities to serve a specific public safety goal, we adopt the Commission's proposal 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 such a DOC.[237] The South Carolina DOC supports our eligibility restriction, noting that it is important for stakeholders to trust the jamming framework and to prevent abuse by "malicious or irresponsible" jamming actors.[238] We concur and find that mitigating the risk that jamming solutions are deployed in contexts other than a correctional facility is a key consideration in delineating eligibility criteria.

80. The Commission also proposed that to be eligible to seek an overlay license for a jamming solution: (1) the applicant 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 spectrum lease arrangement.[239] Because we do not require good-faith negotiations toward a spectrum leasing arrangement for jamming solutions, and also establish the overlay licensing framework as a method of authorizing jamming solutions, we decline to adopt either proposal in establishing eligibility.

81. The Commission also sought comment on whether we should consider additional eligibility restrictions in our overlay licensing framework.[240] The CIS Providers contend that only CIS providers authorized under section 20.23 of the Commission's rules should be eligible for overlay licensing.[241] Section 20.23 applies to any entity seeking CIS certification authorized for use in the submission of qualifying disabling requests to a wireless provider.[242] As explained herein, a jamming solution is distinct from a CIS, both in RF approach and in its intended purpose, and is therefore subject to different rules and requirements. CIS certification applies to entities using interdiction technology, such as MAS, that is not a jamming solution. In accordance with our overall approach of creating a firm regulatory divide between CISs and jamming solutions, as reflected in the definitions adopted herein, we do not find it appropriate to apply this restriction on the eligibility of applicants for overlay licensing.

82. Additionally, the Commission sought comment on whether we should consider, as an eligibility criterion, the location of a correctional facility, e.g., limiting authorization of jamming solutions to facilities in rural areas.[243] Several commenters object to this suggestion.[244] We agree with commenters that our overall framework, including equipment authorization application requirements, and rigorous

[237] *Id*. at 8037, para. 78.

[238] South Carolina DOC Comments at 4.

[239] *Third FNPRM*, 40 FCC Rcd at 8037, para. 78.

[240] *Id*. at 8038, para. 79.

[241] CIS Providers Comments at 7.

[242] *See* 47 CFR § 20.23.

[243] *Third FNPRM*, 40 FCC Rcd at 8022-23, para. 44.

[244] *See, e.g.*, CLA Comments at 6 (arguing that geographic limitations are not necessary, as technology will provide adequate safeguards); J3 Tech Comments at 8; South Carolina DOC Comments at 3-4 (arguing against restrictions that can be nebulous or may not apply equally across different jurisdictions or locales); Vortezon Comments at 5-6; Trace-Tek Comments at 5 (contending that geographical restrictions are unnecessary with strict and enforceable technical requirements).

technical and testing requirements, are designed to provide safeguards against harmful interference to authorized communications, and therefore limiting jamming deployments to certain geographic areas is unnecessary.[245] Indeed, the use of contraband wireless devices in correctional facilities is a nationwide problem, and limiting deployment by geography would deny some facilities access to needed technological alternatives, even where the threats faced are the same or worse. An incremental approach would simply "unnecessarily prolong the public-safety threat" that we seek to overcome.[246] Moreover, we agree that additional eligibility restrictions "can be nebulous" and unclear, which weighs against their adoption.[247] We caution, however, that our adoption of a jamming overlay construct without geographic restrictions on deployments does not imply that such a solution is feasible in all locales, given the variety of technical and financial challenges DOCs face.

83. *Overlay Licensing Bands*. In the *Third FNPRM*, the Commission sought comment on whether to limit the authorization of jamming solutions by overlay licensing to bands wireless providers use to provide commercial services.[248] The Commission specifically sought to ensure that "our approach to authorizing . . . 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."[249] The Commission sought comment on whether additional bands beyond the recognized included services should be part of our proposed framework.[250]

84. We find that, at this time, it is in the public interest to limit the authorization of jamming solutions to bands that have been incorporated into 3rd Generation Partnership Project (3GPP) band plans for operation in the United States and that are currently deployed, or could be deployed in the near term, by wireless providers to provide commercial service to end users. Although the bands on which we permit overlay licensing for jamming solutions are a subset of bands on the included services list applicable to lease arrangements,[251] we find it in the public interest also to include Band 14 as a band available for overlay licensing of jamming solutions. Band 14 is primarily reserved for FirstNet public safety users, such as first responders and the extended public safety community, but AT&T commercial users can access Band 14 when capacity is required and when public safety traffic does not require priority access.[252] As such, it represents an exploitable spectrum hole for jamming solutions. In discussing the feasibility of protecting public safety users from the impact of jamming solutions, Verizon highlights AT&T's commercial use of Band 14.[253]

---

[245] *See, e.g.*, CLA Comments at 6; Trace-Tek Comments at 5.

[246] CLA Comments at 6.

[247] South Carolina DOC Comments at 3.

[248] *Third FNPRM*, 40 FCC Rcd at 8038, para. 80.

[249] *Id*. at 8021, para. 39.

[250] *Id.*

[251] *See infra* note 261.

[252] *See Public Safety Spectrum Alliance and Pub. Safety Broadband Tech. Ass'n v. FCC*, 184 F.4th 640, 646 (D.C. Cir. 2026) (addressing FirstNet use of spectrum other than Band 14, but finding that the "contract authorizes AT&T to use FirstNet's spectrum in the 700 MHz band for AT&T's own commercial purposes, but only on a secondary, interruptible basis. That means AT&T's use of this spectrum may not interfere with primary public-safety operations, and AT&T's communications are not protected from any interference by those operations. *See* 47 C.F.R. § 90.7").

[253] Verizon Comments at 17, n.46 (indicating that "the concept of exempting FirstNet spectrum from the impact of jamming solutions would be next to impossible as those frequencies are in close proximity to other commercial bands, and in any event, all but a fraction of the capacity of FirstNet's assigned spectrum is used for commercial users").

85. In its application for license renewal, FirstNet stated that in operating its network it applied a definition of "public safety" users consistent with the Spectrum Act, under which first responders receive a higher priority level than other agencies that do not provide emergency response, but that support public safety in other ways.[254] Importantly, FirstNet also noted that the Spectrum Act authorizes it to offer service to non-public safety as well as public safety users, so long as public safety receives priority.[255] In renewing FirstNet's license in May 2023, the Commission's Public Safety and Homeland Security Bureau found that FirstNet's definition of "public safety" users, and its tiered priority service approach to public safety users, to be consistent with the Spectrum Act.[256] Also, in a separate proceeding, the Commission confirmed that "[u]nder the public-private arrangement established by the governing statute, Band 14 spectrum is used on a primary basis for public safety and FirstNet's commercial partner(s) can use excess capacity (i.e., capacity not being used by the public safety users)."[257] In this regard, we understand that 3GPP band preference profiles and the SIM card's Public Land Mobile Network (PLMN) permit commercial users to access Band 14, but only when public safety traffic does not require capacity.[258]

86. As a result of the prioritization and preemption that occurs on Band 14 under the partnership between FirstNet and AT&T, inmates that obtain AT&T handsets could be able to access Band 14 on a secondary basis and inmates could access Band 14 if they obtain devices with FirstNet subscriptions that have priority access to that band.[259] We observe that where a jamming solution blocks all other commercial bands deployed to provide service to end user inmates in a correctional facility, AT&T customer contraband wireless devices will seek access to any remaining available channel in the area, including Band 14.[260] To close this spectrum loophole, we find that including Band 14 in our jamming solution framework is necessary in the public interest. Consistent with our approach that makes jamming solutions available in correctional facilities, but does not mandate their deployment, we clarify that a Commission overlay license authorizing the jamming of Band 14 will be subject to the condition

[254] Reply of the First Responder Network Authority to "Opposition Comments" Regarding its Application for Renewal of Station WQQE234, ULS No. 0010176495 at 4-5 (filed Oct. 11, 2022).

[255] *Id*.

[256] *See FirstNet Renewal Order*, 38 FCC Rcd 4989, 5000, para. 29.

[257] *See Single Network Future: Supplemental Coverage from Space, Space Innovation*, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 2622, 2667, para. 108, n.311 (2024) (*SCS R&O*), citing 47 U.S.C. § 1428(a)(2)(B)(i)-(ii). In this proceeding, FirstNet clarified the status of non-commercial user access to Band 14 by indicating that, "[t]o meet its statutory mandate, the FirstNet program provides prioritized primary access to public safety users—with access to Band 14 for AT&T's non-public safety use on a secondary basis only, pursuant to contract—so that first responders and other public safety entities have access to and use of the FirstNet network when and where they need it without competing with commercial users." FirstNet Comments at 3-4.

[258] *See* Jeff Bratcher, Chief Technology and Operations Officer, FirstNet Authority, *Experience FirstNet: How priority and preemption help public safety connect when they need it most* (2020), https://firstnet.gov/newsroom/blog/experience-firstnet-how-priority-and-preemption-help-public-safety-connect-when-they; Government Accountability Office, *Public-Safety Broadband Network: Network Deployment Is Processing, but FirstNet Could Strengthen Its Oversight* at 6 (2020), https://www.gao.gov/assets/gao-20-346.pdf; Congressional Research Service, *First Responder Network (FirstNet) Authority: Reauthorization and Selected Issues* at 4 (2026), https://www.congress.gov/crs_external_products/R/PDF/R48923/R48923.4.pdf.

[259] Because Cricket Wireless is a wholly owned subsidiary of AT&T that exclusively uses AT&T's network infrastructure, Cricket's compatible devices can also access Band 14 when capacity is available.

[260] *See* AT&T, *FirstNet, Built with AT&T is Connecting More First Responders Across the District of Columbia* (2023), https://www.attconnects.com/stories/firstnet-built-with-att-is-connecting-more-first-responders-across-the-district-of-columbia/; James Careless, All Things FirstNet, *Understanding FirstNet Coverage Areas for Public Safety Agencies* (2026), https://allthingsfirstnet.com/understanding-firstnet-coverage-areas-for-public-safety-agencies/.

that Band 14 may not be jammed if FirstNet otherwise prevents access to Band 14 in the jamming containment area. This condition affords FirstNet and AT&T the option to work with DOCs in the first instance to leverage technical solutions if desired and where feasible, thereby precluding jamming of Band 14 at a given correctional facility. We anticipate that authorizing the jamming of Band 14 in jamming containment areas will not pose a significant public safety risk in those areas because, as discussed below in the context of 911, the record reflects that correctional facility staff typically do not use personal wireless devices for emergencies, and instead use internal radio systems or landlines for emergency calls that would not be blocked by a jamming solution.[261] Further, we note that a DOC has the option to require, by contract, a solutions provider to cease operation of a jamming solution where first responders communicating on Band 14 are afforded access to a jamming containment area during an emergency.

87. Accordingly, we permit overlay jamming solutions in spectrum bands identified in certain relevant subsections of 1.9005 of the Commission's rules,[262] as well as the 758-769 MHz and 788-799 MHz bands. We recognize, however, that not all subsections in section 1.9005 reference services that, although eligible for leasing as exclusively licensed, are used in commercial wireless deployments for which DOCs seek jamming solutions. Specifically, we permit jamming solutions in the following frequency bands: 617-652 MHz, 716-728 MHz, 728-746 MHz, 746-757 MHz, 757-758 MHz, 758-769 MHz,[263] 788-799 MHz,[264] 862-869 MHz,[265] 869-894 MHz, 935-940 MHz, 1390-1392 MHz, 1392-1395 MHz, 1432-1435 MHz, 1670-1675 MHz, 1695-1710 MHz, 1930-1990 MHz, 1995-2000 MHz, 2110-2180 MHz, 2180-2200 MHz, 2305-2315 MHz, 2315-2320 MHz, 2345-2350 MHz, 2350-2360 MHz, 2496-2690 MHz, 3450-3550 MHz, 3550-3700 MHz,[266] 3700-4140 MHz,[267] and the frequency bands listed in Commission rule section 30.4 in the Upper Microwave Flexible Use Service.[268] We recognize that a list of bands available for jamming solutions to combat contraband wireless device use in correctional facilities must not remain static given the prospect of technological advances and the industry's clear future need for additional spectrum. We therefore find good cause to delegate authority to WTB to propose and seek comment on, through Public Notice or other means as necessary, the addition of bands eligible for jamming solutions, provided such bands have been incorporated into the

[261] *See infra* para. 100; CLA Comments at 7; SC DOC *Ex Parte* Letter at 4.

[262] 47 CFR § 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 . . .").

[263] The 758-769 MHz and 788-799 MHz segments of the 700 MHz band, known as "Band 14," are licensed to FirstNet and primarily reserved for FirstNet public safety users, such as first responders and the extended public safety community. However, some commercial users can access Band 14 when capacity is required and when public safety traffic does not require priority access. *See supra* paras. 84-86.

[264] *Id*.

[265] Jamming solution operation is permitted only in the portion of the 800 MHz band where high density cellular systems may be deployed. Commercial cellular mobile radio operations in the 800 MHz band are prohibited below this band segment. *See* 47 CFR § 90.614(a)-(b).

[266] We note that jamming solutions are permitted in the 3650-3700 MHz portion of CBRS shared spectrum available to General Authorized Access Users pursuant to Commission rule section 96.11(a)(1), for which leasing is not permitted. *See* 47 CFR § 96.11(a)(1).

[267] This frequency range reflects the Commission's recent action addressing issues in the upper C-Band. *See Upper C-Band (3.98-4.2 GHz)*, Report and Order, Order of Proposed Modification, and Order on Reconsideration, XX FCC Rcd XX (2026) (*Upper C-Band R&O*). Consistent with the *Upper C-Band R&O*, we will condition requests that seek authority to operate jamming solutions in the Upper C-Band on operating in the top 75 Economic Areas (EAs) after December 31, 2030, and in all other EAs after July 1, 2031.

[268] 47 CFR § 30.4. These bands correspond to services listed in section 1.9005 of the Commission's rules. *See* 47 CFR § 1.9005(d), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (v), (kk), (ll), (mm), (nn), and (pp).

3GPP standard and are to be included in wireless handsets provisioned for commercial service by licensed wireless providers.

88. To further address the closing of spectrum gaps that could be exploited by inmates in correctional facilities, some commenters support expanding our deauthorization framework and authorizing jamming solutions outside of the traditional commercial wireless bands.[269] We find it in the public interest, at this time, to obtain further information on issues related to jamming spectrum used by Wi-Fi and satellite providers through the accompanying *Fourth FNPRM*, including the scope of the problem, specific interference considerations in these bands, and appropriate authorization vehicles. Specifically, we consider the extent to which unlicensed devices operating under part 15 and licensed devices operating under part 100[270] are used as contraband, and seek further input on issues associated with permitting jamming solutions on spectrum bands that support those operations.

89. *License Area*. In our overlay licensing framework, we are guided by the need to protect authorized communications from harmful interference caused by jamming solution deployments. The Commission has made clear that jamming solutions in correctional facilities must be carefully installed, managed through network engineering, and updated, given the potential for harmful interference to proximate authorized users.[271] The Commission therefore sought comment on confining the overlay license area to the geographic area affected by the deauthorization rule, such that the licensed jamming operations would comply with section 333 of the Act.[272] Using this model, the overlay license applicant could seek authority to transmit in the entire area within the perimeter of a facility or a defined smaller area(s) within the perimeter of the facility, depending on the applicable law or correctional facility policy regarding wireless device use, and the applicant's (if not a DOC) contractual arrangement with the particular DOC.[273]

90. After reviewing the record, we find that the public interest is best served by authorizing jamming solutions, in an overlay context, for a license area not to exceed those areas of a correctional facility within which contraband wireless device use violates federal, state, or local law, or correctional facility rule, regulation, or policy which, as noted, we define as the "jamming containment area."[274] This approach is consistent with section 333 of the Act and the deauthorization rule we adopt today. To be clear, a DOC/solutions provider can apply for a license that includes the entire correctional facility bounded by the facility perimeter, provided that wireless devices are not permitted within that area under any circumstances. If wireless devices are permitted in certain areas of the correctional facility, a

[269] *See, e.g.*, South Carolina DOC Comments at 4 (supporting the ability to jam Wi-Fi and Bluetooth spectrum bands as necessary, and stating that "tethering" to a device with a cellular connection has been observed); Dedrone Comments at 7 (overlay licenses in unlicensed spectrum should be available to jamming solutions); CLA Comments at 3 (claiming that contraband communications increasingly exploit Wi-Fi hot spots, satellite links, and other emerging technologies); J3 Tech Comments at 7-8, 14 (jamming solutions should be allowed in other bands such as part 15 Wi-Fi and part 25 satellite).

[270] On July 23, 2026, the Commission released a Report and Order and Further Notice of Proposed Rulemaking that replaces part 25 of the Commission's rules with a new part 100 to, *inter alia*, streamline and simplify the satellite application process and operating standards, including a part 100 licensing "assembly line" to expedite and provide flexibility for space companies. *See Space Modernization for the 21st Century*, Report and Order and Further Notice of Proposed Rulemaking, SB Docket No. 25-306, FCC 26-47 (rel. July 23, 2026) (*Space Modernization R&O*). For purposes of this *Third R&O and Fourth FNPRM*, when discussing the use of satellite spectrum for jamming operations, we refer where applicable to either part 25 (in effect at the time of the Commission's *Third FNPRM*) or part 100 (adopted; effective date forthcoming).

[271] *Third FNPRM*, 40 FCC Rcd at 8038, para. 81.

[272] *Id*. at 8038, para. 82.

[273] *Id.*

[274] *See* Appx. A, section 90.1401 (to be codified at 47 CFR § 90.1401).

DOC/solutions provider cannot seek a license for a jamming solution containing those areas and must apply for a smaller area therein, where all such devices are deauthorized under our adopted rule.[275] The applicant will be required to provide sufficient technical information in its application for an overlay license to demonstrate that the jamming solution will not cause harmful interference to authorized users outside of the jamming containment area.[276] We anticipate that some correctional facility locations and environments will only be conducive to deployment of an indoor jamming solution.[277] Indeed, the MITRE Report concludes that the indoor jamming devices deployed in the South Carolina test produced "near-negligible" interference levels on nearby cellular base stations.[278] SC DOC similarly states that, with indoor deployment, participating wireless providers reported no measurable impact on network performance outside the targeted jamming area.[279]

91. To increase flexibility in system design, and because of the required technical showings and mandatory POC and pre-operational tests that collectively act to demonstrate that a jamming solution will be contained within the license area, we decline to adopt a restriction that limits the deployment of jamming devices to indoor locations.[280] As reflected in the VT-ARC Report, we acknowledge that DOCs/solutions providers face increased challenges in deploying jamming solutions in outdoor environments.[281] SC DOC, in its assessment of the VT-ARC test, notes that outdoor jamming deployments will require "site-specific RF planning, multiple units with overlapping coverage, and directional antennas oriented toward the target area."[282] The MITRE Report also discusses the challenges of outdoor jamming, the importance of the configuration of the jamming devices, and the need to perform site-specific testing.[283] We emphasize that those DOCs opting to deploy jammers outdoors must meet our technical requirements focused on ensuring that the jamming solution is engineered and deployed so as not to cause harmful interference to authorized devices outside of the jamming containment area, including public safety operations. Further, given the Commission's oversight responsibilities, we reject as not in the public interest suggestions that we should adopt a "light-licensing" approach where we would issue blanket, nationwide overlay licenses,[284] or adopt other more expansive licensing approaches to authorizing jamming solutions.

---

[275] Although a successful applicant will be granted an overlay license for an area no larger than the jamming containment area, the actual area to be jammed will likely be an area that is within, and therefore smaller than, the jamming containment area. This takes into account RF propagation characteristics; that is, jamming signals must sufficiently fade as they approach the perimeter of the jamming containment area so that their impact is adequately limited to that area, which is the license boundary for a jamming solution.

[276] *Id*.

[277] *See* CLA *Ex Parte* Letter at 2 (urging the adoption of indoor jamming).

[278] *See* MITRE Report at iii. *See also id*. at 4-2 (noting that the data suggest that an indoor-only jamming deployment would likely have minimal effect on uplink performance for the bands observed).

[279] *See* SC DOC *Ex Parte* Letter at 4.

[280] *See, e.g.*, Verizon Comments at 14 (proposing that the Commission restrict a jamming system to transmitters placed indoors on the correctional facility grounds); J3 Tech *Ex Parte* Letter at 6 (reiterating that the Commission should allow only indoor jamming deployments).

[281] *See* VT-ARC Report at 129 (concluding that outdoor testing demonstrated that jammer effectiveness is heavily influenced by the surrounding RF environment and nearby commercial cellular infrastructure, highlighting the challenges associated with controlling RF in open environments, and therefore recommending deployment of directional antennas for outdoor controlled jamming, optimized antenna placement, and improved antenna design).

[282] *See* SC DOC *Ex Parte* Letter at 3.

[283] *See* MITRE Report at 4-1.

[284] *See* Trace-Tek Comments at 12.

92. *License Term/Renewal*. In the *Third FNPRM*, the Commission sought comment on the appropriate overlay license term, noting that commercial wireless provider licensees benefit from a 10-year license term through administrative certainty that facilitates planning, and that the Commission historically has established a 10-year term for WRS licensees.[285] The Commission asked whether it should adopt a shorter license term for overlay licenses or mandate that the term be the same as the jamming solution provider's contract with the DOC.[286] AFTRCC argues that jamming solution operators should be required to renew their authority every three to five years to ensure compliance with applicable technical standards and any required coordination conditions.[287] Although a shorter license term may be appropriate in some circumstances, we believe that our core technical parameters and testing requirements in our jamming solution authorization framework will serve as strong safeguards against harmful interference from jamming solutions and, therefore, more frequent renewal periods are unnecessary and potentially burdensome on stakeholders.

93. In the interest of providing administrative and regulatory flexibility, we adopt a 10-year license term for overlay licenses for jamming solutions, consistent with our standard approach to WRS license terms.[288] Although we do not link the overlay license term to the length of the underlying contract between a jamming solutions provider and a DOC, we remind applicants that they must maintain their eligibility to hold an overlay license, which is limited 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 such a DOC. As such, we find it in the public interest for an overlay license of a solutions provider to automatically terminate if the relevant contract with a DOC expires or is terminated.[289] Relatedly, we clarify that if the underlying wireless provider's license terminates, such that RF transmissions cease, the overlay licensee operating a jamming solution on that particular spectrum must cease operations.[290] Similarly, if FirstNet's license terminates because it expires or is no longer authorized by Congress, or if FirstNet's contract with AT&T terminates, the overlay licensee operating a jamming solution on Band 14 must cease operations, consistent with the required system RF monitoring technical feature.[291]

---

[285] *Third FNPRM*, 40 FCC Rcd at 8039, para. 83; *see, e.g.*, 47 CFR §§ 24.15, 27.13, 30.103.

[286] *Third FNPRM*, 40 FCC Rcd at 8039, para. 83.

[287] Aerospace and Flight Test Radio Coordinating Council, Inc. Comments (AFTRCC Comments) at 4-5 (noting that the renewal process creates the opportunity to make adjustments to accommodate any changes to the RF and/or regulatory requirement in which jamming solutions operate).

[288] The South Carolina DOC suggests that the overlay license term should not be limited to short periods, so that jamming solutions providers and DOCs can have confidence that they will be able to recoup their investment. South Carolina DOC Comments at 5.

[289] We clarify that this does not apply when a DOC elects to become an overlay licensee to implement and operate its own jamming solution.

[290] We anticipate that a wireless provider's cessation of operation resulting from license termination will be immediately identified by the jamming solutions licensee or lessee through the network monitoring requirement we impose on jamming solutions providers. *See infra* paras. 179-181.

[291] The Spectrum Act provides that FirstNet's statutory authority will terminate 15 years after the statutory date of enactment, i.e., on February 22, 2027, and any further extension of that authority requires action by Congress. 47 U.S.C. § 1426(f). In 2023, PSHSB renewed FirstNet's license for ten years from the expiration of FirstNet's initial license, or for the remaining period of authorization from Congress, whichever is sooner. *See Band 14 Renewal Order*. AT&T's contract with FirstNet is for 25 years and is set to expire in 2042. *See* James Careless, All Things FirstNet, *Who Owns FirstNet and Who Controls Network Decisions?* (July 13, 2026), https://allthingsfirstnet.com/who-owns-firstnet-and-who-controls-network-decisions/.

94. In 2017, the Commission amended its rules to provide that WRS licensees would meet a revised renewal standard by making various certifications regarding performance and level of service.[292] The Commission in the *Third FNPRM* sought comment on how to address compliance with its renewal standard at the end of the overlay license term.[293] For overlay licensees in the correctional facility context, the Commission suggested that a possible renewal showing could include a certification that the overlay licensee 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.[294] The Commission reasoned that this type of renewal showing would facilitate efficient spectrum use by ensuring that licensees for jamming solutions continue to use the spectrum productively and in compliance with Commission rules.[295] Although no commenter directly addressed this issue, we find it in the public interest to require such a renewal showing, and therefore a solutions provider overlay licensee seeking renewal must certify that it remains eligible to hold the license, necessitating a continued contractual arrangement with the relevant DOC for jamming solutions, and that it continues to operate consistent with its authorization to operate at the specific correctional facility. A DOC that is licensed to provide jamming solutions directly must certify its continued eligibility regarding its operation of the applicable facility, and also that it continues to operate consistent with its authorization.

95. *Regulatory Status*. In the *Third FNPRM*, the Commission sought comment on applying the Private Mobile Radio Service (PMRS) presumption to overlay licenses issued for the provision of jamming operations.[296] Specifically, the Commission asked whether applying this presumption to eligible entities seeking an overlay license would help align with the jamming services to be provided, which do not meet the Commercial Mobile Radio Service (CMRS) definition.[297] In the leasing context, the Commission explained that a PMRS presumption is most applicable to eligible DOCs/solutions providers seeking to deploy jamming solutions, which are not intended to provide a service that meets the CMRS definition.[298] Commenters responding to this issue generally agree that we should apply the PMRS presumption to entities seeking to provide jamming solutions in correctional facilities.[299] We will apply the PMRS presumption so as to align the licensee's regulatory status with the non-CMRS jamming service to be provided, unless the applicant includes an exhibit to its overlay license application indicating that it is CMRS for regulatory purposes.[300]

---

[292] *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, 8883-4, para. 21 (2017) (*WRS Renewal Reform Second R&O and FNPRM*).

[293] *Third FNPRM*, 40 FCC Rcd at 8039, para. 84.

[294] *Id*.

[295] *Id*.

[296] *Id*. at para. 85.

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

[298] *Third FNPRM*, 40 FCC Rcd at 8029-30, para. 59.

[299] *See, e.g.*, South Carolina DOC Comments at 1-2; CLA Comments at 7.

[300] 47 CFR § 20.3; *see also* 47 U.S.C. § 332. This approach is consistent with the regulatory status treatment of CIS solutions, which also are not services meeting the CMRS definition. *See Third FNPRM*, 40 FCC Rcd at 8029, para. 58 (explaining the Commission's application of the PMRS presumption in the context of CIS leasing).

96. *Secondary Market Transactions*. In the *Third FNPRM*, the Commission sought comment on allowing overlay licensees for jamming solutions to engage in secondary markets transactions only where the licensee is engaging in a transfer of control of the licensee, and not permitting assignment, partitioning, or disaggregation to a third party.[301] We find it in the public interest to permit non-substantial (*pro forma*) assignments and transfers of control of jamming solution licenses, as these common transactions do not raise operational and technical issues related to system security, oversight of operations, and network architecture. Given similar concerns regarding transactions with third parties, we do not permit an overlay licensee to lease its spectrum to another party.[302]

97. *911 Call Transmission Requirements*. Section 9.10 of the Commission's rules describes 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.[303] Section 9.10(a) states that the requirements are only applicable to CMRS providers, except as described in section 9.10(r), which sets out the requirements specifically applicable to CIS providers regulated as PMRS that nonetheless must transmit 911 calls unless the Public Safety Answering Point (PSAP) or relevant emergency authority chooses not to accept the 911 calls from the CIS provider.[304]

98. In the *Third FNPRM*, the Commission reiterated its understanding that a jamming solution blocks wireless device connections to the network in the selected area of operation and is not capable of permitting 911 calls in that area to be transmitted to a PSAP.[305] The Commission then asked whether there were circumstances where it is technically feasible for a licensee that deploys a jamming solution to satisfy the requirements of section 9.10 of the Commission's rules.[306] The Commission also sought comment on not applying the Commission's 911 and E911 rules to overlay licensees regulated as PMRS that are authorized to provide jamming solutions in correctional facilities.[307]

99. Trace-Tek argues that jamming solution providers should be required to abide by the same 911 and E911 requirements as current CIS providers, but fails to explain how a jamming operator, in contrast to a MAS operator, for example, could technically comply with such requirements.[308] Similarly, OmniProphis claims that its "jamming system" can function without interrupting 911 calls, but then describes its technology as a MAS technology that can selectively block calls, not a jamming technology that blocks all calls on particular frequencies in the selected area.[309] The wireless industry opposes the Commission's jamming proposal, in large part due to their concern that 911 communications would be blocked if jamming signals bleed outside of the targeted area.[310] CTIA believes that jamming solutions will interfere with legitimate 911 and other emergency communications because jammers are unable to distinguish between authorized and deauthorized communications, which it argues is a problem both outside and within the correctional facility, including impact to devices used by guards, staff, and

[301] *Third FNPRM*, 40 FCC Rcd at 8040, para. 86.

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

[303] *See id*. § 9.10.

[304] *See id*. § 9.10(a), (r).

[305] *Third FNPRM*, 40 FCC Rcd at 8031, para. 62, 8032, para. 64, 8040, para. 78.

[306] *Id.*

[307] *Id*. at 8040, para. 87.

[308] Trace-Tek Comments at 7.

[309] OmniProphis Corporation Comments (Omniprophis Comments) at 6.

[310] *See, e.g.*, AT&T Reply at 6, note 22 (arguing that commenters saying that the concern about blocking public safety communication is misplaced does not address the consequences of 911 being blocked outside of the perimeter of the correctional facility); CTIA Reply at 3-6 (contending that jamming interference with 911 and other emergency communications is a problem both within the facility and outside the facility).

authorized visitors.[311] Public safety organizations also express concern about the potential impact of jamming on 911 communications.[312] NENA suggests that any jamming system must "include careful engineering" so as not to interfere with 911 calling.[313] APCO supports the adoption of necessary "technical safeguards" and "comprehensive testing (including under real-world conditions), operational safeguards, and careful, measured implementation . . . ."[314]

100. The Commission also sought comment from stakeholders on how emergency calls are addressed today in a correctional facility environment.[315] CLA submits that, for the most part, correctional facility staff do not use personal wireless devices for emergencies, and instead use internal radio systems or landlines for emergency calls that would not be blocked by a jamming system.[316] The South Carolina DOC similarly indicates that correctional staff are not authorized to use personal cell phones inside the facility and use other radios for internal communication and landline phones for external communication, neither of which would be affected by the deployment of a jamming solution.[317]

101. We find that the record includes no evidence that a jamming solution can permit 911 calls from the jammed area to be transmitted to a PSAP, while also preventing deauthorized calls from connecting to the network.[318] Unlike a MAS, a jamming system does not analyze transmissions in the selected area to determine whether or not they are authorized for purposes of accessing the wireless provider's network and cannot be programmed to not interfere with 911 or E911 calls in the jamming containment area. Further, as corrections community stakeholders confirm, the lack of 911 capability from contraband devices, that currently are not permitted within a correctional facility, does not undermine the alternative internal systems available for reporting emergencies in the correctional facility environment, for example, through internal communications systems, landline phones, or other authorized devices.[319] We note that in other restricted environments where cellphones are prohibited in discrete areas, such as courtrooms, hazardous workplaces, schools, and medical facilities, first responders are typically contacted through landline phones or call boxes/panic buttons to respond to emergency situations.[320]

---

[311] CTIA Comments at 3-6, 22-23.

[312] *See, e.g.*, NENA Comments at 1-2 (notes that jamming systems must be carefully engineered so as to not interfere with legitimate public safety traffic in areas surrounding the correctional facilities); APCO Reply at 1-2 (points out the risk to lawful 911 calls from jamming inside facilities as well as outside the facilities).

[313] NENA: The 9-1-1 Association Comments (NENA Comments) at 2.

[314] APCO Reply at 2.

[315] *Third FNPRM*, 40 FCC Rcd at 8031, para. 63.

[316] CLA Comments at 7.

[317] South Carolina DOC Comments at 6; SC DOC *Ex Parte* Letter at 4 (confirming that correctional agencies typically rely on traditional radios and land lines for emergency communications).

[318] In fact, CTIA notes that the VT-ARC Report confirms the expectation that jamming is indiscriminate and blocks all communications in the jamming target area, including 911 emergency communications. *See* CTIA Oct. 1 *Ex Parte* Letter at 5, 8.

[319] *See, e.g.*, CLA Comments at 7; South Carolina DOC Comments at 6.

[320] For example, while the Occupational Safety and Health Administration bans the use of cellphones while operating heavy equipment, workplaces must maintain emergency action plans such as alternative alarms and access to landlines. *See* 29 CFR § 1926.1417(d); U.S. Department of Labor, Evacuation Plans and Procedures eTool, https://www.osha.gov/etools/evacuation-plans-procedures/eap/develop-implement (last visited Oct. 26, 2026). Some schools and courtrooms that ban cellphones have panic buttons used to alert law enforcement and first responders in an emergency. *See, e.g.,* Whitney Downard, School safety top of mind for Pa. House members considering silent alarms, cellphones (Nov. 17, 2025); Williamson Scene, Courthouses add panic buttons, bulletproof judge's benches in security upgrade (Oct. 15, 2019),

(continued….)

102. Given the technical limitations of jamming solutions, we decline to adopt a requirement for overlay licensees of jamming solutions to comply with the Commission's 911 and E911 rules for deauthorized contraband wireless devices located in the overlay license area, which is limited to the jamming containment area as discussed. Regarding concerns on the potential impact of jamming solutions on 911 calls outside the jamming containment area, we believe that our adoption of a carefully considered jamming authorization framework, including requiring real-world pre-operational testing at each specific correctional facility where licenses for such solutions are sought, will help ensure continued access of authorized devices to 911 emergency services. We expect that the overlay license authorization processes for jamming solutions, in particular the initial POC testing requirement, technical parameters, and on-site, pre-operational testing requirements, will limit jamming operations to the authorized jamming containment area within a correctional facility and greatly reduce the risk that jamming operations will impact authorized communications outside of that area. We reiterate that eligible entities seeking authorization for jamming solutions in correctional facilities must ensure that they have the capability to deploy and maintain a system that can be contained to the jamming containment area(s), fully taking into consideration the surrounding and everchanging RF environment, as well as the proximity to commercial and residential areas.

103. In seeking comment on the appropriate technical parameters to minimize the risk of harmful interference from jamming solutions to authorized users, the Commission in the *Third FNPRM* specifically asked whether additional measures are required to protect first responder and priority communications using commercial spectrum, such as FirstNet, Verizon's Frontline, and T-Mobile's T-Priority.[321] Some commenters express concern that jamming solutions will interfere with such first responder communications.[322] These concerns focus on potential interference to public safety communications, both within a correctional facility and beyond its perimeter into an adjoining community. Public safety stakeholders recognize, however, that jamming solutions can be an important tool to combat contraband wireless devices, provided that the Commission adopts appropriate technical safeguards and testing requirements to protect first responders' public safety communications.[323] As stated, we anticipate that the technical parameters and testing requirements will act sufficiently to cabin a jamming solution, including one transmitting on Band 14, to the specified jamming containment area within the boundaries of a correctional facility, and thereby minimize the risk of harmful interference to first responder communications outside the jamming containment area. Moreover, we confirm that a DOC and a jamming solutions provider remain free to contractually agree to the cessation of any and all jamming operations in the licensed jamming containment area(s) when first responders require access to the area in an emergency situation, separate and apart from our mandated interference resolution procedures discussed below.[324]

104. Relatedly, the Commission sought comment on the effect of jamming solutions on the public's ability to receive Wireless Emergency Alerts (WEA).[325] The Commission sought comment on whether the use of jamming solutions would prevent the wireless providers that elect to participate in

(Continued from previous page)
https://www.williamsonscene.com/news/courthouses-add-panic-buttons-bulletproof-judge-s-benches-in-security-upgrade/article_5c05a0f8-d44e-566d-b485-c80c2bd414cf.html.

[321] *Third FNPRM*, 40 FCC Rcd at 8027, para. 53.

[322] *See, e.g.*, AT&T Comments at 9-10 (noting that FirstNet, Frontline, and T-Priority involve first responders and commercial users sharing one or more spectrum bands, with first responders receiving priority access); CTIA Comments at 12.

[323] *See, e.g.*, APCO Reply at 2-4; NENA Comments at 1-2 (advising that the Commission include careful engineering so that public safety traffic will not be blocked).

[324] *See infra* paras. 186-191.

[325] *Third FNPRM*, 40 FCC Rcd at 8027, para. 54.

WEA (Participating CMS Providers) from delivering WEAs in or near facilities employing jamming solutions, and whether this might result in an inability to comply with the Commission's WEA rules, including its geographic accuracy requirements.[326] Our jamming solutions framework only provides authorization for jamming operations within a specified jamming containment area(s) within a correctional facility and, therefore, harmful interference with authorized communications located outside that area, including WEA communications from Participating CMS Providers, is not permitted. For inmates using contraband wireless devices inside a jamming containment area within a correctional facility, the impact of a jamming solution will be the same for WEAs as for 911 and other emergency communications—they will be blocked by the jamming system. Because contraband devices are blocked from connecting to the network, Participating CMS Providers are not expected to deliver WEAs to those deauthorized devices.

105. *Performance Requirements*. In the *Third FNPRM*, the Commission sought comment on not adopting performance requirements on an overlay licensee as unnecessary given the nature of jamming operations.[327] The Commission explained that historically it has established performance requirements to ensure that spectrum does not lie fallow and is intensely and efficiently utilized, and has applied different performance and construction requirements to different spectrum bands based on considerations relevant to those bands and the services provided.[328] We find that jamming operations through an overlay license in satisfaction of a contract with a correctional facility for public safety purposes meets our goal of ensuring spectrum usage.[329] Therefore, we will not impose specific performance requirement applicable to such operations.

106. *Notification to Overlay Licensees of Wireless Provider Technical Changes*. The Commission also sought comment on the applicability to jamming operators of our existing rule requiring advance notice from wireless providers to MAS operators of certain technical changes to wireless providers' networks to assist the operators in maintaining the effectiveness of systems deployed in correctional facilities.[330] Under our leasing rules, a CMRS wireless provider leasing spectrum to MAS operators, including mobile MAS operators, must provide 90 days' advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, while permitting modified notice arrangements through mutual agreement: (1) adding a new frequency band to service offerings; (2) deploying a new air interface technology or changing an existing air interface technology; and/or (3) adding, relocating, or removing a site.[331] Some commenters support applying to wireless

[326] *Id*.

[327] *Id*. at 8040-41, para. 88.

[328] *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).

[329] *Third FNPRM*, 40 FCC Rcd at 8040-41, para. 88. Vortezon also suggests that the threat of danger from use of contraband wireless devices provides adequate incentive to ensure spectrum usage. Vortezon Comments at 18.

[330] *Third FNPRM*, 40 FCC Rcd at 8033, para. 67; *see also* 47 CFR § 20.23(d)(1).

[331] *See Second R&O*, 36 FCC Rcd at 11838-39, para. 74; *see also* 47 CFR § 20.23(d)(1). The Commission also adopted an exception to this requirement for emergencies, and required good faith negotiations for network adjustments not covered by the notice requirement. *See* 47 CFR § 20.23(d)(2), (d)(3).

providers the same notification requirement for jamming solution operators as is currently in place for CIS operators,[332] and no commenter opposes such an approach.

107. When adopting this rule in the MAS context, the Commission balanced its objectives of providing solutions providers sufficient advance notice of significant changes likely to impact the MAS so as to make timely technical adjustments, while not unduly burdening wireless providers.[333] The Commission found that the benefits to MAS operators outweighed the minimal costs imposed on licensees.[334] In the *Third FNPRM*, the Commission anticipated that jamming solutions providers may face "virtually identical network engineering challenges as those presented for deployment of MAS."[335] We agree that there are common RF considerations between MAS and the deployment of jamming solutions in this regard, and therefore adopt a similar 90 days' advance notification rule regarding certain network changes occurring within 15 miles of a correctional facility where a jamming solution has been deployed. We find it in the public interest, given the heightened concern regarding the potential impact of jamming solutions to authorized communications, to require relevant wireless providers to provide 90 days' advance notice to solutions providers of the three types of network changes set forth in the existing rule, and also to provide such notice when the wireless provider makes any change in radiated power levels at a transmitter site within 15 miles of a correctional facility where a jamming solution has been deployed. For purposes of this rule, we define "relevant wireless providers" as any wireless provider holding a license that: (1) authorizes operation on the frequencies on which an overlay licensee seeks to operate a jamming solution; and (2) authorizes service in the geographic area (e.g., census tract, county, Partial Economic Area (PEA), Economic Area (EA), Cellular Market Area (CMA), Regional Economic Area Grouping (REAG)) within which a correctional facility is located where a DOC or solutions provider seeks to deploy a jamming solution. To further reduce the risk of harmful interference, as we introduce jamming solutions for the first time, we do not include exceptions to our notification rule, such as for emergencies or technical changes the parties may seek to negotiate. We expect that this rule, in combination with the network monitoring feature that we adopt herein, will serve to maintain the effectiveness of the jamming solution and guard against the risk of harmful interference outside of the jamming containment area.[336]

108. *Community Notification Requirement*. Finally, with regard to regulatory matters, the Commission sought comment in the *Third FNPRM* on whether we should consider applying other service rules in an overlay licensing framework for jamming solutions.[337] In the leasing context, the Commission sought comment on whether to apply to jamming solutions the rule currently requiring a CIS operator to notify the community in which the correctional facility is located 10 days prior to deploying a CIS.[338] Some commenters support adoption of a community notification rule.[339] Verizon cites the importance of community notification in the jamming context and submits that a jamming system's "impacts are just as relevant—indeed, more acute—" as compared to a CIS.[340] Some commenters, however, disagree and

[332] *See, e.g.*, CLA Comments at 8; J3 Tech Comments at 10; OmniProphis Comments at 8.

[333] *See Second R&O*, 36 FCC Rcd at 11840, para. 68.

[334] *Id*. at 11841, para. 71.

[335] *Third FNPRM*, 40 FCC Rcd at 8033, para. 67.

[336] *See infra* paras. 179-181.

[337] *Third FNPRM*, 40 FCC Rcd at 8046, para. 103.

[338] *Id*. at 8033, para. 66; *see* 47 CFR §§ 1.9020(n), 1.9030(m), 1.9035(o).

[339] *See, e.g.*, Verizon Comments at 16; OmniProphis Comments at 8.

[340] Verizon Comments at 16.

suggest that a community notification requirement for jamming solution operators is unnecessary or not in the public interest.[341]

109. Although the Commission sought comment on a community notification rule for jamming solutions in the leasing context, we find that, regardless of licensing mechanism, there are common considerations regarding RF and the potential impact on the community near a correctional facility. When the Commission adopted the community notification rule for CIS, it found that a flexible and community-tailored notification requirement outweighed the minimal burden of the notification and furthered the public interest consistent with the goal of expediting the deployment of technological solutions to combat the use of contraband wireless devices.[342] The Commission agreed with commenters supporting the rule due to the potential for accidental call blocking and the public safety issues involved.[343] The record does not demonstrate that the existing community notification requirement for CISs has been burdensome or ineffective in assisting DOCs in resolving any issues of system impact on authorized communications in the surrounding community. Therefore, we find it in the public interest to adopt a similar rule for jamming solutions licensees requiring a notification to the community in which the correctional facility is located 10 days prior to deployment that must include a description of what the system is intended to do, the date the system is scheduled to being operating, and the location of the facility. Notification must also be tailored to reach the community immediately adjacent to the facility, including potentially through local television, radio, Internet news sources, or community groups, as appropriate.

b. Application Process and Procedures

110. The overlay license application process to authorize jamming solutions in the narrow context of correctional facilities incorporates strict testing requirements—both POC testing and on-site, pre-operational testing—to ensure that any jamming solution will operate without causing harmful interference beyond the selected jamming containment area. We adopt a process intended to prevent unnecessary delay, and we anticipate that jamming solutions will be authorized expeditiously so that pre-operational testing can commence in the near-term. As explained above, we will not treat a jamming solution as a type of CIS. Overlay licensing is accomplished through a new part 90 subpart, and relies on a process that is distinct from both the existing leasing process for authorization of CIS, and the certification process for CISs seeking to submit qualifying requests to wireless providers to disable contraband devices.[344] We decline to adopt suggestions in the record that a jamming authorization process should mirror the existing CIS certification process.[345] Rather, given the history of stakeholder concerns regarding the potential for jammers to cause harmful interference, we find it appropriate to adopt core jamming rules and both POC and on-site testing requirements applicable to jamming solutions. The following section describes the process by which an applicant can apply for and obtain a non-exclusive overlay license to deploy a jamming solution in a correctional facility, including testing requirements and the required timing of equipment authorization of jamming devices under part 2 of the Commission's rules. We delegate authority to WTB to issue a public notice, if necessary, describing more specific details of the application process and procedures that are not addressed herein.

---

[341] *See, e.g.*, CLA Comments at 7 (arguing that notice could compromise security); J3 Tech Comments at 10 (stating that the rule seems irrelevant); Vortezon Comments at 14 (stating that notice is not in the public interest).

[342] *First R&O*, 32 FCC Rcd at 2364, para. 74.

[343] *Id*.

[344] *See supra* paras. 8-12.

[345] *See, e.g.*, South Carolina DOC Comments at 3 (proposing a certification process for any jamming solution that mirrors the existing CIS process for disabling phones); Trace-Tek Comments at 12-13 (suggesting a light-licensing approach in which a solutions provider would receive an overlay license, execute private agreements with the carriers, and could begin operations after registration); CIS Providers Comments at 6-7 (proposing a jamming license application approach that is linked to the CIS certification process).

111. In the *Third FNPRM*, the Commission proposed a multi-step application process for overlay licensing that generally included the submission of an application with supporting information demonstrating that the applicant is prepared to deploy a jamming solution without causing harmful interference, with on-site testing required prior to the commencement of jamming operations.[346] At that time, the Commission envisioned that it would initially grant licenses conditioned on the performance of on-site testing, and then issue final authority to operate at the particular facility following the completion of successful testing.[347] We adopt a process that differs slightly from our proposal but, importantly, one that still does not permit deployment of jamming operations until successful completion of on-site testing and notification to the Commission. Rather than first granting a conditional license based on a paper showing, followed by on-site testing, and then grant of final authority to deploy, we incorporate the POC testing requirement at the front end of the process. This approach guards against delay at the license grant stage, and prevents DOCs or their contractors from initiating the application process with the intent to later install jamming devices that have not been demonstrably shown to be effective. To summarize, we require, as the first step in the authorization process, a jamming solution provider to successfully conduct a POC test pursuant to a part 5 experimental license,[348] after which the applicant may file an application with WTB confirming the completion of POC testing and including the required technical showings, as described below. After license grant (if warranted), a licensee is required to conduct on-site testing at the facility for which the license was granted, using equipment that has undergone part 2 equipment authorization, and must also notify the Commission of the successful on-site test, prior to commencing operations.

112. *Form 601 Application*. After POC testing, we require an eligible entity seeking an overlay license to operate a jamming solution in a correctional facility to submit an FCC Form 601 in ULS, as proposed.[349] We require that the overlay license application include, in addition to the information currently required by FCC Form 601: (1) proof of concept test results demonstrating that the jamming solution does not cause harmful interference to authorized devices located outside the jamming containment area, and that the test was representative of, and scalable to, the jamming solution to be deployed under the authorization sought; (2) proof that advance notification was given to the relevant wireless providers and FirstNet regarding the proof of concept test, and identification of any such entities that attended the test; (3) the name and address of the correctional facility with which it has a contract where the jamming solution will be deployed; (4) the requested frequency bands of operation; (5) certification that the applicant meets the eligibility requirements and seeks to deploy a jamming solution; and (6) a description of the jamming solution, a shapefile and visual representation of the jamming containment area associated with the proposed operations within which the jamming solution impact will be contained, such that harmful interference will not occur to authorized users located outside of that area, and the methodology as to how the applicant will deploy the jamming solution to not cause harmful interference to authorized devices, including test locations, the complete deployed system configuration, technical parameters, and protection criteria.[350]

---

[346] *Third FNPRM*, 40 FCC Rcd at 8047, para. 104.

[347] *Id*.

[348] *See supra* paras. 69-75. To reiterate, the POC test can be conducted at a correctional facility of the solutions provider's choice, and is not required to be the specific correctional facility for which deployment authority is ultimately sought, and for which a successful pre-operational test at such facility is required.

[349] *Third FNPRM*, 40 FCC Rcd at 8047, para. 105.

[350] *See infra* paras. 160-62. We do not require jamming devices to be used as part of a jamming solution to have equipment authorization at the time an applicant files a WTB licensing application. Rather, equipment authorizations are required, at a minimum, following license grant and *prior* to site-specific testing. *See infra* paras. 196-203 for a description of the equipment authorization process.

113. Although solutions providers may enter into a contractual relationship with a DOC to provide a jamming solution, we find it unnecessary at this time to require such applicants to file a copy of the contract with the Commission to establish eligibility. Rather, we require that a solutions provider applicant to include a certification that it meets the eligibility requirements, i.e., it has a contract with a DOC to provide a jamming solution at the relevant correctional facility. We clarify that an applicant seeking an overlay license for a jamming solution for a specific correctional facility is required to submit the results of a successful POC test with its application for authority to deploy at a correctional facility. Following application grant at that facility, an overlay licensee of a jamming solution that seeks authorization to deploy the same technology and methodology at a separate correctional facility, is permitted to refer to its initial successful POC test results when applying for authorization at another location, and is not required to conduct a second POC test.[351]

114. In its application, an applicant must provide both a description of its interference protection criteria, and the verification method used to confirm the lack of harmful interference to authorized users. Although we do not specify a particular protection methodology in our rules, we anticipate that an applicant will use measurable criteria, where applicable, as one or a combination of the following: a Signal to Interference and Noise Ratio (SINR), carrier-to-interference ratio (C/I), maximum percentage increase in bit error or packet error rates, verification of no harmful interference to calls and data sessions made outside the jamming containment area(s), etc. We find that providing flexibility to applicants in satisfying necessary interference protection criteria will best account for key differences across correctional facility deployments and different propagation/service characteristics over a wide range of frequencies (e.g., wireless provider quality of service, density of proximate wireless users, surrounding RF environment, and geographic features). We also do not mandate a particular methodology to verify compliance with the chosen protection criteria, but instead require applicants to provide a thorough explanation of the selected methodology that they will use at the specific correctional facility. Applicants must include measurement methods, data, test locations, and a visual representation of where the criteria will be met, and how the criteria will ensure protection to all authorized users located outside the jamming containment area, including commercial users and public safety users, whether operating on FirstNet band 14 spectrum or more traditional land mobile radio public safety spectrum (e.g., 800 MHz).

115. We find it in the public interest to consider an overlay license application for jamming solutions as "site-based" for application fee purposes, as proposed, given that the license area is limited to, at maximum, the perimeter of a correctional facility.[352] Following submission, WTB will place the overlay license application on an informational public notice.[353] We recognize that an applicant for an overlay license for a jamming solution may seek to keep certain information in the application confidential, and we affirm that an applicant may request confidential treatment of information contained in its application consistent with section 0.459 of the Commission's rules.[354]

116. With the goal of ensuring that all eligible entities can apply for and obtain, if qualified, a license to deploy a jamming solution in correctional facilities, the Commission in the *Third FNPRM* sought comment on a licensing approach that would allow more than one applicant to provide service at a specific facility, which results in spectrum sharing in the defined geographic area and the absence of

[351] In this case, the applicant may refer to material already on file with the Commission pursuant to section 1.923(b) of the Commission's rules. 47 CFR § 1.923(b).

[352] *Third FNPRM*, 40 FCC Rcd at 8047-48, para. 105; 47 U.S.C. § 158; 47 CFR § 1.1102.

[353] This approach is consistent with section 1.933(d)(9) of the Commission rules, 47 CFR § 1.933(d)(9), which states that any application for authorization in the Private Wireless Services is not required to be placed on Public Notice as accepted for filing prior to grant. As explained above, overlay licensees are presumed to be PMRS for regulatory status purposes, as they do not meet the CMRS definition. *See supra* para. [X].

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

mutual exclusivity.[355] Specifically, the Commission proposed to place applications in a "queue" to be reviewed in the order in which they are filed.[356] The Commission reasoned that this approach would afford a DOC flexibility, including the ability to contract with more than one solutions provider at a specific correctional facility if desired.[357] We agree with CLA that a flexible approach "encourages innovation and competition, enabling DOCs to select the most effective and cost-efficient solutions for their operational environments."[358] We also agree with the South Carolina DOC that this approach would support the reality that there might be "multiple use cases" for deploying jamming and other types of CISs at the same facility.[359] By permitting more than one applicant to serve a given correctional facility, we encourage flexibility and empower DOCs to tailor their approach to contraband wireless device interdiction to specific correctional facility environments.[360] By adopting a non-exclusive overlay licensing framework that does not create mutually exclusive applications, we promote a path forward that avoids delay and encourages a case-by-case approach to the deployment of jamming solutions in a wide variety of types of correctional facilities.

117. *Pre-operational Testing.* In the *Third FNPRM*, the Commission proposed that an overlay licensee would, following the initial grant of an overlay license, be required to perform on-site testing at the correctional facility where it intends to deploy a jamming solution.[361] This test would demonstrate that the system will function as expected and within the boundaries of the licensed jamming containment area, while not causing harmful interference to authorized communications.[362] We adopt our proposed approach and will require testing following license grant, but prior to commencement of operations. The Commission sought comment on wireless provider participation in the pre-operational testing, as well as what information a licensee must provide to the Commission.[363] The Commission noted that, in the context of CIS qualifying requests and disabling, a CIS provider 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.[364] Following the testing, the CIS operator must file a certification with the Commission that the testing is complete and successful.[365] After review of the record, we conclude that adopting similar requirements for the site-specific testing of jamming solutions will serve the public interest by ensuring effective solutions, without being overly prescriptive or causing undue delay.[366]

---

[355] *Third FNPRM*, 40 FCC Rcd at 8036-37, para. 75.

[356] *Id.*

[357] *Id.*

[358] CLA Comments at 8.

[359] South Carolina DOC Comments at 5.

[360] Vortezon also agrees that flexibility for the DOCs is a "highly desired result." Vortezon Comments at 16.

[361] *Third FNPRM*, 40 FCC Rcd at 8048, para. 106.

[362] *Id.*

[363] *Id.* at paras. 106-107.

[364] *Id*. at para. 106; *see* 47 CFR § 20.23(b)(3)(i).

[365] *Third FNPRM*, 40 FCC Rcd at 8048, para. 106; *see* 47 CFR § 20.23(b)(3)(i).

[366] We note that pre-operational testing is required at every correctional facility at which an overlay licensee or lessee has been granted a license to operate a jamming solution prior to commencement of operations, separate and apart from the POC test that is required at the outset at the facility chosen by the solutions provider. We confirm that a pre-operational test is required at the specific correctional facility where a solutions provider seeks to operate, even if the initial POC test was performed at the same correctional facility, as the test parameters under a part 5 experimental license and the granted license parameters could vary significantly.

118. Several commenters support the concept that real-world testing is a key component in any successful path toward the deployment of jamming solutions in specific correctional facilities. For example, Verizon supports the need for robust testing prior to full operation of a jamming system, referencing the existing rules for CIS disabling as a starting point, and notes the need for wireless providers to have a meaningful opportunity to observe the testing.[367] CTIA states that the introduction of jamming solutions would require a process whereby stakeholders obtain "real-world" experience with any proposed approach, and the Commission should mandate testing "to assess real-world consequences."[368] More specifically, CTIA contends that every proposed deployment at a specific correctional facility should be subject to "site-specific testing that is coordinated with affected wireless providers . . . ."[369] iCert points to the CIS certification process, wherein a DCFO may not submit qualifying requests to wireless providers for disabling contraband wireless devices until after on-site testing, as a way to reduce the risk of harmful interference to authorized communications.[370]

119. We require that overlay licensees provide seven days' advance notification of the pre-operational testing at a specific correctional facility to all relevant wireless providers, sufficient to allow them the opportunity to attend. We define "relevant wireless providers" consistent with our approach in the CIS disabling context.[371] The record reflects that wireless carriers seek involvement in the testing process, and we afford the opportunity for the wireless providers to participate, while finding it unnecessary to mandate their participation. In addition, to minimize operational impacts to public safety, we also require that overlay licensees provide seven days' advance notification of the testing to FirstNet, the relevant Statewide Interoperability Coordinator (SWIC) or equivalent representative,[372] and the relevant Public Safety Answering Point (PSAP) or 911 Authority serving the facility,[373] to provide them the opportunity to attend and participate. We define "relevant SWIC" as the SWIC serving the state in which the test facility is located. We define "relevant PSAP or 911 Authority serving the facility" as the jurisdictional entity responsible for handling 911 calls originating from the serving site. This notification must include the anticipated date of commencement of jamming operations, as well as a point of contact capable of deactivating the jamming solution.

120. We also adopt the Commission's proposal that a licensee seeking to operate pursuant to its granted license must perform on-site testing to demonstrate that the jamming system functions as

[367] Verizon Comments at 15.

[368] CTIA Comments at 5.

[369] *Id*. at 28-29 (arguing that wireless providers would be allowed to review test protocols, participate in the testing, and comment on test reports, and that the Commission would ultimately review and approve each deployment after considering public input). *See also* CTIA Oct. 1 *Ex Parte* at 9.

[370] iCert Comments at 9. iCert also suggests that testing be performed in coordination with the wireless carriers. *Id*.

[371] *See* 47 CFR § 20.23(b)(3)(i). This section states that relevant wireless providers include any wireless provider holding a spectrum license that: (A) Authorizes operation on the frequencies on which the CIS seeks to detect contraband use; and (B) Authorizes service in the geographic area (*e.g.,* census tract, county, Partial Economic Area (PEA), Economic Area (EA), Cellular Market Area (CMA), Regional Economic Area Grouping (REAG)) within which the correctional facility is located.

[372] A SWIC is a state official whose duties include overseeing the daily operation of the state's interoperability efforts and coordinating interoperability and communications projects. This individual is the person most likely within that state to be able to identify which public safety agencies serve the facility where a jamming solution is being tested. *See* https://www.cisa.gov/safecom/NCSWIC#swic.

[373] A PSAP is "[a]n answering point that has been designated to receive 911 calls and route them to emergency services personnel." 47 CFR § 9.3. A 911 Authority is a "State, territorial, regional, Tribal, or local governmental entity that operates or has administrative authority over all or any aspect of a communications network for the receipt of 911 traffic at NG911 Delivery Points and for the transmission of such traffic from that point to PSAPs." *Id.* at § 9.28.

described in the overlay license application, and that its RF signal causes harmful interference only to de-authorized contraband wireless devices located within the identified licensed jamming containment area(s), while not causing harmful interference to authorized devices located outside that targeted area, including to public safety communications systems.[374] We agree with stakeholders emphasizing that the performance of a jamming solution is highly dependent on local RF conditions, correctional facility characteristics, and jamming device placement.[375] Therefore, we find that a certification from the licensee is necessary to satisfy the Commission that the system will operate as approved at the specific correctional facility, and we require that a licensee file a notification in ULS certifying that its pre-operational test was successful. Indeed, the record includes support for a certification requirement with regard to this required site-specific, pre-operational testing.[376] We find, however, that prescribing detailed testing parameters or criteria reduces flexibility and is potentially burdensome. We require that the notification include the following: (1) certification that on-site, pre-operational testing at the specific correctional facility was complete and successful when applying the selected protection criteria in accordance with the granted license; (2) proof that all jamming devices used as part of the jamming solution have appropriate equipment authorizations pursuant to part 2 of the Commission's rules, including applicable FCC IDs; and (3) proof of seven days' advance notification to the relevant wireless providers, FirstNet, relevant SWIC or equivalent representative, and relevant PSAP or 911 Authority serving the facility, and identification of any of these entities that participated in the pre-operational testing.[377] To afford licensees flexibility in implementing their business plans and deploying jamming solutions, we do not mandate a timeframe within which the licensee must file this notification following grant of a license to operate at a specific correctional facility, though the notification must be filed in ULS at least one business day prior to the commencement of operations.

121. As discussed, we adopt the Commission's proposal that, following the filing of the notification regarding successful on-site testing, a licensee will be authorized to initiate jamming operations at the specific correctional facility on the next business day.[378] We expect a licensee to continue to operate in accordance with its established interference protection criteria and continue to verify that the authorized jamming solution is not causing harmful interference outside of the license area.[379] To confirm this expectation and ensure the ongoing accuracy and reliability of a jamming solution at a specific facility, thereby reducing the potential of harmful interference to authorized users outside a jamming containment area, including public safety users, we find it appropriate to require the licensee to file an annual certification that the deployed jamming solution is operating as authorized and

[374] *Third FNPRM*, 40 FCC Rcd at 8048, para. 106.

[375] *See* VT-ARC Report at 128 (stating that "[o]ne of the clearest findings from the Broad River pilot was that jammer performance is highly dependent on local RF conditions. Building construction characteristics, serving-cell proximity, network density, frequency-band selection, jammer placement, and jammer-to-signal ratio all influenced outcomes"); J3 Tech *Ex Parte* Letter at 6 (agreeing that jamming solution effectiveness is driven by signal strength, frequency band, building attenuation, and deployment configuration); TalkTelio *Ex Parte* Letter at 6 (explaining the importance of testing the jamming solution setup or cluster of devices at each specific facility location); MITRE Report at 5-4 (concluding that location-specific testing would be needed to precisely determine the impact of a jamming solution installation).

[376] *See, e.g.*, CIS Providers Comments at 7 (noting the need for certification for specific correctional facility deployments); Vortezon Comments at 20 (suggesting that the only information the Commission should require after on-site testing is a certification, as proposed).

[377] These requirements largely mirror the self-certification requirements imposed on CIS solution providers seeking to disable contraband wireless devices following on-site testing. *See* 47 CFR § 20.23(b)(3).

[378] *Third FNPRM*, 40 FCC Rcd at 8048, para. 107.

[379] We note that a jamming device must include a network monitoring feature that requires modification of the signal level or automatic shut-down if there is a significant change in the RF environment that would cause the jamming solution to cause harmful interference beyond the license area. *See infra* paras. 179-181.

not causing harmful interference outside the targeted jamming containment area. Following license grant, we anticipate that a licensee may need to modify its system to account for changes in the RF environment, for example, adjusting power levels, adding shielding, or making antenna placement changes. We clarify that an increase in the size of the jamming containment area is a major modification requiring the filing of a modification application for Commission approval and amend our rules accordingly, and this includes the relocation of a jamming containment area within a correctional facility, for example, moving from one building to another.[380] We note that our current part 1 rules require the filing of a modification application for a major modification where a licensee seeks to add spectrum bands to its authorization.[381]

4. Leasing Arrangements

122. In this *Third R&O*, we present two paths for the authorization of jamming solutions in correctional facilities, with the same core technical and testing requirements applicable to each. We anticipate that non-exclusive overlay licensing, as discussed above, will prove an efficient method for ensuring that jamming solutions are an available tool in the near term for the corrections community. Here, we provide a second, market-based option for authorizing jamming solutions, in the event the parties mutually agree to a spectrum leasing arrangement. In either licensing scenario, we find it appropriate to adopt rules that distinguish jamming solutions from CISs. We also detail how the adopted leasing approach differs from that proposed in the *Third FNPRM*. For example, we decline to impose a good faith negotiation requirement regarding spectrum leasing arrangements.[382]

123. We exclude a jamming solution from our definition of CIS, for both technical and administrative reasons.[383] We amend part 1, subpart X of the Commission's rules governing spectrum leasing arrangements generally to treat jamming solutions as distinct from CIS authorizations, while creating special rules applicable to lease arrangements for jamming solutions. This approach recognizes that CIS is a category of interdiction technologies created and defined by the Commission to effectuate the streamlining of leasing arrangements. We find these distinctions necessary given stakeholder concern regarding the risk of harmful interference associated with jamming solutions if not properly engineered, and our adoption of associated testing requirements that preclude streamlined processing of applications for jamming solutions, including lease arrangements. We therefore apply core jamming technical rules and testing requirements to both the overlay license and leasing contexts. Where applicable and in the public interest, however, we leverage our existing leasing regime for jamming solution lease arrangements.[384]

124. As mentioned above, Verizon offers a proposed "leasing" framework that includes the possibility of the Commission imposing an "involuntary lease" and holding the jamming solutions provider solely liable for the jamming system's effectiveness.[385] In addition to being a departure from our long-standing secondary markets principles, we find that its proposal is overly complex, potentially burdensome, and unlikely to result in timely implementation of jamming solutions. It is clear that certain components of Verizon's eight-step process contradict current secondary markets rules. For example,

---

[380] In contrast, a decrease in the size of the jamming containment area is a minor modification requiring notification to the Commission. *See* 47 CFR § 1.929(k).

[381] *See id*. § 1.929(a)(6) (classifying as major application or amendment requesting to add a frequency or frequency block for which the applicant is not currently authorized, excluding removing a frequency). Under this rule section, the removal of a frequency or frequency block is not considered a major application.

[382] As we afford stakeholders flexibility and do not mandate wireless provider participation through good faith lease negotiations, we need not define good faith negotiations in this context, nor mandate a negotiation time period.

[383] *See supra* paras. 8-12.

[384] *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).

[385] *See supra* paras. 65-66.

step five provides that after the shot clock period for voluntary lease negotiations concludes, the vendor would be eligible to apply for a modification of the license to impose a *de facto* long term lease.[386] Step eight provides a shift in liability, holding the jamming solutions provider solely liable for the jamming system's effectiveness.[387] These steps are inconsistent with our current secondary markets rules and the leasing regime the Commission envisioned when it stated, in the *Third FNPRM*, its goals of reducing regulatory burdens and encouraging stakeholder participation by generally applying existing leasing rules in the jamming context.[388] Step one of the Verizon proposal requires that solutions providers obtain part 2 equipment certification prior to notifying licensees of their intent to pursue lease negotiations and provide complete technical demonstrations at the outset of negotiations, prior to the start of a "shot clock."[389] Steps six and seven include a one-year period of deployment and testing following a conditional lease grant.[390] On the whole, we find that Verizon's approach would interject unnecessary delay in the deployment of jamming solutions and therefore is not in the public interest.

125. We also find that our adopted approach addresses many of Verizon's concerns and that is subsumes within the framework certain components of Verizon's proposed multi-step "leasing" process, albeit not necessarily in the same sequence or time frame. Our process includes a "rigorous equipment authorization process," including important labeling and marketing restrictions, as well as "well-defined technical rules" for jamming devices.[391] Although Verizon proposes that part 2 equipment certification should be required prior to the start of the lease negotiations process, we do not require equipment certification until no later than the mandatory site-based, pre-operational testing at the particular correctional facilities, where jamming solutions will be deployed, thus eliminating up front delay, while continuing to ensure that only authorized equipment is used for a final deployment. Rather than require vendors to provide technical information directly to the wireless providers prior to lease negotiations pursuant to the Verizon proposal, our POC testing requirement, required prior to the filing of a lease application and which provides wireless providers and FirstNet the opportunity to attend, assures the wireless providers that the jamming solution will not interfere with authorized services.[392] Wireless providers will be able to review the jamming system's lease application following POC testing to "make a reasonable, objective assessment of the system's RF impact."[393] In place of Verizon's conditional grant to allow for a period of testing, our process requires site-specific testing prior to commencing operations and following system authorization.[394] Indeed, we take into consideration Verizon's concerns regarding testing, particularly that site-specific testing is critical, that testing under an experimental license is appropriate, provided it is coordinated with the wireless providers, and that wireless providers should

[386] Verizon Reply at 7-8 (describing the process whereby an involuntary lease is imposed).

[387] *Id*. at 9-10 (agreeing with AT&T and CTIA on the need for federal preemption of state law liability for impact on authorized communications and stating that the vendor should bear any applicable liability for the system's effectiveness).

[388] *Third FNPRM*, 40 FCC Rcd at 8019-30, paras. 36, 38.

[389] Verizon Reply at 2-8.

[390] *Id*. at 8.

[391] *See infra* paras. 154-78 (technical parameters), paras. 196-203 (equipment authorization rules); Verizon Reply at 2, 3.

[392] *See supra* paras. 69-75; Verizon Reply at 5-6.

[393] Verizon Reply at 7.

[394] *See infra* paras. 142-43; Verizon Reply at 8-9.

have meaningful opportunity to observe testing.[395] Finally, we agree with Verizon on the need for "stop buzzer" procedures to be available to address credible cases of harmful interference.[396]

126. In the following sections, we describe an authorization path for jamming solutions available to eligible entities by applying for a spectrum lease, with specific rights, responsibilities, and processing timeframes. We believe that solutions providers should have the flexibility to pursue lease arrangements if appropriate on a case-by-case basis. Like the overlay licensing process, we require a POC test at the start of the process and site-specific, pre-operational testing prior to commencing jamming operations, as well as compliance with core technical rules for jamming devices.

a. Regulatory Matters

127. *Type of Leases*. In the *Third FNPRM*, the Commission discussed the different types of leasing permitted under the secondary markets rules.[397] These options further the public interest by 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."[398] 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.[399] Spectrum leasing arrangements[400] under current rules can take two forms: spectrum manager leasing arrangements;[401] or *de facto* transfer leasing arrangements, which can be either long-term (more than one year) or short-term (one year or less).[402] Spectrum manager leasing arrangements generally do not require prior Commission approval; rather, the licensee/lessor must notify the Commission in advance of commencing operations.[403] In contrast, *de facto* transfer spectrum leasing arrangements typically are 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.[404]

---

[395] Verizon Reply at 9, also citing similar comments from CellAntenna, CLA, CTIA, and J3.

[396] *See infra* paras. 186-91; Verizon Reply at 9.

[397] *Third FNPRM*, 40 FCC Rcd at 8020, para. 37; *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*).

[398] *Secondary Markets R&O,* 18 FCC Rcd at 20619, para. 32.

[399] *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).

[400] 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.*

[401] *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).

[402] *Id.* §§ 1.9003, 1.9030(b).

[403] *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).

[404] *Id.* § 1.9030(e).

128. The Commission sought comment on whether jamming solution leases should be subject to its immediate approval procedures, or whether there is reason to exclude leasing arrangements for jamming solutions from immediate processing procedures.[405] As discussed, we are regulating a jamming solution as an interdiction solution that is not a type of CIS, but instead is subject to specialized testing requirements and core technical rules and requirements, and therefore application of all existing leasing rules used for CIS deployments is not appropriate. Because the authorization of jamming requires a stricter regulatory framework from a technical perspective, including POC testing and pre-operational testing at each correctional facility where a lessee desires to deploy a jamming solution, we find that our part 1 rules regarding types of leases available require adjustment in the context of leasing for jamming solutions.

129. We prohibit parties interested in entering into a leasing arrangement for a jamming solution from applying for a spectrum manager lease. Currently, our rules provide that parties seeking to enter into a spectrum manager lease must submit a notification that is processed pursuant to either general notification procedures or immediate processing procedures.[406] In both scenarios, the Commission is not required to approve the notification, and generally the lease may be implemented without waiting for Commission review of the notification.[407] Under the general notification procedures, the licensee must submit the notification at least 21 days in advance of commencing operations, unless the lease is for a term of one year or less, in which case notification must be submitted at least ten days in advance of commencing operations.[408] Under the immediate processing procedures, the lease notification is accepted as reflected in ULS the next business day after submission.[409]

130. We find that the existing processing rules for spectrum manager leasing do not allow for the careful Commission review and testing of a proposed jamming solution at a specific correctional facility that we require for jamming solutions. First, Commission review of the lease application is necessary to address heightened concerns regarding harmful interference potential, including evaluation of the parameters associated with the requested jamming containment area and relevant protection criteria. Current spectrum manager lease processing rules do not require Commission review prior to acceptance. Second, before a lessee can commence jamming operations, both equipment authorization for the jamming devices and successful on-site testing is required—processes that may take some time to complete. The ability to implement a leasing arrangement automatically after a limited period of time under current rules does not allow for the careful testing we require prior to the commencement of jamming operations. Thus, we prohibit spectrum manager leases for jamming solutions, and we amend our part 1 rules accordingly. In any event, as noted based on wireless provider comments in the record, we believe that it is unlikely that parties seeking to deploy a jamming solution pursuant to a leasing arrangement will pursue a spectrum manager lease (rather than a *de facto* transfer lease), given that the

[405] *Third FNPRM*, 40 FCC Rcd at 8028-29, paras. 56-57.

[406] 47 CFR § 1.9020(e).

[407] Under general notification procedures, the notification is accepted if it is sufficiently complete and contains all required information and certifications. *See id*. § 1.9020(e)(1). Under immediate processing procedures, the notification is also accepted if it is sufficiently complete and contains all required information and certifications, and also meets additional qualifications. *See id*. 1.9020(e)(2). The Commission reviews the notifications to ensure that all necessary technical and other information is correctly submitted, and the parties may implement a spectrum leasing arrangement without waiting for Commission 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 Commission acceptance.

[408] *Id.* § 1.9020(e)(1)(ii).

[409] *Id*. § 1.9020(e)(2)(iii).

licensee maintains primary responsibility for ensuring the lessee's compliance with the Act and the Commission's rules and policies.[410]

131. Additionally, for the same reasons, we will not permit *de facto* transfer leasing arrangements to be processed pursuant to immediate approval procedures. Under our current rules, an application for a long-term *de facto* transfer leasing arrangement is processed either pursuant to general approval procedures[411] or immediate approval procedures, if it meets certain criteria.[412] Applications for short-term *de facto* transfer leasing arrangements are processed pursuant to immediate approval procedures.[413] To afford the Commission time to review and evaluate the lease application, we require that *de facto* transfer leasing arrangements, whether short-term or long-term, be processed pursuant to general approval procedures and we modify our rules accordingly.

132. *Eligibility*. We adopt the Commission's proposal that an entity is 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.[414] Under either type of authorization vehicle (overlay license or lease), we limit eligibility to avoid the unwanted proliferation of jamming devices used in contexts beyond the public safety-related use in correctional facilities. We do not limit eligibility, however, to existing CIS provider entities seeking to enter into a leasing arrangements for a jamming solution, and we reiterate that the process for obtaining a lease for a jamming solution is separate from CIS certification and disabling.[415] This approach permits new entrants, including entities seeking to only provide only jamming solutions consistent with our rules, to participate in addressing the problem of contraband wireless device use. We also reject Verizon's suggestion that eligibility be limited to vendors, and not DOCs, as a way to ensure that they comply with Commission policies.[416] Although we seek to contain jamming solutions to the narrow context of correctional facilities, we believe that permitting DOCs or vendors the flexibility to be a lessee is warranted.

133. In the *Third FNPRM*, the Commission proposed that a lease applicant be 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.[417] In our overlay licensing framework, we do not require applicants to certify in their licensing application that all jamming devices used as part of the jamming solution have at that time appropriate equipment authorizations pursuant to part 2 of the Commission's rules. Rather, we require that certification in connection with a licensee's certification that the mandatory on-site, pre-operational testing at a particular facility was complete and successful, prior to the commencement of operations. For

[410] *Id.* § 1.9020(b). *See, e.g.*, Verizon Comments at 11 (suggesting that a *de facto* transfer lease in which the lessee is exclusively responsible for all relevant compliance obligations is the correct starting point for any authorization of jamming solutions); AT&T Comments at 14 n.48.

[411] Under general approval procedures, the Commission affirmatively consents to the application, denies the application, or subjects it to further review following a public notice period. 47 CFR § 1.9030(e)(1).

[412] Under immediate approval procedures, Commission consent is reflected in ULS on the next business day after filing the application. 47 CFR § 1.9030(e)(2).

[413] *Id*. § 1.9035(e).

[414] *Third FNPRM*, 40 FCC Rcd at 8022, para. 42.

[415] *See supra* paras. 10-12.

[416] Verizon Comments at 11-12 (arguing that limiting eligibility to vendors will best ensure compliance with Commission policies and that they are accountable to DOCs about the viability of the jamming solution in the particular facility).

[417] *Third FNPRM*, 40 FCC Rcd at 8022, para. 42.

regulatory consistency in our jamming solution authorization regime, we similarly do not require a certification regarding equipment authorization at the time of the filing of the lease application, but we require that equipment authorization must be obtained for jamming devices used in the pre-operational test, and that certification must be filed as part of the notification of successful pre-operational testing.

134. The Commission also sought comment on whether we should consider, as an eligibility criterion, a geographical component regarding the location of a correctional facility, e.g., limiting authorization to facilities in rural areas.[418] As described above, the record includes objections to this suggestion.[419] We decline to adopt this eligibility restriction for the same reasons as stated in the overlay context.[420] We conclude that the POC testing and on-site, pre-operational testing requirements will guard against harmful interference to authorized communications in any correctional facility environment where lease applicants seek to deploy a jamming solution. We emphasize that some correctional facilities are located in geographic areas that may not be conducive to the deployment of a jamming solution, but we decline to restrict the availability of this important tool from through a gateway eligibility restriction based solely on correctional facility location.

135. *Included Services*. We affirm that certain bands currently set forth in the part 1, subpart X leasing rules as "included services" are the bands eligible for leasing for the purpose of the deployment of jamming solutions.[421] Consistent with our approach to overlay licensing, and to further prevent spectrum loopholes for inmates to exploit, we also permit leasing of Band 14 for the provision of jamming solutions. We discuss the specifics of leasing in this context below, for which certain regulatory adjustments are required given the applicable statutory framework and FirstNet's unique licensing posture. We also note that, consistent with our approach in the overlay context that makes available, but does not mandate the deployment of, jamming solutions in correctional facilities, approval of leasing arrangements for the jamming of Band 14 will be subject to the condition that Band 14 may not be jammed if FirstNet otherwise prevents contraband wireless device access to Band 14 in the jamming containment area. This condition affords FirstNet and AT&T the option to voluntarily avoid the need for jamming by engaging other technological solutions.

136. As explained in the overlay licensing section above, we find that limiting the authorization of jamming solutions to the bands typically used by wireless providers to provide commercial service to subscribers is necessary in the public interest, and is consistent with our deauthorization rule.[422] Verizon argues, in the leasing context, that jamming solutions in its "leasing" proposal should cover spectrum used for all commercial wireless services with coverage in the particular area, at a minimum to include MSS and possibly FSS spectrum, as well as bands that support Wi-Fi connectivity.[423] We are unclear how, under Verizon's leasing proposal, the Commission could authorize Verizon's leasing of spectrum bands for which it has no license, including with respect to devices operating under part 15 of our rules. We seek comment, however, on these and related issues in the accompanying *Fourth FNPRM*.

137. We permit spectrum lease arrangements for jamming solutions in the following frequency bands: 617-652 MHz, 716-728 MHz, 728-746 MHz, 746-757 MHz, 757-758 MHz, 758-769

[418] *Id.* at 8022-23, para. 44.

[419] *See supra* note 244.

[420] *See supra* para. 82.

[421] *Third FNPRM*, 40 FCC Rcd at 8021, para. 39; 47 CFR § 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 . . .").

[422] *Id.*

[423] Verizon Comments at 14-15.

MHz, 788-799 MHz,[424] 862-869 MHz, 869-894 MHz, 935-940 MHz, 1390-1392 MHz, 1392-1395 MHz, 1432-1435 MHz, 1670-1675 MHz, 1695-1710 MHz, 1930-1990 MHz, 1995-2000 MHz, 2110-2180 MHz, 2180-2200 MHz, 2305-2315 MHz, 2315-2320 MHz, 2345-2350 MHz, 2350-2360 MHz, 2496-2690 MHz, 3450-3550 MHz, 3550-3700 MHz,[425] 3700-4140 MHz,[426] and the frequency bands listed in Commission rule section 30.4 in the Upper Microwave Flexible Use Service.[427]

138. *Application Process*. Consistent with overlay licensing, eligible parties must complete a POC test prior to submission of a jamming solution *de facto* transfer lease application.[428] As proposed, after POC testing, parties seeking a lease to operate a jamming solution are required to submit an FCC Form 608 in ULS.[429] We believe that the use of existing Form 608, with attachments, adequately serves the purpose of authorizing leases for relatively complex jamming solutions, and we reject suggestions to use a more minimal, registration-type process.[430] Similar to overlay license applicants, lease applicants must include, in addition to the information currently required by Form 608: (1) proof of concept test results demonstrating that the jamming solution does not cause harmful interference to authorized devices located outside the jamming containment area, and that the test was representative of, and scalable to, the jamming solution to be deployed under the authorization sought; (2) proof that advance notification was given to FirstNet and the relevant wireless providers regarding the proof of concept test, and identification of any such entities that attended the test; (3) the name and address of the correctional facility with which it has a contract where the jamming solution will be deployed; (4) the requested frequency bands of operation; (5) certification that it meets the eligibility requirements and seeks to deploy a jamming solution; and (6) a description of the jamming solution, a shapefile and visual representation of the jamming containment area associated with the proposed operations within which the jamming solution impact will be contained, such that harmful interference will not occur to authorized users located outside of that area, and the methodology as to how the applicant will deploy the jamming solution to not cause harmful interference to authorized devices, including the complete deployed system configuration, technical parameters, test locations, and measurable protection criteria.[431]

139. In the event that a prospective lessee also seeks authority to deploy a jamming solution that includes Band 14, in lieu of directly leasing spectrum from FirstNet, it must demonstrate to the Commission that it has an agreement with FirstNet to operate on Band 14 to deploy a jamming solution at the specified correctional facility. We permit such an approach because, as stated, FirstNet's license and operating structure is unique and not well-suited to a leasing requirement under our current part 1, subpart X rules. This demonstration must be included as an attachment to Form 608 and must accompany the

[424] We discuss at para. 139, *infra*, special requirements to effectuate leasing of the 758-769 MHz and 788-799 MHz bands, currently licensed to FirstNet, for jamming solutions.

[425] *See supra* note 246.

[426] *See supra* note 247.

[427] 47 CFR § 30.4. These bands correspond to certain services listed in section 1.9005 of the Commission's rules. *See* 47 CFR § 1.9005(d), (g), (h), (i), (j), (k), (l), (m), (n), (o), (p), (q), (v), (kk), (ll), (mm), (nn), and (pp).

[428] *See supra* paras. 69-75.

[429] *Third FNPRM*, 40 FCC Rcd at 8022, para. 42. As a reminder, we prohibit lease applicants for jamming solutions from applying for spectrum manager leasing arrangements.

[430] *See, e.g.*, DI Group Comments at 7 (suggesting that rather than use Form 608 for leasing, applicants could complete a basic form).

[431] Similar to overlay licensing, we do not require jamming devices to be used as part of a jamming solution to have part 2 equipment authorizations at the time an applicant files a lease application. Rather, equipment authorizations are required, at a minimum, following lease grant and *prior* to site-specific testing. *See infra* paras. [X-X] for a description of the equipment authorization process.

lead application seeking authority to operate in a correctional facility, in the event that the applicant files more than a single lease application.[432]

140. Further, as with overlay license applications, the leased area, which must be no larger than the jamming containment area, will be based on the applicant's underlying contract with the relevant DOC. We reduce burdens by not requiring the applicant to file that contract with the Commission, but we require the applicant to certify, as part of establishing eligibility, that it has executed a contract with a DOC to provide jamming solutions at the specific correctional facility. With regard to the POC test results, if an applicant has an existing lease to operate a jamming solution in a correctional facility and seeks authority to operate the same solution in a different facility, it may rely on the POC test results previously filed in connection with the original facility application if the test was representative of, and scalable to, the solution to be deployed under the new authorization sought.[433]

141. We confirm that the lease area must be no larger than the geographic area(s) affected by the deauthorization rule, so as to comply with section 333 of the Act; that is, the area within the correctional facility where operation of a contraband wireless device is a violation of federal, state, or local law, or correctional facility rule, regulation, or policy. We require an applicant to include the requisite protection criteria that will be maintained at the licensed jamming containment area boundary, as well as the method of verification used to confirm the lack of harmful interference to authorized users, including public safety users. We anticipate that a prospective lessee applying for authorization of a jamming solution may seek to keep certain information in the application confidential, and we affirm that an applicant may request confidential treatment of information contained in its application consistent with section 0.459 of the Commission's rules.[434]

142. Because applications for *de facto* transfer spectrum lease arrangements for jamming solutions will not be subject to immediate approval procedures under our revised leasing rules, following submission of the application and acceptance for filing, WTB will place the application on an accepted for filing public notice and will review each application individually to ensure that the applicant has satisfied all requirements.[435] Following Commission consent to the lease arrangement, the lessee must follow the same on-site, pre-operational testing procedures as we adopt for overlay licensees to demonstrate that the jamming system will function as expected and within the boundaries of the leased jamming containment area, while not causing harmful interference to authorized communications located beyond that area.[436] We conclude that, whether a jamming solution is authorized through an overlay license or a lease, the same considerations are relevant with regard to the need to ensure that the effects of a jamming solution is restricted to the jamming containment area. We therefore require that lessees provide seven days' advance notice to FirstNet, all relevant wireless providers, the relevant SWIC or equivalent representative, and relevant PSAP or 911 Authority, of the pre-operational testing at the specific correctional facility. As described above for overlay licensing, notification to the public safety entities must include the anticipated date of commencement of jamming operations, as well as a point of contact capable of deactivating the jamming solution.[437]

---

[432] This approach recognizes that lessees of jamming solutions may typically lease from multiple wireless providers licensed on multiple bands serving the geographic area that includes the specified correctional facility.

[433] In this case, the applicant may refer to material already on file with the Commission pursuant to section 1.923(b) of the Commission's rules. 47 CFR § 1.923(b).

[434] *See id*. § 0.459 (detailing procedures to request withholding materials from public inspection).

[435] *See generally id*. § 1.9030(e)(1).

[436] *See supra* paras. 117-21.

[437] *See supra* para. 119.

143. Following site-specific testing, the lessee is required to file a notification in ULS that includes the following: (1) certification that on-site, pre-operational testing at the specific correctional facility was complete and successful when applying the selected protection criteria in accordance with the granted lease; (2) proof that all jamming devices used as part of the jamming solution had appropriate equipment authorizations pursuant to part 2 of the Commission's rules, including applicable FCC IDs; and (3) proof of seven days' advance notification to FirstNet, the relevant wireless providers, the relevant SWIC or equivalent representative, and relevant PSAP or 911 Authority, and identification of any of these entities that participated in the pre-operational testing. To afford lessees flexibility in implementing their business plans and deploying jamming solutions, we do not mandate a timeframe within which the lessee must file this notification following grant of a lease to operate at a specific correctional facility, though the notification must be filed in ULS at least one business day prior to the commencement of operations. Following this submission regarding the on-site testing, the lessee will be authorized to initiate jamming operations at the specific correctional facility on the next business day.[438] We expect a lessee to continue to operate in accordance with its established interference protection criteria and verify that the authorized jamming solution is not causing harmful interference to users outside of the leased jamming containment area.[439] As with overlay licensees of jamming solutions, to confirm our expectation and ensure the ongoing accuracy and reliability of a jamming solution at a specific facility, we find it appropriate to require the lessee to file an annual certification that the deployed jamming solution is operating as authorized and not causing harmful interference outside the targeted jamming containment area.[440] Following lease approval, although we anticipate that a lessee may seek to modify its system to account for changes in the RF environment, e.g., shielding or antenna placement changes, we will not require the filing of a lease modification application unless the size of the jamming containment area increases. A lessee seeking to operate in additional spectrum bands that are licensed to the lessor wireless provider must file a new Form 608 seeking Commission approval.

144. In the *Third FNPRM*, the Commission sought comment on whether to 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 new lease for a jamming solution.[441] The record does not reflect that existing CIS lessees and their lessor wireless providers are likely to seek modification of existing leases to obtain authorization of a newly proposed jamming solution.[442] We conclude that it would not be overly burdensome for a CIS solutions provider seeking to provide jamming solutions through a lease arrangement to file a new lease application with the required information and certifications. This approach also reduces complexity and provides clarity, as a CIS solutions provider might be a party to an existing spectrum manager lease subject to immediate approval procedures, and leasing for jamming solutions is restricted to *de facto* transfer spectrum leasing arrangements subject to our general approval procedures.

145. *Regulatory Status*. Based on the record, we do not believe that DOCs and solutions providers seeking to deploy jamming solutions in the narrow context of correctional facilities will be providing a service that meets the definition of CMRS, and therefore, a jamming solution is presumed to

[438] *Third FNPRM*, 40 FCC Rcd at 8048, para. 107.

[439] We note that a jamming solution must include a network monitoring feature that requires modification of the signal level or automatic shut-down if there is a significant change in the RF environment that would cause the jamming solution to cause harmful interference beyond the leased jamming containment area. *See infra* paras. 179-81.

[440] *See supra* para. 121.

[441] *Third FNPRM*, 40 FCC Rcd at 8027-28, paras. 55-56.

[442] *See, e.g.*, CIS Providers Comments at 6 (arguing that overlay licensing should be the only path available for the authorization of jamming solutions); Tecore Comments at 11 (contending that neither CIS lease modifications nor new leases are required to add jamming authorization).

be a PMRS.[443] Commenters agree that we should apply the PMRS presumption to all spectrum leasing arrangements entered into for the provision of jamming solutions, unless the lessee includes an exhibit to its lease application indicating that it is CMRS for regulatory purposes.[444] This approach aligns the presumed regulatory status for jamming solutions with other existing CIS interdiction solutions that also do not meet the CMRS definition. Accordingly, we presume that a jamming solution lessee is PMRS for regulatory status purposes, unless the lessee indicates in its lease application that it seeks to be treated as CMRS.

146. *911 Call Transmission Requirements*. In this *Third R&O*, we establish that, in the relevant area, jamming solutions block calls on all affected frequencies and are unable to allow 911 calls to be transmitted to a PSAP while preventing other calls from connecting to the network.[445] We have also confirmed that overlay licensees for jamming solutions have no obligation to comply with the Commission's 911 and E911 rules in the overlay license area, not only because they are presumed to be PMRS for regulatory status purposes, but also because we have no evidence in the record that they are technically capable of compliance.[446] In the leasing context, for the same reasons, we confirm that we will not apply the Commission's 911 and E911 rules to DOCs or their contracted solutions providers (presumed to be regulated as PMRS) that have entered into leasing arrangements for the provision of jamming solutions in correctional facilities.[447]

147. With regard to WEAs, as discussed in the overlay licensing context, our jamming solution authorization framework is designed to successfully contain jamming operations within an authorized jamming containment area within a correctional facility so as not to interfere with authorized communications, including WEA communications from Participating CMS Providers.[448] The general public using non-contraband wireless devices are anticipated to continue receiving WEAs. For inmates using contraband wireless devices inside a correctional facility, the impact of a jamming solution will be the same for WEAs as for 911 and other emergency communications: i.e., they will be blocked by the jamming system. That said, as contraband devices are blocked from connecting to the network, Participating CMS Providers would not be expected to be able to deliver WEAs to those devices.

148. *Community Notification*. The Commission's rules currently require that CIS operators notify the surrounding community in which the correctional facility is located 10 days prior to deploying a CIS that prevents communications to or from mobile devices.[449] The Commission sought comment in the *Third FNPRM* on applying the notification requirement to jamming solutions.[450] Verizon notes that a jamming system's impact on the local community is just as relevant and "indeed, more acute" than the impact of a CIS and that the flexible notification requirement is manageable.[451] We adopt above the notification requirement for overlay licensees authorized to deploy a jamming solution in a correctional

[443] *Third FNPRM*, 40 FCC Rcd at 8029-30, paras. 59-60. *See* 47 CFR § 20.3 (defining "commercial mobile radio service"). *See also* 47 CFR § 20.3. (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 . . .").

[444] *See, e.g.*, South Carolina DOC Comments at 1-2; CLA Comments at 7; Vortezon Comments at 12.

[445] *See supra* para. 101.

[446] *See supra* para. 102.

[447] *Third FNPRM*, 40 FCC Rcd at 8032, para. 64.

[448] *See supra* para. 104.

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

[450] *Third FNPRM*, 40 FCC Rcd at 8033, para. 66.

[451] *See* Verizon Comments at 16; Verizon Reply at 9.

facility, and conclude that the same approach is warranted for such solutions authorized through lease arrangements.[452] Therefore, we require notification to the community in which the correctional facility is located 10 days prior to deployment that must include a description of what the system is intended to do, the date the system is scheduled to being operating, and the location of the facility. Notification must be tailored to reach the community immediately adjacent to the facility, including potentially through local television, radio, Internet news sources, or community groups, as appropriate.

149. *Notification to Solutions Providers of Wireless Provider Technical Changes*. In this *Third R&O*, we adopt a rule in the jamming context similar to our existing rule requiring advance notice from wireless providers to MAS operators of certain technical changes to wireless providers' networks to assist the operators in maintaining the effectiveness of systems deployed in correctional facilities.[453] Under our leasing rules, a CMRS wireless provider leasing spectrum to MAS operators, including mobile MAS operators, must provide 90 days' advance notice to MAS operators of the following network changes occurring within 15 miles of the correctional facility, while permitting modified notice arrangements through mutual agreement: (1) adding a new frequency band to service offerings; (2) deploying a new air interface technology or changing an existing air interface technology; and/or (3) adding, relocating, or removing a cell site.[454] As explained above in the overlay licensing context, we expand the notification rule to include required advance notice when a wireless provider changes the radiated power level at a cell site within 15 miles of the correctional facility.[455] In the leasing context, for the same reasons, we conclude that the same approach is warranted for jamming solutions that are authorized at correctional facilities through spectrum lease arrangements.

150. *Length of Lease*. Current spectrum leasing rules provide that the term of a lease may not be longer than the term of the underlying lessor's license, and that the leasing parties may, contingent on the Commission's grant of the license renewal, extend the leasing arrangement into the term of the renewed license authorization.[456] In the *Third FNPRM*, the Commission sought comment on whether to apply these existing leasing rules to leasing arrangements for jamming solutions, or whether to limit the lease term to the length of the contract with the applicable DOC.[457] The record includes support for applying current part 1 lease term requirements.[458] We permit parties to a leasing arrangement for jamming solutions to extend the lease term consistent with the renewed term of the wireless provider's license or FirstNet's license, provided that the lessee solutions provider maintains its eligibility to provide jamming solutions through a contract with a DOC. We seek to maintain the current part 1 lease term rules for jamming solutions where appropriate; however, given our strict eligibility restrictions, and to maintain consistency with the overlay approach, we adopt a rule providing that the lease for a jamming

[452] *See supra* paras. 108-09.

[453] *See supra* paras. 106-07.

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

[455] *See supra* para. 107.

[456] *See* 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.*; 47 CFR §§ 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.

[457] *Third FNPRM*, 40 FCC Rcd at 8034, para. 68.

[458] *See, e.g.*, CLA Comments at 8 (opposing leases of more restricted duration); Vortezon Comments at 14 (recommending application of the same rules as currently exist for length of jamming leases).

solution will automatically terminate if the underlying contract between a solutions provider and a DOC expires or is terminated. Relatedly, we clarify that if the underlying wireless provider's license terminates, such that RF transmissions cease, the lessee operating a jamming solution on that particular spectrum must cease operations.[459] Similarly, if FirstNet's license terminates because it expires or is no longer authorized by Congress, or if FirstNet's contract with AT&T terminates, the lessee operating a jamming solution on Band 14 must cease operations, consistent with the required system RF monitoring technical feature.[460]

151. *Subleasing*. We adopt the Commission's proposal to not allow subleasing under our proposed jamming authorization framework and affirm our belief that subleasing would raise practical and technical issues, in particular with respect to jamming system security, oversight of operations, and increase risk of harmful interference.[461] Commenters agree.[462] Verizon specifically recognizes that the identity of the jamming solutions provider operating under the lease is essential for Commission enforcement and monitoring, considering the risks posed by the misuse of jamming solutions and the need to protect public safety.[463] Accordingly, we prohibit a spectrum lessee DOC or solutions provider under contract to provide jamming solutions at a specific correctional facility from subleasing its spectrum usage rights.[464]

152. *Construction attribution*. Our current leasing rules generally allow a lessor to attribute the construction activities of its lessee to the lessor's performance requirements. For example, 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.[465] Because jamming solutions are deployed to prevent "service" in a limited public safety-related circumstance, however, the Commission proposed 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.[466] As we explain in the overlay licensing context, unlike the typical provision of

[459] *See supra* para. 93.

[460] The Spectrum Act provides that FirstNet's statutory authority will terminate 15 years after the statutory date of enactment, i.e., on February 22, 2027, and any further extension of that authority requires action by Congress. 47 U.S.C. § 1426(f). In 2023, PSHSB renewed FirstNet's license for ten years from the expiration of FirstNet's initial license, or for the remaining period of authorization from Congress, whichever is sooner. *See Band 14 Renewal Order*. *See* James Careless, All Things FirstNet, *Who Owns FirstNet and Who Controls Network Decisions?* (July 13, 2026), https://allthingsfirstnet.com/who-owns-firstnet-and-who-controls-network-decisions/.

[461] *Third FNPRM*, 40 FCC Rcd at 8034, para. 69.

[462] *See, e.g.*, Verizon Comments at 15; J3 Tech Comments at 11; Vortezon Comments at 15.

[463] Verizon Comments at 15.

[464] Current rules permit subleasing for spectrum manager leases (47 CFR § 1.9020(l)) and long-term *de facto* transfer leases (47 CFR § 1.9030(k)). The licensee must submit a notification regarding the spectrum subleasing arrangement in accordance with the applicable notification procedures set forth in these rule sections. *Id.* §§ 1.9020(l), 1.9030(k). Subleasing is not permitted under a short-term *de facto* transfer lease. *Id.* § 1.9035(m)

[465] 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.").

[466] *Third FNPRM*, 40 FCC Rcd at 8034-35, para. 70, note 185. Licensee build-out requirements include, where applicable, the construction and operation one or more specific facilities; coverage of a certain percentage of the population; coverage of a percentage of geographic area, or the provision of "substantial service."

commercial services where performance requirements are necessary to ensure that licensed spectrum does not lie fallow, the deployment of jamming solutions in the discrete public safety context of correctional facilities does not warrant the imposition of construction obligations on the jamming solutions provider.[467] Accordingly, we adopt the Commission's proposal that the jamming solution provider lessee's deployment of a jamming solution may not be attributed to the wireless provider licensee's satisfaction of its performance requirements.

153. *ECIP Holding Period Exception.* In the *Third FNPRM*, the Commission explained that the Enhanced Competition Incentive Program (ECIP) 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.[468] 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.[469] 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.[470] 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.[471] In the Commission's proposed jamming solution authorization framework, it proposed to also apply the exception to the ECIP holding period for lease arrangements involving providers of jamming solutions in correctional facilities because they also promote public safety.[472] Because the public safety goals of CISs are identical to leases for jamming solutions, i.e., to combat contraband wireless devices in correctional facilities, we adopt the proposed exception for lease arrangements involving jamming solutions providers.

5. Technical Parameters

154. In the *Third FNPRM,* the Commission sought detailed comment on the technical requirements that should apply to jamming solutions in correctional facilities, while also protecting authorized licensees, both co-channel and adjacent-band, from harmful interference.[473] Importantly, the Commission noted that there may be areas within a given correctional facility where certain wireless devices are permitted under state law or DOC policy, and sought comment on how solutions providers could deploy an effective jamming solution, while limiting the impact solely to deauthorized contraband wireless devices.[474] The Commission further noted that jammers have been deployed in foreign countries and tested in federal correctional facilities, sought comment on challenges faced and solutions that have been identified in the development of jamming solutions, and also invited the submission of technical studies and analysis on different types of jamming solutions.[475]

155. The Commission sought comment on whether to set limits on radiated power or power spectral density per band, out-of-band-emission (OOBE) limits, field strength limit at a correctional

[467] *See supra* para. 105.

[468] *Third FNPRM,* 40 FCC Rcd at 8035, para. 71; *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) (*ECIP Order*).

[469] *ECIP Order*, 37 FCC Rcd at 8825-26, paras. 1-2.

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

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

[472] *Third FNPRM*, 40 FCC Rcd at 8035, para. 71.

[473] *Id*. at 8041-8042, para. 89.

[474] *Id*. at 8042, para. 90.

[475] *See id*. at 8041, para. 89.

facility boundary, power flux density (PFD) limit measured at a certain point from a transmitter, and/or SINR at the boundary of proposed jamming operation to limit harmful interference.[476] The Commission asked whether technical parameters should vary depending on various factors including, but not limited to, the location of the correctional facility (e.g., rural, suburban, or urban); the size of the correctional facility and the topography of the surrounding area; the materials used in constructing the facility; the proximity of wireless provider networks in the area; the proximity to residential/business areas/highways; and the corresponding strength of RF signals entering the correctional facility.[477] The Commission also sought comment on how to adequately protect public safety communications from potential harmful interference.[478]

156. Regarding interference testing in connection with the overlay license authorization process, the Commission sought comment on whether to require specific testing parameters, results, or certifications, on how signals should be measured, and on what criteria should be used to evaluate such tests.[479] Consistent with its lead proposal to authorize jamming solutions through leasing, the Commission proposed and sought comment on separate technical rules for jamming solutions that would operate under a lease with a wireless provider and those that would operate under a non-exclusive overlay license.[480] Finally, given the heightened concern about the impact of the introduction of jamming solutions, the Commission sought comment on whether a stricter regulatory framework from a technical perspective was needed, as compared to the current maximum levels set out in various Commission rule parts to ensure that authorized communications are not subject to harmful interference, even though lease arrangements are negotiated at arms-length.[481]

157. Commenters agree that jamming solutions should be required to protect authorized devices from harmful interference, and the record reflects a wide range of suggestions regarding how and to what extent this might be achieved. For example, the South Carolina DOC states the Commission should "avoid assigning prescriptive technical parameters around . . . jamming solutions in general, as these could inhibit flexibility and innovation."[482] South Carolina DOC prefers a "functional requirement" that jamming solutions not interfere with legitimate communications outside the facility.[483] StealthRF notes that jamming systems require the same level of planning and approvals as cellular and public safety system providers to be successful and mitigate interference; adding that the process could be as easy as submitting the system plans to CTIA or a carrier.[484] Vortezon, while opposing stringent technical standards, makes several specific technical recommendations to limit interference, including a requirement for periodic field strength testing at multiple points along the property perimeter to verify non-interference with wireless public services.[485] Trace-Tek states that jamming device operators should comply with baseline technical rules applicable to the bands in which they operate, while also supporting

[476] *Id*. at 8026, para. 52.

[477] *Id*. at 8027, para. 53.

[478] *Id*. at para. 53.

[479] *Id*. at 8048, para. 107.

[480] *See id*. at 8025, para. 48, at 8041, para. 89.

[481] *Id*. at 8025, at para. 50.

[482] South Carolina DOC Comments at 5.

[483] *Id*.

[484] StealthRF Comments at 4. StealthRF also states that "[s]tandards need to be deployed that involve signal mapping, walk testing outside a fenceline, and working with the carriers to ensure that their KPIs are unaffected by the system." *Id*. at 5.

[485] Vortezon Comments at 10-12.

strict power-related safeguards to prevent harmful interference.[486] Trace-Tek also contends that the Commission should forego adopting specific or uniform technical parameters at this time, as it may stifle jammer deployment and lead to waiver requests by entities seeking to deploy effective, though non-compliant, systems.[487]

158. Wireless providers urge caution and contend that a pilot testing program is necessary before technical limits can be established.[488] Verizon believes that jamming solutions should comply with band-specific technical rules as a starting point, and that additional safeguards must also be required commensurate with the risk of harmful interference to legitimate users.[489] Verizon also indicates that interference protection rules applicable to licensee spectrum use as a license condition should also apply to lessee spectrum use, including at a minimum: power and HAAT limits for fixed stations, which are a basic responsibility across all commercial wireless spectrum bands.[490] Aviation Spectrum Resources, Inc., CTIA, AT&T, and GPSIA express concern that jammers will interfere with legitimate operations and urge caution and further study through a pilot program before the Commission moves forward and establishes technical limits for jammers.[491] CCA believes that a framework of permitting jamming under technical parameters tied to existing base-station limits is "premature and insufficiently protective of authorized users and public safety."[492] AT&T supports a pilot program of tests and submits that only those jammer solutions that are proven "not to experience 'signal bleed' into adjacent bands or geographic areas should receive any further consideration."[493] Similarly, APCO and CTIA state that a limited pilot trial could produce data regarding the extent to which jamming systems are able to avoid unintended spillover effects on lawful communications and under what circumstances, and that results of the trial would help the Commission develop technical rules specifically tailored to jamming.[494]

159. A review of the record demonstrates that no single type of jamming solution will best meet the needs of the wide variety of correctional facilities that exist across the country. An effective jamming solution must account for a number of factors in both its design and deployment, including the range of correctional facility building materials and configurations affecting signal propagation, the variety of geographic locations, from dense urban to rural environments, and the topography and related physical features of the surrounding area. Accordingly, our rules must allow both flexibility to meet these challenges and space for innovation for a range of jamming solutions using varying methods, from distributed antenna systems, to strategic placement of a series of independent transmitters that might need to penetrate walls, to deployment of body-worn, very low-power jammer transmitters.[495]

---

[486] Trace-Tek Comments at 6.

[487] *Id*. at 7.

[488] *See, e.g*., AT&T Reply at 6; CTIA Reply at 15; Verizon Comments at 10.

[489] Verizon Comments at 10.

[490] *Id*. at 12-13.

[491] *See* Aviation Spectrum Resources, Inc. Reply at 6; CTIA Comments at 3-4; AT&T Comments at 2; GPSIA Comments at 7.

[492] CCA Comments at 6.

[493] AT&T Reply at 7.

[494] CTIA Comments at 27-28; APCO Comments at 2-3.

[495] *See* Jamming attacks in 5G wireless networks – detection and mitigation, Feb 12, 2026 (https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/jamming-attacks-in-5g-wireless-networks), orhttps://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/jamming-attacks-in-5g-wireless-networks); Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey, IEEE Communications Surveys & Tutorials (Volume: 24, Issue: 2, 2Q 2022) (https://ieeexplore.ieee.org/document/9733393).

160. We anticipate that solutions providers, at the request of DOCs, might take a variety of approaches to the deployment of jamming solutions in targeted areas. For example, a high security prison in a rural area with a large distance to public spaces may seek to jam outdoor spaces and virtually all buildings on the premises, whereas other correctional facilities may seek only to jam a limited number of buildings housing inmates. Regardless of the approach, we expect that, as stakeholders recommend, a solutions provider will incorporate detailed RF surveys and network characterization activities before system design and ultimate installation.[496] VT-ARC specifically recommends that jammer-to-signal ratios be considered to improve consistency and predictability of jamming deployments.[497] The MITRE Report also highlights the significance of the jammer-to-signal ratio and observes that no single value determines whether a communication will be blocked by a jamming solution.[498] We do not find it appropriate, however, to require a jamming solutions provider to comply with rigid, "one size fits all" protection criteria, for example at a correctional facility boundary, applicable in *all* environments. Such an approach would not be technologically neutral, would be unnecessarily challenging to implement for certain system architectures, and likely would result in receipt of an abundance of administratively burdensome and time-consuming requests for waiver of Commission rules. In lieu of adopting set protection criteria, we require, as discussed above, a demonstration from the jamming solutions provider with its license application setting forth the criteria (e.g., SINR) it will meet within its proposed jamming containment area to afford requisite protection to authorized users located outside that area.[499] We find that a case-by-case evaluation through the licensing process promotes innovation and allows necessary flexibility to design appropriately targeted jamming solutions.

161. In addition to our case-by-case approach to evaluating applications for jamming solutions that include protection criteria and demonstrate signal containment, we find it in the public interest to establish basic technical parameter limits, and to require jamming solutions to implement certain key features. The rules we adopt include radiated power limits, OOBE limits, restrictions on methods of jamming based on wireless provider technology deployed (e.g., frequency division duplexing (FDD) downlink), RF sensing capability, and a jamming solution locking mechanism. These rules support our goal of preventing harmful interference to authorized users outside of the jamming containment area. We decline, however, to adopt other technical parameters upon which the Commission sought comment, including setting a field strength limit at a correctional facility boundary or a PFD limit measured at a certain point from a transmitter.[500] An established field strength boundary limit typically results in negotiations between commercial wireless licensees having mutual interest in serving users across common license boundaries. Applying this metric in the correctional facility context reduces flexibility and could result in jamming solutions that comply with a rule-based limit at a given boundary, but nonetheless cause harmful interference to authorized users in violation of section 333 of the Act, thus requiring technical adjustment. We also decline to establish a specific SINR at the boundary of proposed jamming operations, recognizing that wireless providers operating near correctional facilities will offer services through differing signal levels, after adjusting for varying architectures and terrain. As stated, however, we require the submission of this information with each application for technical evaluation.[501]

162. We also do not find it in the public interest to adopt, for jamming solutions, specific frequency stability, duty cycle, synchronization requirements, and other limits that apply to CMRS base

[496] *See* VT-ARC Report at 128.

[497] *Id*.

[498] *See* MITRE Report at 4-2 – 4-3 (suggesting that an operator of a jamming solution must be prepared to address significant fluctuations in the local RF environment).

[499] *See supra* para. 114.

[500] *See supra* note 476.

[501] *See supra* para. 114.

stations and devices.[502] These types of technical requirements previously have been applied to ensure that authorized transmitters did not affect other services and assume that the transmitters are deployed as a communication device, whereas jamming equipment is not intended to be operated as such and, depending on the design and the location of deployment, a jamming signal may sweep across an entire service band or generate a wideband signal to disrupt multiple carriers within a service. Similarly, we do not mandate specific design features offered in the comments,[503] although we recognize some might ultimately be necessary to design an effective jamming system (e.g., specific antenna pattern and tilt requirements, antenna height limitations, limits on outdoor placement, signal mapping requirements, contraband detection capabilities, response time and other timing limitations). We recognize the wide array of techniques available in jamming system design, and find that imposing the referenced limitations reduces flexibility and could render jamming solutions less effective.

163. Although we seek to provide flexibility, we must address concerns in the record that jamming solutions, regardless of licensing mechanism, if not subject to strict technical controls and testing, could cause harmful interference to authorized devices.[504] We also seek to provide regulatory certainly for stakeholders, and therefore do not find it appropriate to adopt differing technical rules for jamming solutions based on the licensing mechanism. We therefore adopt a single set of technical limits and safeguards applicable to all jamming solutions, whether authorized through overlay licensing or leasing, located in a new part 90 subpart. Both overlay licensees and lessees authorized to deploy jamming solutions are governed by part 90 technical rules applicable to their operations in correctional facilities. This approach is administratively more efficient, reduces burdens, and achieves regulatory parity where possible. Below we establish and discuss technical parameters for jamming solutions to facilitate deployment and coexistence with authorized wireless devices.

164. *Power Limits*. In the *Third FNPRM,* the Commission sought comment on the appropriate power limits for jamming operations in correctional facilities.[505] The Commission recognized that a jamming solution using higher power levels could increase the risk of harmful interference to authorized devices, particularly if not properly engineered.[506] The Commission sought comment on whether to adopt band-specific power limits, adopt a uniform power limit, or tailor limits based on facility size or geographic location (for example, permitting higher power in rural areas).[507] The Commission also asked whether to apply a power spectral density model, and whether technical parameters should be adjusted depending on the technology wireless providers deploy (e.g., FDD or time division duplexing (TDD) bands).[508]

165. Commenters offer a wide range of views on appropriate power limits and related technical constraints for jamming systems, with solution providers urging flexibility,[509] and other stakeholders urging caution until further study is completed to assess the effectiveness and potential harm from jammers.[510] Although the record does not reflect a consensus on an appropriate power limit, there is

[502] *Third FNPRM*, 40 FCC Rcd at 8046, para. 102.

[503] *See* Vortezon Comments at 11-12; Verizon Comments at 13; StealthRF Comments at 5.

[504] *See supra* paras. 157-58.

[505] *Third FNPRM*, 40 FCC Rcd at 8042, paras. 91-92.

[506] *Id*. at para. 91.

[507] *Id*. at para. 92.

[508] *Id*. at 8043, para. 93.

[509] *See, e.g*., Viapath Reply at 5 (asserting that correctional facilities must have sufficient options for technological solutions, including jamming).

[510] *See, e.g*., CTIA Reply at 15-16 (supporting pilot program trials should the Commission move forward with jamming to inform the specific conditions imposed in authorizing limited jamming).

a common theme that jamming solution providers must engineer each deployment, based on the local RF environment, to use the appropriate power to block contraband wireless devices, while also containing the effects of jamming signals to the targeted area to avoid interference to legitimate operations.[511] Regarding potential specific power limits, J3 Tech recommends that jamming equipment be subject to a maximum Equivalent Isotropic Radiated Power (EIRP) of 1 watt (30 dBm) per band, arguing that no additional artificial limits are needed and that stricter constraints could impede effective operation.[512] Of the power proposals in the record, Verizon prefers J3 Tech's proposed 1 watt EIRP limit.[513] Vortezon opposes stricter technical limits than those already embedded in existing Commission service rules, but nevertheless recommended detailed interference-mitigation practices, including a maximum transmit power of 2 watts EIRP per antenna, antenna down-tilt requirements, and physical shielding to suppress rear and side radiation.[514] Although DI Group does not advocate for a specific power limit, it states that its proposed solution uses a very low power, body-worn jammer that meets the radiated emissions for unintentional radiators in section 15.109(a) of the Commission's rules and only transmits when it first detects a call attempt.[515] StealthRF suggests that jamming signals outside a correctional facility's fenceline should be no stronger than 20 dB below the received signal level from commercial towers, offering this as a practical containment benchmark.[516] Dedrone focuses on jamming-to-signal (J/S) ratios, and explains that an effective jammer typically requires a J/S ratio of about 15 dB, and therefore power levels must be determined by facility-specific propagation conditions, including consideration of the geography where the system is deployed, rather than uniform national caps.[517]

166. After review of the record, we find it in the public interest to adopt power limits for jamming solutions in the form of a maximum power spectral density (PSD) and to adopt discrete radiated power limits for jamming solutions operating in bands above and below 1 GHz, respectively, rather than adopt a power limit for each specific band. This approach reduces burdens, provides regulatory certainty, and avoids unnecessary complexity. We note that the Commission has taken such an approach in other instances to account for varying propagation characteristics, including the fact that signals using lower frequencies are better able to penetrate various materials than signals using higher frequencies.[518] By establishing a radiated power limit for jamming solutions deployed in commercial wireless bands under 1 GHz, and a separate radiated power limit for jamming operations in commercial wireless bands above 1 GHz, we provide flexibility for solutions providers. Our approach also avoids the administrative delay associated with amending our rules to reflect new power limits each time the Commission establishes and makes available for licensing a new band that permits mobile services.

[511] *See, e.g.*, StealthRF Comments at 6; Viapath Reply at 5; Dedrone Comments at 5; NENA Comments at 2.

[512] J3 Tech Comments at 9. StealthRF argues that, rather than setting a power limit, the Commission should allow flexibility as long as protection criteria are met, suggesting that power and other technical limits should be based on the deployment of a system that meets a set protection standard, rather than establishing a set power limit for the underlying specific transmitting equipment. StealthRF Comments at 4.

[513] Verizon Reply at 3.

[514] Vortezon Comments at 11-12.

[515] DI Group Comments at 8.

[516] StealthRF Comments at 4.

[517] *See* Dedrone Comments at 5-6. Dedrone also urges flexibility, stating that "correctional facilities do not have the budget to support military-style advanced jamming systems," and therefore require higher power than the system being jammed. *Id*. at 3-4.

[518] *See, e.g.*, 47 CFR § 2.948(d) (applying different radiated emission measurement methods below and above 1 GHz); *id*. § 95.2579(a)(5) (applying different measurement technique for Medradio operations below and above 1 GHz); *id*. § 90.543(c) (applying different measure bandwidths for OOBE measurements below and above 1 GHz).

167. We recognize that radiated power levels will necessarily vary based upon the ultimate configuration of the deployed jamming solution and the specific conditions at a correctional facility. We also recognize that solutions providers must engineer each jamming deployment to contain RF signals within a targeted area after considering a variety of factors, including: (1) the signal strength of wireless provider base stations and mobiles in these areas; (2) the proximity of the targeted area(s) to locations where authorized mobile operations are permitted and the density of such authorized users; (3) the building design and construction materials of the correctional facility; (4) the terrain surrounding the targeted area(s) of the correctional facility; and (5) the signal characteristics of transmitters deployed in jamming solutions (e.g., waveform matching, sweeping signals or other waveforms).[519] We believe that successful jamming solutions will necessarily be based on a careful network design, including targeted placement of multiple jamming antennas in controlled areas using limited radiated power, and not through deployment of a low number of high powered jammers covering larger areas of a correctional facility, which could result in RF signal leakage and impact to authorized users located beyond the intended authorized jamming containment area. We agree, however, with stakeholders' caution that the design of a jamming solution should consider the aggregate effects of all deployed jamming devices on authorized devices located outside the jamming containment area.[520]

168. To provide manufacturers and solutions providers certainty and to facilitate near-term deployment of jamming solutions, we adopt the following radiated power limits for jamming solutions: jamming operations in frequency bands below 1 GHz are subject to a radiated power limit of 18 dBm/MHz (63.1 mW/MHz) EIRP; and jamming operations in frequency bands above 1 GHz are subject to a radiated power limit of 24 dBm/MHz (251.2 mW/MHz) EIRP. As discussed below, we calculate these PSD limits based on a basic link budget free space propagation calculation intended to facilitate the design of jamming equipment and deployment of jamming solutions in realistic operational scenarios, while also limiting the jamming solution's potential area of impact. Applying these limits will afford solutions providers the flexibility to design effective jamming solutions across varying configurations in environments where strong base station wireless provider signals are present, including deploying a series of antennas that can limit the jamming signal impact to devices within the jamming containment area, as required under our approach. We anticipate, however, that in many correctional facility environments, the actual radiated power required for an effective jamming solution is likely to be substantially less than the Commission-adopted limit, based on the need for a custom engineered system at each specific correctional facility.[521]

169. The adopted PSD limits address the wide variability of mobile signal bandwidths and technologies across multiple bands to accommodate usage of various waveforms in jamming solutions,[522]

---

[519] *See* VT-ARC Report at 128 (recommending that "future jamming designs place increased emphasis on RF containment, power management, signal confinement, and deployment techniques that minimize leakage outside targeted coverage area with continuous operations monitoring and potential independent validation"). *Id*.

[520] *See id*. at 79, 99-102, 123, 126-128; J3 Tech *Ex Parte* Letter at 8 (opining that increasing the number of jamming devices does not necessarily cause a harmful interference problem and agreeing with the need to test the aggregate jamming solution); TalkTelio *Ex Parte* Letter at 5, 6, 8, 15 (emphasizing that TalkTelio's jamming solution uses a "cluster" of devices which must be tested altogether, as installed in a particular configuration at a facility, in order to produce accurate test results and be an effective solution).

[521] We note that the power limits we adopt in Commission rule section 90.1419 (*see* Appx. A) also apply to jamming solutions operating on Band 14, where substantially higher power limits would otherwise apply pursuant to Commission rule section 90.542, 47 CFR § 90.542, as those higher levels are intended to maximize coverage for FirstNet subscribers providing public safety services.

[522] *See* Jamming attacks in 5G wireless networks – detection and mitigation, Feb 12, 2026 (https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/jamming-attacks-in-5g-wireless-networks), or https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/jamming-attacks-in-5g-wireless-networks); Jamming Attacks and Anti-Jamming Strategies in

(continued….)

from basic waveforms that create noise across an entire band to more sophisticated waveforms that may target certain subchannels/time slots with varying duty cycles. Our PSD-based approach also allows jamming solution transmitters to increase power as bandwidth increases, consistent with current rules applicable to commercial wireless systems.[523] We adopt spectral density limits that will accommodate a range of potential jamming solutions, while also allowing for future design innovation. We find that specifying the radiated power limit for a jamming solution on a per megahertz power spectral density basis is consistent with our approach for base station power in commercial mobile services and accounts for a variety of antenna deployments and the wide range of channel bandwidths used in various commercial wireless bands. Some commenters suggest that the Commission adopt power limits on a total power per antenna or per band basis.[524] We decline to unnecessarily limit jamming solutions design options. We believe that the power limits we establish will facilitate effective, custom designed jamming solutions that can be deployed near-term without causing harmful interference to authorized users. We also permit power to be measured using either a peak or average method. Given that jamming signals can be delivered through various signal formats (e.g., wideband noise, rapidly sweeping narrowband signal across a band, or a targeted synchronized advanced signal jamming technique), this flexible approach will allow licensees to use either measurement technique based on the characteristics of a jamming signal. Consistent with the Commission's approach in wireless radio services, we adopt a peak-to-average ratio of 13 dB for average power measurements.[525]

170. *Out of Band Emission Limits*. In the *Third FNPRM*, the Commission explained that various Commission rule parts currently define OOBE limits for different wireless bands,[526] and sought comment on whether those existing limits should apply to overlay jamming operations.[527] The Commission also asked whether stricter or more tailored emission limits were needed to better protect adjacent-band and nearby spectrum users and invited commenters to make specific recommendations.[528]

171. The record reflects no consensus on the appropriate OOBE limits that should be applied to jamming solutions. Some commenters argue for flexibility and believe it is premature to establish set technical limits. For example, Trace-Tek supports the adoption of strict OOBE rules to ensure protection of authorized devices outside a facility, but states that it "may be too early in the implementation and deployment process . . . [to set] uniform technical requirements for jamming operations across a wide range of bands."[529] Trace-Tek argues against implementing specific parameters at this time to avoid stifling deployment of jamming technology and the anticipated surplus of waiver requests by entities trying to deploy effective jamming solutions.[530]

(Continued from previous page)
Wireless Networks: A Comprehensive Survey, IEEE Communications Surveys & Tutorials (Volume: 24, Issue: 2, 2Q 2022) (https://ieeexplore.ieee.org/document/9733393).

[523] *See, e.g.*, 47 CFR §§ 24.232(a)(2), 27.50 (specifying base station powers as PSD for emissions greater than a megahertz to account for variability in the bandwidth used by different technologies).

[524] *See* J3 Tech Comments at 9; Vortezon Comments at 11-12.

[525] *See, e.g.*, 47 CFR §§ 27.50(a)(1)(i)(B), 27.50(d)(5). Questions regarding demonstrating compliance with these requirements may be submitted to OET's Laboratory Division (Lab) Knowledge Database (KDB) inquiry system at https://apps.fcc.gov/oetcf/kdb/forms/InquiryForm.cfm.

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

[527] *Third FNPRM,* 40 FCC Rcd at 8043, para. 94.

[528] *Id*.

[529] Trace-Tek Comments at 6-7.

[530] *Id*. at 7.

172. J3 Tech and StealthRF contend that jamming solution providers should meet the applicable OOBE limit that applies to the band being jammed.[531] Dedrone argues that current OOBE rules for wireless carriers are too stringent for the efficient operation of a wideband jammer that must address multiple frequency bands to jam narrowband handsets that can much more easily meet the OOBE standards.[532] Dedrone proposes a 30 dB roll-off out of the licensed band to limit interference to authorized devices, while also recognizing that wideband systems will necessarily have poorer power roll-off at the edge of functional bands due to the limitations of amplifier, antenna, and filter technology.[533]

173. For a number of reasons, we find it in the public interest to apply to jamming solutions the existing OOBE limits applicable to commercial wireless systems operating in the same bands, and those applicable to FirstNet on Band 14.[534] First, we note that these limits were established through a number of proceedings addressing commercial wireless band deployments that fully considered adjacent channel impacts.[535] Second, the limits have for decades successfully contributed to mitigating harmful interference to adjacent band users, and we are not persuaded that more stringent standards are needed for jamming solutions. Third, under this flexible approach, a solutions provider will be required to suppress its jamming transmitter signal outside of the authorized service bands, but not between individual license blocks within a service, so as to be able to jam multiple service provider bands within the same radio service where necessary at a correctional facility. Further, we permit jamming solutions to operate across contiguous authorized jamming bands that are allotted for different services, without meeting the emission limit for those services at the band edge. We find it unnecessary and inefficient to require signal suppression in filtering at the band edge of a service if the jamming solution is also operating in the immediately adjacent band. As suggested by several commenters, we also require that OOBE compliance, including rules for spurious emissions,[536] first be demonstrated in the equipment authorization process, ensuring that jamming equipment is subject to procedures applicable to base station transmitters used in commercial bands.[537] We note that the VT-ARC Report's observations regarding the micro-jamming test suggest that emissions were not always confined to the authorized frequency ranges and that emission characteristics may vary among individual jamming devices and solution deployment locations and configurations.[538] J3 Tech agrees that a configuration error contributed to the observed OOBE behavior.[539] TalkTelio confirms that a programming error caused these particular emissions, and

[531] StealthRF Comments at 7; J3 Tech Comments at 12.

[532] Dedrone Comments at 4.

[533] *Id*. at 4-5 (includes figure showing proposal).

[534] The OOBE limits applicable to Band 14 operations are set forth in Commission rule section 90.543(e), 47 CFR § 90.543(e).

[535] *See, e.g.*, *Service Rules for the 698-746, 747-762, and 777-792 MHz Bands et al.*, WT Docket No. 06-150 et al., Report and Order, 22 FCC Rcd 8064, 8104-08, paras. 107-119 (2007); *Service Rules for the 698-746, 747-762, and 777-792 MHz Bands et al.*, WT Docket No. 06-150 et al., Second Report and Order, 22 FCC Rcd 15289, 15381, 15386, 15481, paras. 250-251, 262, 360-362 (2007); *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, 4635-38, paras. 61-65 (2014).

[536] *See* 47 CFR §§ 2.1051, 2.1053, 2.1057.

[537] *See, e.g.*, Verizon Comments at 13; J3 Tech Comments at 14.

[538] *See* VT-ARC Report at 82-88.

[539] J3 Tech *Ex Parte* Letter at 7, 9 (claiming that a configuration error by the vendor resulted in emissions beyond the authorized 700 MHz band). J3 Tech also contends that the quality of the equipment and jamming solution design is an important factor in the ability to contain the jamming signal within a targeted area. *See id.* at 6-7.

an adjustment made during the test showed corrective containment.[540] These findings support our requirement that OOBE limits must first be met in the equipment authorization process for jamming solutions, and then during testing and subsequent operation at a specific correctional facility.

174. *Technical Restrictions for FDD and TDD Bands*. In the *Third FNPRM,* the Commission sought comment on whether to adopt technical rules for jamming solutions that distinguish between the potential for harmful interference in bands using FDD, as compared to those using TDD.[541] The Commission asked whether alternative technical parameters should be established to ensure authorized devices are not subject to harmful interference.[542] For example, in the context of TDD operations, the Commission asked whether desired-to-undesired signal ratios should be considered at a provider's base station.[543] The Commission explained that commercial wireless networks can be deployed using FDD, which allows simultaneous uplink and downlink transmissions between a subscriber's device and a base station on separate channels, or TDD, in which a common channel is shared between the uplink and downlink, and its use is switched in time.[544] For networks using TDD—in which the channel is shared—the Commission sought comment on whether specific measures were needed to prevent harmful interference to wireless providers' base stations.[545] For example, the Commission sought comment regarding whether to require synchronization between a jamming solutions provider and a wireless provider serving the area to avoid jamming transmissions when the wireless provider base station is receiving signals.[546] The Commission also asked whether different considerations should apply when jamming solutions are deployed in bands using FDD.[547] Although the Commission raised these concerns as relevant in both a leasing scenario and an overlay licensing scenario, the Commission asked whether, in a leasing scenario, any distinctions could be addressed solely through spectrum leasing arrangements and the underlying contracts between the leasing parties.[548]

175. Dedrone argues that requiring solutions to adhere to the technical parameters of the signal being jammed would severely limit the use of jammers currently in the market because they are not designed to have waveforms compliant with cellular communication standards.[549] Dedrone states that if a jammer can confine its signal through power and propagation, it is unnecessary to require that it also meet strict protocol standards having no bearing on the jamming function.[550] Verizon contends that in any FDD-based spectrum bands, the jamming solution should limit transmissions to the downlink band, as a

[540] *See* TalkTelio *Ex Parte* Letter at 5. *See also* SC DOC *Ex Parte* Letter at 4 (agreeing that a configuration error led to emissions into unauthorized frequency bands and arguing that these findings were a strength of the process, supporting a requirement that compliance with limits must be demonstrated before commencement of operations.)

[541] *Third FNPRM*, 40 FCC Rcd at 8026, para. 51.

[542] *Id.*

[543] *Id*.

[544] *Id*. at para. 51, n.139.

[545] *Id*. at para. 51.

[546] *Id*.

[547] *Id.*

[548] *Id*. at 8043, para. 93; 8026, para. 51.

[549] Dedrone Comments at 4.

[550] Dedrone explains that cell base stations can cooperate with the end user devices to coordinate frequency hopping, modulation schemes, and other parameters of the waveform. *Id.* Dedrone believes that without cooperation from the device being jammed, it is "much more difficult for jammers to follow signal hoppers in time and frequency, and few jammers would be available to meet more advanced protocols required to do so." *Id.*

way to mitigate the risk of harmful interference.[551] StealthRF also supports minimizing uplink interference that may prevent legal phones from communicating.[552]

176. After careful review of the record, we conclude that limiting jamming solution transmissions to the downlink portion of FDD bands, in either an overlay or lease arrangement scenario, is in the public interest and will further minimize the risk that deployment of a jamming solution will impact authorized communications. Accordingly, we prohibit jamming solutions from transmitting on the uplink portion of FDD frequencies where the wireless provider base stations receive signals transmitted from end users. We find that restricting jamming signals to the downlink portion of the band will not materially impact jamming solution designs, as solution providers already must customize their signals in the power and frequency domain to effectively jam wireless provider signals within a targeted area. We believe that this restriction, in conjunction with our other adopted technical safeguards, will minimize the impact on a wireless provider base station's ability to receive signals from authorized devices located outside of the jamming containment area.

177. With regard to the potential impact of jamming solutions on TDD systems, we recognize that protecting wireless provider base stations operating TDD technologies may present more complicated RF scenarios than those using FDD technologies. We agree with stakeholders that TDD deployments warrant particular attention when evaluating the impact of a jamming solution at a specific correctional facility.[553] We do not permit harmful interference from jamming solutions to wireless provider base stations operating TDD technologies, and solutions providers must therefore design their systems accordingly. As with the FDD downlink jamming only restriction, this prohibition applies equally to both overlay and lease arrangement scenarios, and we require overlay license or lease arrangement applicants for a jamming solution to explain in their application how their solution will prevent such harmful interference to wireless provider base stations deployed using TDD. We provide flexibility, however, and although it may be a viable option in many instances, we do not find it appropriate to mandate synchronization with mobile service base stations to avoid transmitting during the uplink time slot. We agree with commenters suggesting that mandating more complicated jamming solution design protocols like synchronization of jamming signals to base station downlinks in TDD bands, or other comparable techniques, may eliminate or limit effective jamming options that could otherwise protect authorized users through alternative methods.[554]

178. As stated, we anticipate that each jamming solution deployment will be engineered for the conditions present at the given correctional facility and will be subject to Commission review and testing, and therefore we decline to adopt overly prescriptive requirements. We afford increased flexibility for solutions providers to custom design a compliant jamming solution. For example, as reflected in its comments, DI Group's proposed solution detects a contraband call attempt and relies on very low power, short duration jamming transmissions from a body-worn device that DI Group states is highly unlikely to impact a wireless provider's nearby base station receiver.[555] Where the effects of jamming signals are sufficiently contained within the targeted area for a wide range of reasons (e.g., jamming signal power control, building construction, surrounding terrain, distance to areas where authorized phones are permitted), there may be no need for more complicated timing or other synchronization methods to protect carrier base stations using TDD technologies. In other cases, for example where a nearby TDD base station provides a very strong signal into the targeted jamming area, it may prove difficult to overcome the base station downlink in the targeted area without leakage of the

[551] Verizon Comments at 14; Verizon Reply at 4.

[552] StealthRF Comments at 4.

[553] *See* VT-ARC Report at 8-9, 117; MITRE Report at 5-4.

[554] *See, e.g.*, Dedrone Comments at 4.

[555] *See* DI Group Comments at 4-5.

jamming signal at the base station receiver.[556] In that situation, it may be necessary for the jamming solution provider to institute other methods, including synchronization, to jam the signal without impacting base station uplink time slots. We will fully evaluate each jamming solution application, including the proposed design, protection methodology and criteria, in an effort to ensure that mobile service base stations are not subject to harmful interference from jamming solution operations. A case-by-case evaluation process is a necessary tool to consider the impact of a wide range of deployment scenarios. Importantly, as discussed below, our adopted framework also affords wireless providers the ability to utilize a "stop-buzzer" type mechanism in credible instances of harmful interference to authorized users.

179. *Network Monitoring Requirement*. To protect authorized communications from harmful interference as a result of the deployment of a jamming solution, the Commission sought comment on whether it should adopt as part of its framework additional licensing or operating rules.[557] In meeting the goal of preventing harmful interference to authorized users, we seek to account for unexpected changes in the RF environment in and surrounding the correctional facility that could result in the unwanted transmission of jamming signals outside of the jamming containment area(s). The Commission envisioned that additional technical requirements might be required as guardrails.[558] Some commenters suggest a requirement that jamming solutions incorporate a mechanism to monitor the status of the mobile phone networks at correctional facilities to be aware of the effectiveness of the jamming solution and to detect possible jamming signal leakage.[559] For example, the VT-ARC Report recommends that the Commission adopt a requirement that a jamming solution deployment be continuously monitored to verify that emissions remain within the approved operating parameters, maximize solution effectiveness, and minimize unintended impacts to lawful users.[560] The MITRE Report suggests that the jamming solution operator should be expected to monitor the RF environment over time and make system adjustments as necessary to account for changes in the cellular environment.[561] TalkTelio suggests the adoption of oversight and monitoring requirements performed on an "annual schedule."[562] Vortezon recommends routine RF power audits and spectrum scans for verification of jamming effectiveness and spillover containment, as well as 24/7 real-time monitoring and automated alerting capabilities.[563] Vortezon also recommends adaptive power control to dynamically adjust the jamming device power based upon occupancy and device density in real time.[564]

180. We find that deploying jamming solutions without causing harmful interference to authorized users requires continuous awareness of the RF environment in and around the relevant correctional facility. Jamming solution providers must maintain such awareness of the RF environment to not only effectively jam contraband wireless devices, but to ensure that their operations do not cause

[556] *See* VT-ARC Report at 8-10, 108-111, 116.

[557] *Third FNPRM*, 40 FCC Rcd at 8046, para. 103.

[558] *Id*. at paras. 102-03.

[559] *See, e.g*., iCERT Comments at 10 (suggesting a real time monitoring to determine the effectiveness of jammers).

[560] *See* VT-ARC Report at 11, 128. We find it unnecessary and overly burdensome to adopt the additional recommendation that we require, where appropriate, independent third-party validation by authorized oversight entities in this regard. *See id.*; TalkTelio *Ex Parte* Letter at 11-12 (disagreeing with the recommendation that we require independent third-party validation). We believe that adopting a network monitoring requirement, coupled with mandatory automatic system modification or shutdown, achieves our public interest goal.

[561] *See* MITRE Report at 4-3.

[562] TalkTelio *Ex Parte* Letter at 12.

[563] Vortezon Comments at 11.

[564] *Id*. at 12.

harmful interference outside of the jamming containment area in the event that there is a material change in the wireless provider's network power levels. Accordingly, we require a jamming solution to: (1) monitor the RF environment for the bands in which jamming operations are active at a correctional facility; (2) detect a material change in the power level (e.g., a significant decrease) of a particular carrier's signals at the correctional facility; and (3) automatically modify the jamming solution architecture, such as by changing the power of the relevant jamming signal, adjusting antennas, or implementing other immediate mitigations sufficient to maintain the protection criteria upon which its application was granted to not cause harmful interference to authorized users, or else immediately cease jamming operations in that band.

181. This requirement ensures that, in the event of an emergency, malfunction, or unplanned network event, the jamming solution will not adversely impact authorized users outside of the licensed jamming containment area(s). We require overlay license or lease arrangement applicants for a jamming solution to explain in their application how their solution will comply with our network monitoring requirement to trigger a system modification or a shutdown upon significant RF signal changes. In the interest of providing flexibility and maintaining technological neutrality, we decline to mandate how a solutions provider must meet this requirement, but we require such functionality, and therefore an applicant must fully explain its approach in its application. On balance, we believe that adopting a network monitoring requirement with mandatory automatic system modification or shutdown is warranted. Although we anticipate that this safeguard will not often need to be employed, we find it in the public interest to impose this requirement as a key protection against unexpected RF events. Further, although the capability of automatic power adjustment, for example, may be more sophisticated than that of automatic shutdown in response to a material wireless provider network event, this option provides a jamming solutions provider the flexibility to continue important jamming operations when facing significant fluctuations in the wireless provider network RF environment.

182. *Locking Mechanism Requirement*. To prevent jamming devices from being misappropriated for unauthorized uses, the Commission sought comment in the *Third FNPRM* on whether it would be in the public interest to require jamming devices to include a locking mechanism feature that, if technically feasible, would prevent unauthorized entities from using the device outside of the correctional facility context.[565] The Commission sought comment on whether, for example, it would be possible to control the activation of the jamming devices by geo-location, such that the device would de-activate when used outside of the correctional facility.[566] In the same vein, the Commission sought comment on whether there are other features or mechanisms that could be imposed on jamming devices to prevent them from being diverted to uses outside of authorized locations and purposes.[567]

183. The Commission has explored throughout this proceeding the viability of geolocation-based denial, also known as geofencing, whereby mobile device software and/or hardware might be used to disable contraband wireless devices that violate a perimeter surrounding a correctional facility.[568] The Commission sought comment specifically on the feasibility of a network-based geofencing solution where wireless providers would identify and disable contraband wireless devices in correctional facilities located using geofencing.[569] In the *Third FNPRM*, the Commission sought to refresh the record on this topic as it relates to denial of service to contraband wireless devices.[570] The Commission also separately sought comment regarding whether it is in the public interest to require jamming devices to have a

[565] *Third FNPRM*, 40 FCC Rcd at 8057, para. 129.

[566] *Id*.

[567] *Id*. at 8058, para. 129.

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

[569] *Id.*

[570] *Third FNPRM*, 40 FCC Rcd at 8059-60, para. 136.

locking mechanism, geo-location controls, or other features to ensure jammers are only used by those authorized to do so in approved areas.[571]

184. The record demonstrates general concern about the potential for the proliferation of jamming devices used for unauthorized purposes outside of the correctional facility context.[572] Commenters urge the Commission to mandate technological solutions to mitigate unauthorized jammer use.[573] For example, GPSIA recommends that the Commission take precautions through regulation or equipment authorization standards that can help mitigate the proliferation of jammer equipment and its misuse.[574] CTIA specifically suggests a GPS-based automatic shut-off mechanism similar to what the Commission established in its 6 GHz proceeding.[575] Public Knowledge expresses concern regarding possible unauthorized use of jammers, urging that jamming solutions not be authorized as a mobile service, and recommending that the Commission use a third party spectrum access system that verifies the location of the jamming devices at least once every 24 hours.[576] The DI Group's interdiction solution uses ankle bracelets to track inmates' locations using triangulation, and uses geofencing to ensure that its jamming solution will not work beyond the jamming containment area in the correctional facility.[577]

185. Based on our review of the record, and to limit the potential for the proliferation of jamming devices outside the correctional facility context, we also find it in the public interest to require jamming solution providers to include a geofencing feature in the design and operation of their systems, such that any of the jamming devices will automatically shut down if removed from the licensed jamming containment area(s). We believe that, combined with marketing and labeling requirements,[578] a locking mechanism based on geofencing technology will help curb attempts to relocate jamming devices for use outside of a correctional facility.[579] We understand from the record that the implementation of a locking mechanism using geofencing in a jamming solution can be accomplished in a variety of ways.[580] For

[571] *Id*. at 8057-58, para. 129 (addressing the use of geofencing in a jamming solution to prevent such operations outside of the correctional facility's jamming containment area).

[572] *See, e.g.*, GPSIA Comments at 6; CTIA Comments at 31; Verizon Comments at 19; SIA Comments at 4.

[573] *See, e.g.*, CTIA Comments at 32-33.

[574] GPSIA Comments at 6.

[575] CTIA Comments at 32-33, citing *Unlicensed Use of the 6 GHz Band*, 38 FCC Rcd 10523, et al., Second Report and Order, Second Further Notice of Proposed Rulemaking, and Memorandum Opinion and Order on Remand, 38 FCC Rcd 10523 (2023) (proposing to allow very low power devices to operate at higher power levels if they operate under the control of a geofencing system that prevents them from operating in close proximity to co-channel licensed incumbent services in the band). *See also* CTIA Oct. 1 *Ex Parte* Letter at 9 (recommending steps to prevent the proliferation of jammers outside correctional facilities).

[576] Public Knowledge Reply at 19.

[577] DI Group Comments at 5.

[578] *See infra* paras. 205-08.

[579] The Commission previously has facilitated geofencing technology in other contexts, for example, by recently authorizing a new category of unlicensed devices in the 6 GHz band known as geofenced variable power (GVP) devices that are prevented from operating in exclusion zones on certain frequencies to protect incumbent licensed services from significant risk of harmful interference. *See Unlicensed Use of the 6 GHz Band*, *Expanding Flexible Use in Mid-Band Spectrum Between 3.7 and 24 GHz*, ET Docket No. 18-295, GN Docket No. 17-183, Fourth Report and Order and Third Further Notice of Proposed Rulemaking, 41 FCC Rcd 623, 667-68, paras. 108-110 (2026). In the 6 GHz proceeding, exclusion zones are calculated consistent with the protection methodology used by automated frequency coordination (AFC) systems and each GVP access point is required to have a geolocation capability to determine its location and avoid operating on prohibited frequencies within the exclusion zones. *Id*. at 667-68, paras. 109-110.

[580] *See, e.g.*, Public Knowledge Reply at 19 (urging the use of a spectrum access system administrator to ensure jamming devices only operate in authorized DOC facilities); DI Group Comments at 5 (explaining its jamming (continued….)

example, jamming solutions could include an internal geolocation capability within the associated jamming devices, or the system could have an integrated capability to securely connect to external geolocation devices or service to automatically determine the jamming devices' geographic coordinates. Our goal is to render the jamming device incapable of transmitting if the device is removed from the licensed jamming containment area of the correctional facility.[581] We also require that jamming devices include a feature that will assist in Commission enforcement efforts to determine the location of any jamming device illegally moved beyond the containment area of a correctional facility, for example, a tracking mechanism. We seek to provide flexibility and to maintain technological neutrality, and therefore do not mandate a specific approach in meeting these requirements. Potential implementations of such a feature include radio-based systems that transmit a signal to enable the device to be tracked or systems that integrate GPS and cellular technology to enable real-time tracking.[582] Although we do not mandate a specific approach, we require that an applicant for a jamming solution through either an overlay license or lease arrangement include an explanation in its application demonstrating how the jamming solution's geofencing capabilities will be implemented to prevent any jamming device from functioning if removed from the licensed jamming containment area within a correctional facility, and to subsequently locate a removed jamming device if necessary.

186. *Interference Resolution Procedures*. In the *Third FNPRM*, the Commission sought comment on whether we should require the operator of a jamming solution to respond to every complaint of interference to a non-contraband wireless device, including whether to mandate that such an operator immediately shut down all operations pending resolution of the interference.[583] Specifically, the Commission sought comment on whether we should impose specific requirements regarding the interference resolution mechanism, such as procedures for the reporting of complaints, the contents of a complaint, or the response time of the jamming solution operator to analyze and resolve the complaint.[584] The Commission also asked generally whether we should adopt any additional rules that would protect against harmful interference to authorized communications.[585]

187. Commenters generally agree that an interference resolution mechanism is needed to address harmful interference to authorized communications that might occur outside of the jamming containment area. Verizon and CTIA support the adoption of "stop buzzer" procedures to address interference complaints on an expedited basis.[586] CTIA suggests that jamming operators be required to provide a 24/7 contact to receive reports of interference to legitimate communications.[587] Verizon

(Continued from previous page)
feature can be automatically disabled outside the prison's proprietary communications network with geofencing capabilities); CTIA Comments at 32-33 (urging a GPS-based mechanism to ensure jamming solutions only operate in authorized locations).

[581] We recognize that jamming devices may require maintenance or repair by the manufacturer or jamming solutions provider, which we anticipate will be conducted in a shielded facility to prevent signal leakage and harmful interference to authorized services.

[582] Approaches to locating illegally removed jamming devices might leverage technologies used in commercially available products, such as LoJack for locating stolen vehicles and Apple's AirTag devices and associated Find My network. *See* LoJack, *Classic LoJack FAQs*, https://www.lojack.com/customer-support/faqs/ (last visited Oct. 26, 2026); LoJack, *LoJack Stolen Vehicle Recovery System for Cars*, Trucks & SUVs, https://www.lojack.com/products/stolen-vehicle-recovery-cars-trucks-suvs/ (last visited Oct. 26, 2026); Apple, *AirTag*, https://www.apple.com/airtag/ (last visited Oct. 26, 2026).

[583] *Third FNPRM*, 40 FCC Rcd at 8044, para. 97.

[584] *Id*. at 8044-45, paras. 98-99.

[585] *Id*. at 8046, para. 103.

[586] Verizon Comments at 23-24; CTIA Comments at 31; CTIA Oct. 1 *Ex Parte* Letter at 9.

[587] CTIA Comments at 31.

recommends a secure point of contact to receive complaints of interference and an approach to interference complaints consistent with existing part 5 stop buzzer procedures.[588] Trace-Tek also supports a 24/7 point of contact that can "immediately cease all operations upon notification that it has caused harmful interference to an authorized device."[589] iCERT recommends the establishment of a clear shut-down process that is strictly enforced to eliminate harmful interference to authorized devices.[590]

188. The Commission also sought comment in the *Third FNPRM* regarding whether to impose a response time on the overlay licensee to respond to a notification of interference (e.g., no later than 24 hours) or a timeframe by which corrective action must occur (e.g., within 48 hours).[591] J3 Tech suggests that the jamming solutions provider should respond to any valid interference concern in a timely manner, adding that 48 hours seems too stringent, but it should depend on the severity of the interference.[592] Bluetooth SIG states that authorized jamming operators should be required to promptly adjust or deactivate jamming systems if harmful interference to lawful unlicensed devices occurs outside correction facilities.[593] One commenter, CLA, contends that the Commission should not require automatic shutdowns upon receipt of an interference complaint because such a rule would invite abuse.[594] Instead, CLA recommends an "evidence-based" resolution process that would require complaints to include sufficient detail for meaningful investigation, thereby balancing the protection of legitimate users with preventing abuse.[595]

189. After review of the record, we require overlay licensees and lessees to establish a single point of contact that will be available at all times to respond to Commission complaints of harmful interference or requests to cease jamming operations and also to receive credible complaints from FirstNet or wireless providers of harmful interference to authorized users resulting from jamming operations, and to update the contact information, as necessary. We require that applications for overlay licenses or leases for a jamming solution include the name and contact information, including a secure electronic transmission method, of the point of contact available to receive such complaints. WTB will include this information in the license or lease grant so that it will be available to FirstNet and the relevant wireless providers to view in ULS. If the contact information changes going forward, the overlay licensee or lessee must notify WTB through a ULS administrative update so that information will also be viewable. Although we anticipate that jamming operations will be contained within the licensed jamming containment area(s) in a correctional facility consistent with the limits of our deauthorization framework, we also believe that establishing a mechanism for the submission of credible complaints is vital to the successful implementation of jamming solutions in correctional facilities. For purposes of efficiency and to prevent abuses in the resolution process, we require that a complaint of harmful interference to the solutions provider come directly from the Commission, FirstNet, or a wireless provider, not an individual user, and if coming from FirstNet or the wireless provider, the complaint must be credible, i.e., contain sufficient information and supporting documentation to establish its contention that the jamming solution is the source of the harmful interference to an authorized user.

190. Upon request from the Commission or receipt of a credible complaint of harmful interference, an overlay licensee or lessee must immediately cease jamming operations until the complaint

[588] Verizon Comments at 24, referencing 47 CFR § 5.308.

[589] Trace-Tek Comments at 8.

[590] iCERT Comments at 10.

[591] *Third FNPRM*, 40 FCC Rcd at 8044-45, paras. 98-99.

[592] J3 Tech Comments at 13.

[593] Bluetooth SIG Comments at 4.

[594] CLA Comments at 9.

[595] *Id.*

is investigated and resolved. We emphasize that our harmful interference resolution rule for overlay licensees and lessees of jamming solutions is an obligation separate and apart from any agreement negotiated between a DOC and jamming solutions provider regarding circumstances that might warrant mandatory cessation of operations. For example, a DOC might require a solutions provider to cease operation of a jamming solution where first responders require access to the jamming containment area due to an emergency.

191. Pursuant to our rule, an overlay licensee or lessee is required to expeditiously investigate and resolve complaints from the Commission and credible complaints from FirstNet or wireless providers of harmful interference. By requiring cessation of jamming operations pending resolution of the complaints, we incentivize expeditious resolution, while balancing the potential for abuse by those seeking to thwart the implementation of jamming solutions in the correctional facility context. We recognize that the length of time required to investigate and take required corrective action regarding a complaint of harmful interference will vary on a case-by-case basis, and we believe the overlay licensee or lessee is in the best position to assess the facts of the case and react expeditiously. Some commenters recommend the adoption of additional rules requiring jamming solution operators to file reports with the Commission regarding instances of harmful interference caused by jamming operations.[596] We seek to limit regulatory burdens where possible, and decline to adopt such reporting requirements at this time, but will continue to monitor the effectiveness of jamming solutions, the harmful interference resolution process, and whether process abuses arise.

192. *RF Exposure*. In the *Third FNPRM*, the Commission proposed 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.[597] Commenters generally support this proposal.[598] In light of this support and the importance of maintaining RF exposure compliance, we adopt the Commission's proposal. We do not mandate additional user instruction requirements beyond existing rules, as we expect that all jamming devices will be professionally designed and deployed such that proper consideration will be given to the proximity of inmates, correctional facility personnel and visitors relative to the radiating antennas. We believe that the combination of requiring compliance with our RF exposure rules and radiated power limits, and the mandatory containment of the impact of jamming signals to an authorized area, will dictate the careful deployment of antennas for jamming solutions in correctional facilities. We remind stakeholders that Commission rules require applications for equipment authorization for jamming devices, as discussed below, to contain a statement confirming compliance with the RF exposure limits for both the fundamental and unwanted emissions.[599]

193. *Canada/Mexico Agreements.* After acknowledging in the *Third FNPRM* that jamming solution deployments must not cause harmful interference across international borders and must comply with international agreements, the Commission sought comment on whether existing agreements are sufficient to prevent harmful interference.[600] No commenter suggests that additional limitations are required regarding the risk of harmful interference from jamming solutions across international borders.

---

[596] *See, e.g.*, iCERT Comments at 10 (suggesting that jamming solution operators be subject to the same reporting obligations as CIS operators); Trace-Tek Comments at 8 (recommending notice to the Commission's Ombudsperson and a quarterly reporting requirement).

[597] *Third FNPRM*, 40 FCC Rcd at 8045, para. 100; *see* 47 CFR §§ 1.1307(b), 2.1091, 2.1093.

[598] *See, e.g.*, Verizon Comments at 13; Vortezon Comments at 11; StealthRF Comments at 3.

[599] *See* 47 CFR §§ 2.1091(d), 2.1093(d).

[600] *Third FNPRM,* 40 FCC Rcd at 8045, para. 101.

J3 Tech contends there is no need for Canadian or Mexican coordination since their particular signals are designed to be less than 10 dB below the carrier signal at 100 feet from the covered building.[601] Verizon generally argues that the range of technical requirements that apply to wireless licensees should also apply to jamming solutions, including management of Canadian and Mexican border coordination.[602] We clarify that jamming solution providers must meet relevant treaty agreements with Canada and Mexico, which are available for review on the Commission's website.[603]

6. Part 15 Prohibition

194. The framework we adopt for the authorization of jamming solutions in correctional facilities, either through an overlay license or a spectrum leasing arrangement, is intended to subject all jamming devices to the same rigorous testing requirements, equipment authorization rules, and technical limitations. We adopt new rules and amend existing rules across several Commission rule parts to implement our framework to achieve consistency across various authorization methods, with the goal of preventing the proliferation of jamming devices beyond the limited environment of correctional facilities.

195. As the Commission recognized in the *Third FNPRM*, jamming device proponents could argue that, following adoption of rules permitting any jamming, our current part 15 rules would permit operation of jamming devices on commercial bands without a license or lease, provided power levels were sufficiently low.[604] To address this potential loophole, the Commission proposed that *any* Commission–authorized jamming solution, regardless of power level, would only be so authorized through a part 1 leasing process and/or a part 90 overlay licensing mechanism, rather than through low-power part 15 authorized operation.[605] We adopt this proposal in the public interest. We emphasize that a goal in this proceeding is to limit the operation of jamming solutions solely to correctional facilities, and therefore, we must maintain strict control over the operation of these systems to prevent harmful interference to authorized communications. To guard against the unwanted proliferation of jamming devices, we require that jamming operators apply for either a part 90 overlay license or a part 1 lease for a jamming solution and comply with the core technical rules in part 90, and we prohibit any jamming operations under part 15. Combined with a prohibition against part 15 equipment authorization for jamming solutions discussed below, we believe that this will ensure that the authorization of jamming solutions does not lead to the production, marketing, or sale of "unlicensed" low-power jamming devices.[606]

7. Part 2 Equipment Authorization

196. The Commission carries out its responsibilities under section 302 of the Act with respect to RF equipment by establishing technical rules to address regulatory objectives such as preventing harmful interference.[607] To ensure compliance with these technical rules, the Commission generally

---

[601] J3 Tech Comments at 13.

[602] Verizon Comments at 13.

[603] *See* https://www.fcc.gov/canadian-agreements-frequency and https://www.fcc.gov/mexican-agreements-frequency (last visited Oct. 26, 2026).

[604] *Third FNPRM*, 40 FCC Rcd at 8051, para. 114; *see generally* 47 CFR pt. 15. These devices may generally operate across any spectrum band, except for bands specifically restricted to only spurious emissions. 47 CFR § 15.205.

[605] *Third FNPRM*, 40 FCC Rcd at 8051, para. 114.

[606] *See infra* paras. 194-95.

[607] 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.

requires RF equipment to be authorized under part 2 of the Commission's rules prior to marketing or importation into the United States.[608] With regard to equipment authorization, there are three methods for authorizing equipment: (1) Certification; (2) Supplier's Declaration of Conformity; and (3) Exemption.[609] Certification, the most rigorous approval process, is required for RF devices with the greatest potential to cause harmful interference to radio services.[610] Under the certification process, an FCC-recognized accredited testing laboratory[611] 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).[612]

197. In the *Third FNPRM*, the Commission proposed to apply the current equipment authorization procedures to entities seeking equipment certification for equipment to be used as part of a jamming solution in correctional facilities.[613] Specifically, the Commission proposed to require entities to comply with existing part 2, subpart J, procedures for the certification of equipment used as part of a jamming solution that would be authorized pursuant to a lease or a part 90 overlay license.[614] This proposal was considered consistent with the Commission's treatment, for part 2 equipment authorization purposes, of CIS base stations in correctional facilities.[615] Commenters largely agree that equipment authorization under part 2 should be required for jamming solution equipment,[616] though one commenter disagrees, arguing that merely requiring testing of the jamming solutions is sufficient.[617]

198. As we establish a path for licensed operations of jamming solutions through this *Third R&O*, we find that certification under part 2 to ensure compliance with our part 90 core technical rules for jamming devices is necessary to protect against harmful interference to authorized communications. We require jamming devices to be used as part of a jamming solution to be certified under our part 2 equipment authorization procedures. Typically, an RF device must comply with various Commission rule parts, depending on the spectrum on which it will be used, and its equipment certification grant will reflect the determination that the device complies with specific service rule parts. Here, however, we do not require jamming equipment to be certified under each distinct commercial wireless rule part, even when seeking ultimately to operate in those bands. Rather, we require all jamming devices used as part of

[608] 47 CFR pt. 2. (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.

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

[610] *Id.* §§ 2.906, 2.1031 *et seq*.

[611] 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.

[612] Information, including the authorized technical parameters and descriptive information, for all certified equipment, is posted on a Commission-maintained public database. *See* FCC Office of Engineering and Technology, *Equipment Authorization Search*, https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm.

[613] *Third FNPRM*, 40 FCC Rcd at 8054, para. 121.

[614] *Id*.

[615] *Id*.

[616] *See, e.g.*, J3 Tech Comments at 14; Verizon Reply at 3 (arguing that robust equipment certification thresholds are critical); GPSIA Comments at 6 (recommending equipment authorization standards); CLA Comments at 8; Bluetooth SIG Comments at 4; Trace-Tek Comments at 4-6; Oklahoma DOC Comments at 2.

[617] *See* StealthRF Comments at 4, 6-7 (suggests that we not require jamming equipment to be certified, but instead, just require testing of a jamming solution and self-certification).

a jamming solution to obtain equipment certification under part 90.[618] Thus, the core technical rules for jamming devices used as part of a jamming solution are located in a new part 90 subpart, applicable solely to jamming solutions authorized through either overlay licensing or leasing. The part 90, subpart Z technical limits are, in some instances (e.g., maximum radiated power levels), stricter than those applicable to wireless provider operation in commercial wireless bands, and equipment certification testing of jamming devices should necessarily reflect compliance with part 90 requirements applicable to jamming solutions. Also, we recognize that the function of jamming devices, to block receipt of RF signals, differs substantially from commercial base stations seeking to communicate with handsets, and that many of the technical requirements listed in our commercial wireless service rules are not applicable to jamming devices deployed in a jamming solution (e.g., frequency stability, duty cycle, and synchronization requirements).

199. As explained above, to ensure that the authorization of jamming solutions for use in correctional facilities does not result in the proliferation of unlicensed low-power, hand-held jamming devices, we prohibit jamming devices from operating under part 15.[619] To support this prohibition, as proposed, we do not permit jamming devices to be certified under part 15 of our rules. This approach helps ensure that jamming equipment will not be produced, marketed, or sold outside of the narrow context of correctional facilities, or operated outside of our regulatory framework for the authorization of jamming solutions.[620] To achieve the same goal of non-proliferation, we also prohibit a modular transmitter from being certified as a jamming device. Although modular transmitters currently are used more in the part 15 unlicensed device context, we recognize that TCBs have certified certain modular transmitters for operation in commercial wireless bands. By prohibiting modular transmitters from being certified through our part 2 equipment authorization process as part of a jamming solution, we deter instances where an approved modular transmitter would be installed in equipment unrelated to a jamming solution without obtaining separate equipment authorization.

200. In the *Third FNPRM*, the Commission sought comment on whether applying current Commission rule sections 2.911 and 2.1033 regarding application procedures are appropriate to apply to jamming solution applications, or whether amendments to our rules are necessary.[621] The Commission also sought comment on whether any additional rule changes were required to enable certification for jamming solutions.[622] Further, in light of heightened stakeholder sensitivities surrounding jamming devices, the Commission proposed to include jamming solution equipment on the "Pre-approval Guidance List."[623] We did not receive comments on these issues.

201. Consistent with our decision to authorize jamming solutions and require equipment certification for jamming devices, we find it appropriate to apply the procedures contained in rule sections 2.911 and 2.1033.[624] These sections specify the process for obtaining equipment certification, including what information must be included in an application.[625] Additionally, as specified in our rules, equipment on the Commission's Covered List is not eligible for certification and cannot be used as part of a jamming

[618] *See supra* para. 78.

[619] *See supra* paras. 194-95.

[620] *Third FNPRM*, 40 FCC Rcd at 8054, para. 121.

[621] *Id*. at 8054, para. 122.

[622] *Id*. at 8054-55, para. 122.

[623] *Id*. at 8055, para. 122.

[624] *See generally* 47 CFR §§ 2.911 (application requirements for equipment authorizations), 2.1033 (application for certification).

[625] *Id*.

solution.[626] Finally, because the Commission is authorizing jamming solutions for the first time, such equipment will be subject to pre-approval guidance procedures until such time as the Commission determines that jamming devices have reached a sufficiently mature stage and equipment certification procedures for such devices are well established.[627]

202. *Operation of Equipment Used for Jamming Solutions Prior to Equipment Authorization*. In the *Third FNPRM*, the Commission sought comment on whether we should make any change to our part 2 rules governing the operation of equipment prior to equipment authorization.[628] The Commission explained that rule section 2.805 provides that an RF device may not be operated prior to equipment authorization unless certain conditions are met.[629] 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.[630] The Commission explained that an entity seeking to implement a jamming solution, 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.[631] Such a test might be needed, for example, in response to a DOC's request for proposal or to be eligible to enter into a contract with a DOC. The Commission asked whether to amend section 2.805 to specify that jamming solutions may not be operated for testing purposes prior to equipment authorization or whether we should adopt more flexible rules to permit jamming solution testing prior to equipment authorization, but only pursuant to special temporary authority or an experimental license.[632]

203. After review of the record, we find it appropriate to permit the testing of jamming solutions prior to equipment authorization through a part 5 experimental license granted by OET pursuant to current section 2.805(b) of the Commission's rules.[633] This approach is consistent with Verizon's recommendation that jamming solutions should not be permitted to operate prior to equipment authorization *except for limited testing purposes*,[634] and will facilitate compliance with the POC test required at the initial licensing stage of our authorization framework. Relatedly, we adopt targeted amendments to our part 5 experimental licensing rules to accommodate POC testing for jamming solutions.

8. Marketing, Labeling, and Importation of Jamming Devices

204. A primary goal in this proceeding is to cabin jamming solutions to the narrow context of jamming containment areas within correctional facilities and to prevent jamming devices from being deployed outside the correctional facility context, for example in schools, theaters, restaurants, other business establishments, or places of worship. One method of facilitating this goal is to adopt marketing,

---

[626] *See* 47 CFR § 2.903 (prohibition on authorization of equipment on the Covered List).

[627] *See* 47 CFR § 2.964 and KDB Publication 388624 "Pre-approval Guidance (PAG)," https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=28319&switch=P.

[628] *Third FNPRM*, 40 FCC Rcd at 8055-56, para. 124.

[629] *See* 47 CFR § 2.805(a).

[630] *Id.* § 2.805(b).

[631] *Third FNPRM*, 40 FCC Rcd at 8055, para. 124.

[632] *Id*. at 8055-56, para. 124.

[633] *See* 47 CFR§ 2.805(b). 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" consistent with section 333 of the Act. Therefore, under our deauthorization rule, contraband wireless devices would not be protected against harmful interference under part 5 of our rules, or section 333 of the Act, when a solutions provider tests a jamming solution under a part 5 experimental authorization.

[634] Verizon Comments at 21 (emphasis added).

labeling, and importation rules applicable to equipment used for jamming solutions. Below, we adopt targeted rules in this regard.

205. *Marketing*. In furtherance of our goal of containing jamming operations to the narrow context of correctional facilities where authorized, the Commission sought comment on whether it should limit the marketing of jamming devices, in particular, solely to DOCs and their contracted jamming solutions providers.[635] The Commission asked what rule changes should be required to limit marketing.[636] Stakeholders share our concern that jamming devices might be misappropriated for unauthorized uses, and there is a consensus that some restrictions are necessary to mitigate the problem.[637] Verizon and CTIA generally support the Commission's proposed safeguards for the marketing and sale of jamming solution equipment.[638] CTIA states that the Commission should limit marketing of jamming solution equipment only to a DOC or to a jamming provider that has a contract with a correctional facility.[639]

206. We first apply the rules in Commission rule section 2.803, that generally limit marketing of devices prior to equipment authorization, to jamming devices.[640] Under the rules we adopt today, applicants for authority to operate a jamming solution in a correctional facility, either through overlay licensing or leasing, must be either a DOC with authority over the correctional facility for which authority to operate is sought, or a solutions provider that has entered into a contract with such a DOC.[641] To reinforce this eligibility restriction and guard against the spread of jamming devices to unauthorized users, we find it in the public interest to adopt a part 90 rule that restricts marketing of jamming devices to only those entities eligible to operate a jamming solution. Consistent with this restriction, we note that because marketing under the Commission's definition includes sales, jamming devices cannot be re-sold by a DOC or jamming solutions provider except to another DOC or jamming solutions provider that has a contract with a DOC.[642]

207. In the *Third FNPRM*, the Commission sought comment on whether additional requirements were needed to ensure compliance with any marketing restrictions.[643] Some commenters recommend additional rules such as required marketing disclosures and other mechanisms to track a jamming device's chain of custody.[644] CLA agrees with targeted marketing only to eligible entities, but

[635] *Third FNPRM*, 40 FCC Rcd at 8056, para. 125; *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).

[636] *Third FNPRM*, 40 FCC Rcd at 8056, para. 125.

[637] *See, e.g.*, GPSIA Comments at 6 (admitting that marketing limitations would be vital and laudable steps and urging regulations that ensure jamming devices are not commercially available); Verizon Comments at 8-9 (supporting the need for strong restrictions).

[638] *See* Verizon Comments at 20; CTIA Comments at 32.

[639] CTIA Comments at 32.

[640] *See generally* 47 CFR § 2.803 (marketing of RF devices prior to equipment authorization).

[641] *See supra* paras. 79-82, 132-34.

[642] *See* 47 CFR § 2.803(a) (defining marketing, as used in this section, to include sales 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).

[643] *Third FNPRM*, 40 FCC Rcd at 8056-57, para. 125-26.

[644] *See, e.g.*, APCO Reply at 3 (supporting clear and comprehensive disclosures regarding the technologies' capabilities and limitations); Verizon Comments at 20 (advocating for product and marketing disclosure standards, and other chain of custody rules such as a SKU to track devices); CTIA Comments at 32 (recommending disclosures and requiring sellers to verify and retain documentation regarding sales).

also recommends that the Commission avoid overly restrictive marketing rules until evidence emerges that our "narrowly tailored authorizations have led to misuse."[645] On balance, and in light of our strict technical requirements and safety features for jamming devices, we conclude that additional rules in this area are not required at this time. We anticipate that our marketing restriction limited to eligible entities will sufficiently curtail the use of jamming devices in unauthorized contexts. Moreover, the locking mechanism requirement for jamming solutions also directly serves this important purpose.[646]

208. *Labeling*. Recognizing the importance of containing jamming solutions to a correctional facility environment, the Commission sought comment on whether to require a label on jamming devices to warn users that the equipment can only be used by a DOC or solutions provider that has contracted with a DOC to provide a jamming solution in a correctional facility as a Commission licensee or lessee.[647] Commenters generally support a labeling requirement.[648] The Commission also asked whether, given the concern regarding potential misuse, we should prohibit use of e-labeling for any warning information requirements.[649] Commenters did not address the e-labeling issue. To enforce the restrictions on marketing and operation of jamming devices, and to guard against the spread of jamming devices to unauthorized users, we adopt a rule requiring a physical label on jamming devices, and their packaging, warning that only users authorized to operate jamming devices may purchase or operate such devices. We prohibit use of e-labeling to satisfy this requirement.

209. *Importation*. In the *Third FNPRM*, the Commission sought comment on whether equipment used to provide jamming solutions should be permitted to be imported prior to receiving equipment authorization.[650] The Commission noted that various Commission rules provide exceptions for importing and marketing RF devices prior to equipment authorization.[651] We did not receive comments directly addressing this issue.

210. We find it necessary and in the public interest to permit equipment intended for use in a jamming solution to be imported prior to receiving equipment authorization. This will allow jamming equipment to be available for the required POC test conducted at the outset of the authorization process pursuant to a part 5 experimental license. This approach also provides flexibility to solutions providers as they seek to develop effective jamming solutions that comply with our requirements.[652] Under section 2.1204(a)(3) of the Commission's rules, parties generally may import up to 4,000 devices prior to receiving equipment authorization, if the devices are for testing and evaluation to determine compliance with Commission rules, product development, or suitability for marketing.[653] We find that this provision provides the necessary flexibility for manufacturers of jamming equipment to import their devices for the required POC testing, compliance testing, and other activities that will need to be performed prior to receiving equipment authorization.

---

[645] CLA Comments at 10 (also noting that even though the BOP has been testing jamming for some time, there is no evidence regarding the proliferation of illegal jamming activity).

[646] *See supra* paras. 182-85.

[647] *Third FNPRM*, 40 FCC Rcd at 8057, para. 127.

[648] *See, e.g.*, CLA Comments at 10 (supporting clear labeling indicating that jamming devices are for authorized correctional use only); Verizon Comments at 20; CTIA Comments at 32 (suggesting labeling on jamming devices).

[649] *Id.*

[650] *Third FNPRM*, 40 FCC Rcd at 8057, para. 128.

[651] *See, e.g.*, 47 CFR §§ 2.1204(a)(3), (a)(4), (a)(11), and 2.803(c).

[652] We reiterate that equipment authorization is required prior to on-site testing and commencement of jamming operations at the relevant correctional facility.

[653] *See* 47 CFR § 2.1204(a)(3). Parties also may seek written approval from the Chief of the Office of Engineering and Technology to import a greater number of devices. *Id.* § 2.1204(a)(3)(i).

211. In the interest of fostering a level playing field and allowing for the testing of a wide variety of jamming equipment that will best be able to comply with our technical requirements, we do not adopt a requirement that jamming devices be manufactured or assembled in the United States.[654] We believe that our new rules governing the technical specifications and safety features of jamming devices, as well as marketing and labeling rules regarding eligibility to operate jamming solutions, are reasonable and sufficient to restrict jamming operations to authorized users and locations. A "Made in the USA" requirement could stifle innovation and impede our goal of promoting effective jamming solutions as a tool to facilitate correctional community efforts to combat contraband wireless device use in correctional facilities.

D. Facilitating Other Interdiction Technologies

212. The Commission has historically pursued a policy of technology neutrality when promulgating rules.[655] In this proceeding, in its efforts to combat contraband wireless devices in correctional facilities, the Commission has consistently explored the viability of a range of technical interdiction solutions and considered the necessary regulatory steps to give additional tools to the corrections community in this regard.[656] The Commission previously adopted rules to help streamline the process of deploying CISs in correctional facilities and to require the disabling of contraband devices, provided certain conditions are met and the system meets our definition of a CIS. Today, we adopt rules to authorize jamming solutions that utilize transmitters meeting our definition of a jamming device. In addition to MAS and other CIS technologies, the Commission has explored whether it could support the development of other device-based interdiction solutions such as geofencing or beacon technology.[657] Although the *Third FNPRM* focused on ways to authorize jamming solutions in correctional facilities, the Commission also sought to refresh the record on the feasibility of other potential technologies and sought comment on steps the Commission could take to facilitate their development.[658]

213. The record includes comment encouraging the Commission not to move forward with the authorization of jamming technology and to instead focus on existing interdiction solutions[659] or other technologies, such as geofencing. For example, the Satellite Industry Association urges the Commission to consider MAS, "MAS-Evolved systems, detection systems, and carrier-enabled contraband elimination" rather than authorizing jamming.[660] Polaris Wireless contends that the Commission should take a technology-neutral approach to encourage innovation and facilitate geofencing solutions instead of jamming.[661] Marcus Spectrum Solutions suggests that geofencing by the wireless providers should be considered in certain correctional facilities.[662]

---

[654] *See* StealthRF Comments at 5-6. *See also Third FNPRM*, 40 FCC Rcd at 8057, para. 128.

[655] The Commission's long-standing policy has been to promulgate rules that are technology neutral to allow competing telecommunications technologies to succeed or fail in the marketplace on the basis of their merits or other market factors, and not primarily because of government regulation. *See Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket No. 03-264, Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 13900, 13925, 13926, paras. 53, 56 (2005).

[656] *Third FNPRM*, 40 FCC Rcd at 8059, para. 134, n.290.

[657] *Id*.

[658] *Id*. at 8059-61, paras. 134-38; 8063, para. 144.

[659] *See, e.g.*, AICC Comments at 2, 5; CCA Comments at 1-3; iCERT Comments at 1, 4; AT&T Comments at 1-2; CTIA Comments at 4.

[660] SIA Comments at 4-5.

[661] Polaris Wireless, Inc. Comments at 5.

[662] MSS *Ex Parte* Letter at 3, 7-9.

214. We find it in the public interest to implement a regulatory framework for the authorization of jamming solutions as an additional technological option. We remind stakeholders, however, that today's action in no way supplants existing CIS leasing and certification/disabling mechanisms as market-based solutions. We are not persuaded by the record that our current regulations prohibit the introduction of other solutions that industry might seek to develop and implement such that further Commission action is required at this time. For example, in supporting market-based industry solutions, we encourage DOCs, in collaboration with solutions providers, to work with wireless providers and equipment manufacturers to explore geofencing solutions that the Commission's current rules permit. We note that such solutions might require industry cooperation to implement hardware or software upgrades to commercial wireless handsets to address the issue, rather than further Commission involvement through regulatory changes.

E. Further Facilitating and Streamlining the Authorization of CIS Technology

215. As explained herein, our new regulatory framework for the authorization of jamming solutions in correctional facilities is separate and distinct from the existing regulatory framework for CIS leasing and certification/disabling, with more rigorous testing and core technical requirements.[663] Accordingly, the processes for CIS leasing and CIS certification for purposes of requesting contraband device disabling remain in place. In the *Third FNPRM*, the Commission invited stakeholders to refresh the record on the question of whether we should make any changes to our rules to further streamline the current CIS leasing process.[664] Some commenters recommend rule changes that would eliminate or change the requirement to obtain leases from the Commission for certain types of CISs or how we process CIS leases.[665] We find that there is not sufficient evidence in the record showing that our current leasing rules—as they apply to CIS deployments—require further streamlining. We note that CTIA recognizes that MAS has been an effective interdiction technology and does not suggest any further streamlining measures in this regard.[666] Today, we provide an alternative regulatory path for the corrections community to combat contraband wireless devices using a different technology, i.e., jamming, and we decline to adopt any additional requirements in connection with the CIS leasing process or to amend the current streamlined process.[667]

216. The Commission also sought comment on whether we should amend any regulatory procedures in section 20.23 of the Commission's rules, the rule section governing CIS Phase 1 authorization, Phase 2 self-certification, and the disabling process.[668] Specifically, the Commission sought comment on rule section 20.23(c), which addresses when a DCFO may send a qualifying request to a CMRS licensee.[669] As the Commission explained, under the current rule, a DCFO may send a qualifying request to a CMRS licensee on the sixth business day following the date of the filing of a

[663] As we are not including jamming solutions as a type of CIS, we reject suggestions to apply the same CIS processes to the authorization of jamming solutions. *See, e.g.*, South Carolina DOC Comments at 7; Trace-Tek Comments at 9; CIS Providers Reply at 4-5.

[664] *Third FNPRM*, 40 FCC Rcd at 8062, para. 141.

[665] *See, e.g.*, iCERT Comments at 6 (suggesting that the Commission should eliminate the lease requirement for portable CIS solutions and consider using consent letters instead); Verizon Comments at 26 (suggests that the Commission use consent letters for portable or temporary MAS); AT&T Reply at 8-11 (recommending ULS reform, automatic lease grants one day after filing, and treating detection interdiction systems differently).

[666] CTIA Comments at 8-9.

[667] For example, we decline to mandate roaming agreements as overly burdensome in the context of voluntary lease arrangements. *See, e.g.*, Trace-Tek Comments at 11; OmniProphis Comments at 9.

[668] *Third FNPRM*, 40 FCC Rcd at 8062, para. 142; 47 CFR § 20.23.

[669] *Id*.

Phase 2 self-certification, provided no objections from CMRS licensees are received.[670] Since WTB began receiving certifications under this process, WTB has found that, despite a lack of wireless provider objection, certain filings from solutions providers have necessitated staff outreach and subsequent discussion, resulting in the filing of amended certifications, carrying beyond the sixth business day.[671] 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.[672] Therefore, for administrative clarity, the Commission proposed that a DCFO can submit a qualifying request, provided there are no wireless provider objections received within five business days, on the date WTB updates the Commission's website to reflect certification of a specific facility. We received no objections to this proposed rule change, and we therefore amend section 20.23(c) to permit a DCFO to submit a qualifying request, absent wireless provider objections, beginning on the date WTB updates the Commission's website to reflect Phase II certification, or recertification following mandatory retesting every three years, of that specific facility.[673]

217. With regard to the CIS certification and disabling process, we decline to adopt any additional requirements or changes to the existing CIS framework at this time. For example, we decline to mandate that wireless providers add the IMEIs of the disabled contraband wireless devices to the Stolen Phone Database.[674] We also decline to change our Phase 1 or Phase 2 self-certification process for CIS deployments at specific correctional facilities.[675] The CIS Providers propose that, rather than authorize jamming, the Commission should use overlay licensing for CIS providers and an altered section 20.23 process.[676] We decline to make such sweeping changes to our current CIS authorization framework, as we continue to believe that our CIS disabling process is not unduly burdensome. We also find it in the public interest to maintain our existing rules based on wireless provider participation in leasing arrangements, given the need for wireless provider cooperation in the contraband wireless device disabling process. Numerous solutions providers have relied successfully on this process over the past five years following the Commission's adoption of the CIS certification and disabling process.[677] We are encouraged that Verizon suggests that no additional rules or clarifications are necessary for the disabling process, as licensees "already coordinate with each other, with MAS solution vendors, and with other stakeholders, in terminating service to devices identified as contraband, in order to troubleshoot and refine

[670] *Id*.

[671] *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).

[672] *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 Oct. 26, 2026).

[673] We note that Omniprophis does not object to extending the time permitted for receipt of wireless provider objections and for Commission staff review of self-certifications for a "reasonable period of time." OmniProphis Comments at 10.

[674] *See, e.g.*, Trace-Tek Comments at 10; OmniProphis Comments at 9.

[675] *See, e.g.*, Trace-Tek Comments at 9 (recommending that we replace the self-certification process with a notification of the locations of the correctional facilities where it has deployed); CIS Providers Comments at 5.

[676] CIS Providers Reply at 5-7; *see* Letter from Marjorie K. Conner, Counsel to CIS Providers, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 13-111 (filed July 9, 2026) (proposing a "secondary license process" for CIS as an alternative to the authorization of jamming solutions).

[677] *See generally Second R&O*. In the *Third FNPRM*, the Commission summarized the current status of CIS deployment. *Third FNPRM*, 40 FCC Rcd at 8007-08, para. 12.

the process." Verizon further notes that the process has worked "with great success."[678] We will continue to monitor developments regarding the efficiency of lease arrangements in the CIS disabling process.

F. Costs and Benefits

218. This *Third R&O* adopts rules to authorize jamming solutions for traditional commercial spectrum bands in non-federal correctional facilities to combat contraband wireless device use. Jamming technologies disrupt wireless signals on specific bands within a specific geographic area, thereby rendering wireless devices in that area non-operational. This action provides DOCs an additional tool to combat contraband wireless devices, but does not require its use.

219. The *Third R&O* does not impose costs on correctional facilities or other parties. Any cost associated with jamming solutions would arise only if a correctional facility voluntarily selects jamming as a contraband interdiction option. With respect to external costs from implementing a jamming solution, engineering requirements—including POC testing, technical parameters that confine the effects of the jamming solution to the containment area(s), and post-authorization, pre-operational on-site testing—help ensure that the jamming solution does not cause harmful interference to authorized users outside the jamming containment area(s).

220. To the extent correctional facilities opt to implement jamming solutions, the public benefits stem primarily from the expected reduction in criminal activity enabled by contraband wireless devices. By preventing unauthorized communications within targeted areas, jamming technology can significantly disrupt illicit coordination, protect victims and witnesses from intimidation, and curtail the organization of criminal enterprises both inside and outside correctional facilities. Jamming solutions enhance institutional security and improve safety conditions for staff, inmates, and the surrounding public. Therefore, this item will result in meaningful public safety benefits, though the overall magnitude of benefits will depend on the number of facilities that ultimately choose to deploy a jamming solution.

221. The voluntary nature of utilization of this interdiction tool indicates that any economic effects will be limited and facility-specific. Further, technical safeguards and testing requirements help ensure that authorized communications outside of the jamming containment areas of correctional facilities remain protected from harmful interference. To the extent jamming is implemented, the action is expected to generate meaningful public safety benefits by reducing criminal activity enabled by contraband wireless devices. Overall, the net impact of this item is positive, with voluntary costs and adoption-dependent, security and public safety benefits.

IV. FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING

222. In the *Third R&O*, we adopt rules implementing a regulatory framework authorizing non-federal operation of RF jamming solutions on certain spectrum bands in correctional facilities. The framework allows an eligible jamming solutions provider to obtain a Commission license to operate a jamming solution in a correctional facility, while subject to strict testing requirements and technical safeguards to ensure that jamming is confined to jamming containment areas of correctional facilities. Our approach permits jamming solutions through a revision of section 1.903 of our rules, which only applies to fixed and mobile stations in the WRS. As commenters note, revising section 1.903 to deauthorized subscribers using licensed wireless spectrum does not impact the authority of a contraband wireless device operating on an unlicensed basis such as Wi-Fi or other part 15 devices, or those using spectrum separately licensed for satellite communications under part 100 of the Commission's rules.[679]

[678] Verizon Comments at 26.

[679] On July 23, 2026, the Commission released a Report and Order and Further Notice of Proposed Rulemaking that replaces part 25 of the Commission's rules with a new part 100 to, *inter alia*, streamline and simplify the satellite application process and operating standards, including a part 100 licensing "assembly line" to expedite and provide flexibility for space companies. *See Space Modernization R&O*. For purposes of this *Third R&O and Fourth*

(continued….)

223. Although today we limit our newly adopted regulatory framework to jamming solutions operating on the bands identified in the *Third R&O*, we also seek to avoid creating spectrum holes that inmates are likely to exploit to perpetuate contraband wireless devices use. Accordingly, in this *Fourth FNPRM*, we propose and seek further comment on an approach that expands our adopted framework to unlicensed part 15 operations consistent with section 333 of the Act. We also seek additional comment on the scope of inmate use of contraband wireless devices communicating via satellite networks and an appropriate means to authorize jamming operations on this separately licensed spectrum consistent with statutory constraints. Finally, we seek comment on potential additional safeguards for jamming solutions, including adjustments to wireless provider networks, additional solutions provider compliance or monitoring obligations to protect authorized users, including vital public safety operations, as well as an approach whereby the Commission would establish "quiet zones" in and around certain correctional facilities.

A. Unlicensed Operations Under Part 15

224. In the *Third FNPRM*, the Commission sought comment on whether we should expand deauthorization to enable jamming that might address contraband wireless devices not relying on spectrum commonly licensed to wireless providers and deployed as part of a commercial wireless network.[680] The Commission sought comment on whether devices operating on an unlicensed basis or other radio services not covered by the deauthorization rule are a substantial problem in correctional facilities and, if so, on the appropriate framework through which to authorize jamming solutions.[681] As the Commission explained, part 15 of the Commission's rules permits users to operate RF devices without a Commission-issued individual license, and therefore, our amendment to rule section 1.903 does not affect wireless devices operating under the part 15 rules.[682] Specifically, the Commission sought comment on the scope of inmate use of Wi-Fi in contraband wireless devices in correctional facilities,[683] including whether inmates are using Wi-Fi hotspots inside or outside of correctional facilities to access Wi-Fi signals.[684] Also, recognizing the widespread use of Wi-Fi and unlicensed devices for security applications, the Commission asked whether correctional facilities rely on unlicensed devices for essential security operations, e.g., wireless security cameras.[685]

225. Commenters offer some evidence that inmates are exploiting unlicensed devices for contraband use. CLA asserts that contraband wireless devices are now using Wi-Fi and Bluetooth, and that limiting jamming to commercial bands would leave "exploitable gaps" for inmates.[686] The South Carolina DOC claims that it has observed "numerous instances" of inmates using Wi-Fi and Bluetooth

(Continued from previous page)
FNPRM, when discussing the use of satellite spectrum for jamming operations, we refer where applicable to either part 25 (in effect at the time of the Commission's *Third FNPRM*) or part 100 (adopted; effective date forthcoming).

[680] *Third FNPRM*, 40 FCC Rcd at 8049-53, paras. 109-119.

[681] *Id*. at 8049, para. 109. Although the Commission asked about the potential operation in correctional facilities of private land mobile radios typically regulated by the Commission as PMRS in non-commercial radio services or devices licensed by rule under part 95, we received no comments substantiating the use of these devices in correctional facilities as contraband.

[682] *Id*. at 8049, para. 110; *see generally* 47 CFR pt. 15. As noted, 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. *Id*. at n.245.

[683] *Third FNPRM*, 40 FCC Rcd at 8050, para. 111.

[684] *Id*.

[685] *Id*.

[686] CLA Comments at 3, 10 (claiming that contraband communications increasingly exploit Wi-Fi hot spots, satellite links, and other emerging technologies).

communications on contraband wireless devices, as confirmed by "intelligence collection, inmate testimony, and forensic examination of confiscated devices."[687] Vortezon states that inmate use of Wi-Fi "is definitely a potential problem in correctional facilities, if it isn't already."[688] Dedrone asserts that use of Wi-Fi is an "ongoing" problem in correctional facilities.[689] Existing CIS providers indicate that Wi-Fi connectivity currently is being used by contraband wireless devices, including devices that have been disabled through the Commission's disabling process.[690] The record also includes substantial opposition to authorizing jamming of spectrum used by unlicensed devices from groups arguing that such an approach is premature or not adequately considered.[691] Bluetooth SIG is concerned about the impact of jamming on unlicensed devices, both those operating outside of correctional facilities in surrounding areas and authorized part 15 devices used inside facilities for security, operations, and prison management.[692] Similarly, the Wi-Fi Alliance expresses concern that permitting jamming of spectrum used by Wi-Fi could disrupt Wi-Fi communications in surrounding areas, as well as legitimate Wi-Fi operations inside of correctional facilities.[693]

226. Our goal in this proceeding is to provide the corrections community with additional tools to combat contraband wireless devices in correctional facilities by authorizing jamming solutions that can be deployed expeditiously and effectively, with appropriate safeguards built into the regulatory framework. We share the concern that if inmates are able to easily circumvent jamming solutions by using unlicensed devices, then jamming could become less effective.[694] We therefore seek additional comment on the scope of the problem of contraband devices operating on an unlicensed basis and propose a framework below to authorize jamming solutions of such devices. We welcome submission of additional information in the record evidencing inmates communicating via unlicensed devices, including the types of devices inmates are using. Are inmates using cellphones with built-in Wi-Fi hotspot capabilities or stand-alone transmitting devices that act as mobile hotspots to enable access to the Internet? Are other protocols being used in addition to Wi-Fi and Bluetooth? Do stakeholders anticipate that contractual arrangements for the deployment of jamming solutions will include requirements to cover both traditional commercial spectrum, as well as unlicensed devices?

227. Public Knowledge contends that "tethering"—when a contraband device uses unlicensed spectrum to tether to an authorized cellular device to circumvent cellular restrictions—is not a problem because if jamming is authorized on commercial spectrum, then there would be no functioning devices available for tethering.[695] Public Knowledge also contends that the use of Wi-Fi is under the control of the correctional facility, and claims it is "beyond absurd" that correctional facilities would be unable to limit Wi-Fi access.[696] Public Knowledge asserts that facilities can simply turn off the ability of MAS

[687] South Carolina DOC Comments at 4 (stating that "tethering" to a device with a cellular connection has been observed).

[688] Vortezon Comments at 21.

[689] Dedrone Comments at 6.

[690] Tecore Reply at 5-6; OmniProphis at 8.

[691] *See* Bluetooth SIG Reply at 3; *see generally* Wi-Fi Alliance Comments.

[692] Bluetooth SIG Comments at 1, 5.

[693] Wi-Fi Alliance Comments at 5-6.

[694] *See* CTIA Comments at 27; CTIA Reply at 13 (stating that by not extending jamming to non-commercial spectrum, inmates could easily exploit loopholes for the use of contraband devices).

[695] Public Knowledge Comments at 13-14, responding to South Carolina DOC's argument that inmates can tether to devices with cellular service. *See* South Carolina DOC Comments at 4.

[696] Public Knowledge Comments at 14-15, responding to Dedrone's arguments that inmates will switch from using 5G LTE to Wi-Fi or Bluetooth. *See* Dedrone Comments at 6.

authorized devices to act as mobile hotspots and control access of devices using Wi-Fi or Bluetooth through common network management tools.[697] We seek comment on this assertion, and also on the extent to which contraband wireless devices could "tether" to authorized devices in the surrounding area outside of the correctional facility (e.g., the parking lot or other geographic areas in sufficiently close proximity to the facility perimeter) or potentially authorized wireless devices inside of the facility (e.g., employee devices, vendor devices). To what extent is "tethering" an existing problem? Further, we seek comment on the technology available and measures needed for jamming solutions to achieve the stated goal of blocking contraband Wi-Fi devices, while protecting devices operating on unlicensed spectrum that are essential to providing security and monitoring in correctional facilities, or that are used by inmates for educational purposes. Are inmates able to misappropriate authorized Wi-Fi devices, for example tablets, to circumvent security and monitoring protocols?

228. *Deauthorization of Contraband Part 15 Devices*. In the *Third FNPRM*, the Commission sought comment on the appropriate deauthorization approach and authorization framework to permit jamming solutions to target unlicensed devices consistent with section 333 of the Act.[698] Some commenters argue that the Commission did not offer a legal theory for how a deauthorization rule based on section 1.9003 could apply to unlicensed operations.[699] Bluetooth SIG suggests that we would need to amend part 15 in this regard and that we should require a jamming solution provider seeking to jam part 15 devices to be licensed under part 90, acknowledging that part 1 leasing rules do not apply to the operation of part 15 devices.[700] The Wi-Fi Alliance warns that merely asserting that part 15 devices already operate without protection from interference that may be caused by the operation of authorized stations, i.e., jamming devices, would upset the premise of part 15 operations and not be in the public interest.[701] Dedrone suggests that the Commission deauthorize part 15 devices by including such devices in the definition of "contraband wireless device" and clarifying that deauthorized part 15 stations would no longer be protected from interference.[702] Public Knowledge argues that the same statutory arguments (including MQD concerns) it raises with regard to authorizing jamming on commercial spectrum apply equally to unlicensed devices.[703]

229. We propose to deauthorize contraband part 15 devices by amending section 15.1 of the Commission's rules to indicate that, where an intentional radiator meets the definition of a contraband wireless device in section 1.9003 of the rules (i.e., where possession or operation within a correctional facility is prohibited by federal, state, or local law, or a correctional facility rule, regulation, or policy), operation of such device is not permitted and therefore may be subject to jamming solutions consistent with section 333 of the Act.[704] Although part 15 devices must accept any and all interference, and the Commission has not adopted specific rules prohibiting Wi-Fi blocking, the Commission previously has found that Wi-Fi blocking is a violation of section 333.[705] We believe that our proposal to deauthorize

[697] Public Knowledge Comments at 16.

[698] *Third FNPRM*, 40 FCC Rcd at 8050, 51, paras. 112, 113.

[699] *See, e.g.*, Bluetooth SIG Reply at 3; CTIA Comments at 4, 27.

[700] Bluetooth SIG Comments at 2-3.

[701] Wi-Fi Alliance Comments at 3-5.

[702] Dedrone Comments at 6.

[703] Public Knowledge Comments at 11-12 (arguing that the use of the term "any" in section 303(m)(1)(E) makes clear that Congress did not permit the Commission to authorize deliberate jamming on any spectrum, including unlicensed spectrum); *see supra* paras. 42-44 (discussion of Public Knowledge's legal arguments).

[704] 47 CFR §§ 15.1, 1.9003; 47 U.S.C. § 333.

[705] *See M.C. Dean, Inc.*, Notice of Apparent Liability for Forfeiture, 30 FCC Rcd 13010, 13031 (EB 2015) (dissenting statement of Commissioner Ajit Pai).

contraband wireless devices in correctional facilities operating pursuant to part 15 will address stakeholder uncertainty regarding compliance with section 333 of the Act. We recognize that our proposed approach to part 15 device deauthorization would apply only to areas where the operation of *all* part 15 devices is expressly prohibited as contraband, and we do not propose to deauthorize, or permit the jamming of, part 15 devices in correctional facilities in areas where part 15 device usage is permitted by a correctional facility, for example inmate tablet use for educational purposes. Contrary to Public Knowledge's contention, we do not believe that proposing to authorize jamming solutions to address contraband part 15 device use in correctional facilities rises to the level of economic or political importance requiring application of the major questions doctrine.[706]

230. *Authorizing Part 15 Jamming Solutions.* We note that the Commission's *Third FNPRM* did not propose a specific regulatory framework that permits jamming solutions for part 15 operations consistent with section 333 of the Act, but sought comment on whether such an approach was in the public interest. Notwithstanding their legal and policy objections to the authorization of jamming generally, both CTIA and Verizon suggest that any Commission approach to authorizing jamming should not exclude technologies, such as Wi-Fi, as failure to do so creates loopholes for inmates to exploit.[707]

231. The record describes inmate use of unlicensed devices for unauthorized communications that can jeopardize public safety, and we therefore propose rules to authorize jamming solutions operating on spectrum currently used on an unlicensed basis under part 15, particularly Wi-Fi. We propose that a solutions provider seeking to operate a jamming solution in a correctional facility intended to prevent unlicensed contraband wireless device use must obtain a part 90 overlay license and fully comply with the adopted part 90 rules governing POC testing, overlay license application requirements, and core technical rules and safeguards, in the same manner as applicants seeking to deploy jamming solutions on licensed commercial spectrum.[708] We propose to amend part 15 of the Commission's rules to indicate that the operation of a jamming solution on certain spectrum bands,[709] heretofore available for unlicensed part 15 device operations, requires a Commission license under our new part 90 overlay licensing rules.[710] Importantly, however, we clarify that the part 1 leasing approach to authorizing jamming solutions, available in licensed bands as reflected in part 90, would not be an option for an applicant seeking an authorization to operate a jamming solution in a correctional facility targeted at unlicensed part 15 operations. As the Commission emphasized, wireless providers do not have licenses to operate on spectrum identified as available for Wi-Fi under part 15, and therefore the part 1, subpart X leasing approach is entirely inapplicable. Accordingly, we propose that applicants seeking authorization for a jamming solution in a correctional facility must apply for an overlay license under our new part 90 rules adopted in the *Third R&O*. We seek comment on this proposed approach, including the costs and benefits.

232. In the *Third FNPRM*, the Commission specifically asked whether a part 90 overlay license for spectrum on which unlicensed devices operate should be a separate part 90 license only for those identified spectrum bands, or whether it should be combined with a more expansive part 90 license that covers a mix of licensed bands, as well as the bands most commonly used by unlicensed devices.[711] We propose that for administrative efficiency, overlay license applicants can apply for whichever spectrum bands they seek authority to jam, including a mix of licensed bands and bands currently used for unlicensed operations. We seek comment on these proposals and whether there are other preferred

[706] Public Knowledge Comments at 11.

[707] CTIA Reply at 13; Verizon Comments at 14-15.

[708] *See supra* paras. 69-121, 154-91.

[709] *See infra* para. 236.

[710] *See* 47 U.S.C.§ 301 (requiring a license for the "transmission of energy or communications or signals by radio").

[711] *Third FNPRM*, 40 FCC Rcd at 8051, para. 113.

alternatives to license jamming operations targeting unlicensed operations, including specific changes that would be required to our part 15 rules and the part 90 rules adopted herein.

233. In today's *Third R&O*, we recognize that a solutions provider will typically enter into a contractual relationship with a DOC to provide a jamming solution, and we require that an applicant seeking such a license through either an overlay or lease to include a certification in its application that a contract with a DOC exists to provide jamming at the relevant facility.[712] As leasing is not an option for part 15 operations, we propose and seek comment on requiring applicants seeking a part 90 overlay authorization to operate jamming solutions on the bands that support part 15 operations to include in its application a certification that it has entered into a contract that requires the solutions provider to block or otherwise deny access to unlicensed part 15 transmissions.

234. In terms of technical requirements, the Commission sought comment in the *Third FNPRM* on the specific bands we should authorize for jamming solutions aimed at stemming the use of unlicensed devices. Specifically, the Commission asked whether the rules should be flexible to permit jamming solutions for any band where unlicensed devices can operate (including the same bands on which services allocated in the frequency allocation table operate), or only the most commonly used bands.[713] The Commission explained that part 15 of the Commission's rules permits users to operate RF devices without a Commission-issued individual license.[714] Although users can access many spectrum bands on this basis, the majority of unlicensed devices used for communications (e.g., Wi-Fi and Bluetooth) typically only operate across a few bands, i.e., in the 2.4 GHz, 5 GHz, and 6 GHz bands.[715]

235. Verizon contends that jamming solutions should cover spectrum used for any commercial wireless services, including unlicensed services, and that any rules should apply in a technology-and competitively-neutral manner.[716] Verizon specifically states that with regard to unlicensed operations, at a minimum, jamming solutions should be permitted on bands that support Wi-Fi connectivity, such as the 900 MHz, 2.4 GHz, 5 GHz, and 6 GHz bands.[717] Dedrone urges that all spectrum commonly used by drones be included in the rule; that is, the Commission should authorize jamming solutions that prevent the operation of Wi-Fi devices or other part 15 devices using spectrum including 433.05-434.79 MHz, 902-928 MHz, 2.4-2.5 GHz, 5.15-5.25 GHz, and 5.65-5.95 GHz.[718]

236. We propose at this time to license jamming solutions for operation on the following bands currently available for part 15 unlicensed operation: 2400-2483.5 MHz, 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz, 5850-5895 MHz, 5925-6425 MHz, 6425-6525 MHz,

---

[712] *See supra* para. 113.

[713] *Third FNPRM*, 40 FCC Rcd at 8051-51, para. 115.

[714] *Id*. at 8049, para. 110; *see generally* 47 CFR pt. 15. As noted, 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. *Id*. at n.245.

[715] *See Third FNPRM*, 40 FCC Rcd at 8051-52, para. 115 (citing as examples, *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) (2.4 GHz); *Infrastructure (U-NII) Devices in the 5 GHz band*, ET Docket No. 13-49, First Report and Order, 29 FCC Rcd 4127 (2014) (5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz); *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) (5850-5905 MHz); *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) (6 GHz)).

[716] Verizon Comments at 14-15.

[717] *Id*.

[718] Dedrone Comments at 3 (noting that 5.65-5.95 GHz includes the 5.8 GHz ISM band, as well as adjacent bands used for common commercial video links on contraband wireless devices).

6525-6875 MHz, and 6875-7125 MHz. We believe this approach addresses the most commonly used unlicensed devices, including Wi-Fi devices, that could be operational in correctional facilities, and we seek comment on our proposal, including the costs and benefits.

237. *Table of Allocations*. To facilitate deployment of jamming solutions in the bands where Wi-Fi typically operates, we propose to apply the US footnote to the U.S. Table, adopted in the *Third R&O*, that established a primary fixed and land mobile service allocation for jamming solution operations, to the following additional bands: 2400-2483.5 MHz, 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz, 5850-5895 MHz, 5925-6425 MHz, 6425-6525 MHz, 6525-6875 MHz, and 6875-7125 MHz. Specifically, to reflect the additional bands, we propose and seek comment on amending this footnote to read as follows: "USXXX A jamming solution may be authorized subject to part 90, subpart Z of this chapter to prevent the operation of wireless devices in correctional facilities deemed contraband through a federal, state or local law, or a correctional facility rule, regulation, or policy. Jamming solution operation is permitted under a primary allocation in the fixed and land mobile services, limited to an authorized jamming containment area within a correctional facility. Operation beyond the authorized jamming containment area is strictly prohibited, is on a non-interference basis, and shall not cause harmful interference to authorized services or devices." We seek comment on this proposal, including the costs and benefits.

238. In the *Third FNPRM*, the Commission noted that unlicensed operations, in contrast to licensed operations where technical rules assume an exclusive licensee, often require technical provisions to facilitate sharing of the bands and to protect authorized incumbents in the bands from unlicensed users.[719] Therefore, the Commission sought comment on how to ensure that jamming solutions adequately protect authorized incumbent users operating on such bands from harmful interference.[720] The Commission sought comment on what technical rules should apply to jamming solutions intended to prevent unlicensed devices from communicating, including the specific rules that should or should not apply in each band of interest.[721] The Commission asked whether, for example, we should allow a jamming solution to transmit over entire bands used by unlicensed devices with one hundred percent duty cycle, and what the transmit power limit and out-of-band emission limit characteristics should be for such a jamming solution.[722] The Commission also sought comment on the appropriate interference protection obligations to impose on jamming solutions with respect to authorized unlicensed device operations inside or in the surrounding area outside of a correctional facility.[723] For example, should jamming solutions comply with a field strength limit similar to those applicable to operations in licensed bands?[724] With regard to these technical issues, the Commission requested that commenters provide relevant interference analyses to justify their positions.[725]

239. The Wi-Fi Alliance expresses concern that allowing jammers to interfere with Wi-Fi and other unlicensed devices would be a *de facto* licensed service, operating with primary status in bands that are designated for unlicensed use, a result that would require changes to the Table of Frequency

[719] *Third FNPRM*, 40 FCC Rcd at 8052, para. 116. The Commission noted, as examples, frequency hopping systems operating in the 2.4 GHz band (that require a minimum number of channels and limit the average time of occupancy on any channel), the Dynamic Frequency Selection mechanism in the 5.25-5.35 GHz and 5.47-5.725 GHz bands to protect radars, and Wi-Fi access points in the 6 GHz band. *Id*.

[720] *Id*.

[721] *Id*. at para. 117.

[722] *Id*.

[723] *Id*. at 8052-53, para. 118.

[724] *Id*. at 8053, para. 118.

[725] *Id*. at 8052-53, paras. 117-118.

Allocations and essentially upend the premise of part 15 operations.[726] Further, the Wi-Fi Alliance argues that, unlike the tailoring of authorizations on licensed spectrum in a way that avoids the jamming of permitted devices, there could be no such tailoring if the Commission permits the jamming of unlicensed devices, leading to unacceptable collateral damage to nearby communities, essential services, and legitimate communications inside correctional facilities.[727] The Bluetooth SIG expresses particular concern regarding how a jamming solution deployment might affect unlicensed devices operating in the vicinity of a correctional facility, including critical health-related devices, and urges the Commission to impose a requirement on licensees not to cause interference to these devices.[728] To address this concern, the Bluetooth SIG recommends the following potential solutions: signal capturing, containment requirements, remediation duty, pre-deployment interference analysis, and transparency and oversight.[729] The Bluetooth SIG also suggests that the Commission ensure protections for authorized part 15 devices inside correctional facilities, listing examples of wireless devices used for facility operations and management, such as body-worm cameras, security cameras, security systems, and lighting systems.[730] We seek comment on these issues.

240. *Power Limits for Jamming Solutions that Target Unlicensed Operations*. We propose to apply a radiated PSD limit for jamming solutions aimed at stemming unlicensed device usage in correctional facilities that corresponds with the power limit typically used for part 15 Wi-Fi operations. In the *Third FNPRM*, the Commission highlighted the most commonly used bands for Wi-Fi and sought comment on a variety of issues related to how jamming solutions can best address unlicensed operations within a correctional facility.[731] These issues include the need to account for the diverse set of protocols and modulation schemes, including frequency hopping, used by these devices to maximize their ability to successfully operate in noisy RF environments, which bands jamming should be permitted in, and what technical rules should apply to jamming solutions that target unlicensed operations.[732] We received no comments providing input on appropriate technical limits for jamming solutions for Wi-Fi connections that might be established to enable communications with contraband wireless devices.

241. We note that the maximum power permitted varies in the bands commonly used for Wi-Fi, and that our part 15 rules are designed to be flexible to accommodate a wide range of applications. We seek to facilitate effective jamming solutions and recognize that it may not be feasible to apply the exact current part 15 power limits for all jamming solutions. We therefore propose and seek comment on a single radiated power limit for jamming solutions that is equivalent, on a per megahertz basis, to a transmitter operating at a typical bandwidth at maximum power for most of the bands currently used for Wi-Fi (i.e., 4 watts total radiated power[733]). Although this power is permitted in a channel bandwidth as low as 500 kHz,[734] most Wi-Fi devices spread the power over at least a 20 megahertz bandwidth, equating

[726] Wi-Fi Alliance Comments at 4-5 (also pointing out that some unlicensed devices operate on spectrum shared with licensed services, notably the 6 GHz band, and that authorizing the use of jammers in that spectrum would affect not only Wi-Fi, but also those incumbent operations).

[727] *Id*. at 5-6 (explaining not only negative consequences to nearby areas, but also to internal communications such as Wi-Fi communications supporting education, telehealth, and facility operations, and noting that authorizing specific segments of Wi-Fi spectrum would be ineffective).

[728] Bluetooth SIG Comments at 3-4.

[729] *Id*. at 4.

[730] *Id*. at 5-6.

[731] *See Third FNPRM,* 40 FCC Rcd 8050-8053, at paras. 110-118.

[732] *Id*.

[733] The typical maximum power is based on 1 watt conducted power and a 6 dBi antenna. *See*, *e.g.*, 47 CFR §§ 15.247(b), 15.407(a).

[734] *Id*. § 15.247(a)(2).

to a power spectral density of 200 mW/MHz (23 dBm/MHz) EIRP.[735] We propose this power level as necessary to effectively jam contraband devices operating as part 15 devices within the jamming containment area(s). We believe that there are several factors supporting the use of this power limit for jamming solutions across a range of bands that support unlicensed operations, such as Wi-Fi. For example, we expect jamming solutions to be professionally installed in controlled environments so as not to cause harmful interference outside the jamming containment area. Further, for jamming solutions that seek to operate on various Unlicensed National Information Infrastructure (U-NII) bands[736] across the 5.15-7.125 GHz band, it may prove more efficient to produce a single transmitter that operates across the entire band, and for a solutions provider to install notch filters where necessary to meet applicable band-specific OOBE limits, rather than to adjust power levels on a band-by-band basis when many of these bands are adjacent. Moreover, the PSD we are proposing would be uniformly applied across the 2.4 GHz, 5 GHz, and 6 GHz bands. We believe that any solution that meets such criteria for the 2.4 GHz band should similarly meet that same criteria for the higher bands, given that they are subject to more propagation and building penetration losses. We recognize that our proposal assumes that the jamming solution is properly installed to curb emissions outside the jamming containment areas, so as to not cause harmful interference to authorized devices.

242. Given the controlled deployment environment of correctional facilities, and to facilitate a streamlined regulatory approach that allows consistent operation across adjacent bands with varying power limits, we propose and seek comment on permitting a 23 dBm/MHz EIRP for jamming solutions across all the bands noted above that support Wi-Fi operations, in the interest of regulatory parity and efficient jamming solution design. We seek comment on whether this PSD level is necessary regardless of whether the jamming solution uses a wideband noise signal to blanket the spectrum bands, which may be more effective for jamming frequency hopping systems, or uses a sweeping signal that rapidly sweeps across the bands to match unlicensed devices that use other modulation techniques, such as OFDM. Is the proposed 23 dBm/MHz EIRP level appropriate or should a lower limit be considered given that we anticipate that the antennas associated with jamming solutions will likely be located closer to a contraband device than a Wi-Fi hotspot? Would this power be sufficient for jamming solutions that are mounted behind a concrete wall and designed to radiate through the wall into inmate living spaces or should additional power be permitted in such instances? If so, what is the appropriate level of additional power and should it apply to all jamming solutions, recognizing that deployments must be customized to address the needs of each specific correctional facility?

243. In contrast, we note that in some bands used for Wi-Fi, specifically the 5.25-5.35 GHz, 5.47-5.725 GHz, 6.425-6.525 GHz, and 6.875-7.125 GHz bands, the maximum radiated power under part 15 is lower than other bands accommodating Wi-Fi operations.[737] In the 5.25-5.35 GHz and 5.47-5.725 GHz bands, this reduced power level equates to a maximum radiated power of 50 mW/MHz (17 dBm/MHz) EIRP, assuming a 20 megahertz channel bandwidth. The 6.425-6.525 GHz and 6.875-7.125 GHz bands also are subject to reduced power, with a maximum radiated power density of 5 dBm/MHz EIRP, though licensees are able to spread such power over significantly wider bandwidths, in some cases up to 320 megahertz wide channels.[738] We seek comment, in the alternative, on whether to apply the

[735] *See id*. §§ 15.247(b) and (c), 15.407. The 2.4 GHz, 5.15-5.25 GHz, 5.725-5.895, 5.925-6.425 GHz, and 6.525-6.875 GHz bands are currently subject to this power limit. *Id*. *See also* https://www.dell.com/support/contents/en-hr/article/product-support/self-support-knowledgebase/networking-Wi-FiWI-FI-and-bluetooth/wi-fi-network-standards-overview (last visited Oct. 26, 2026).

[736] U-NII devices are defined as "[i]ntentional radiators operating in the frequency bands 5.15-5.35 GHz, 5.47-5.895 GHz, and 5.925-7.125 GHz that use wideband digital modulation techniques and provide a wide array of high data rate mobile and fixed communications for individuals, businesses, and institutions." 47 CFR § 15.403.

[737] *See id*. §§ 15.407(a)(2), (a)(5), and (a)(6).

[738] *See id*. § 15.407 (a)(11).

corresponding lower radiated power limit (17 dBm/MHz EIRP) to jamming solutions operating in 5.25-5.35 GHz and 5.47-5.725 GHz bands, and 5 dBm/MHz EIRP for the 6.425-6.525 GHz and 6.875-7.125 GHz bands, or 17 dBm/MHz EIRP for all the bands. Would establishing lower limits in these bands, resulting in differing power levels across bands used for Wi-Fi applications, unnecessarily complicate the design and deployment of jamming solutions? Would different power levels have a material impact on the potential for authorized devices to receive harmful interference, given the requirement that jamming solutions need to limit emissions outside of jamming containment areas to ensure such a situation does not occur, as well as the differences in propagation and building penetration loss for various bands? We also seek comment on whether the existing peak and average power measurement techniques currently permitted for unlicensed devices should be applied to jamming solution transmitters. As jamming signals have unique characteristics that may be incompatible with existing measurement methods, do more suitable techniques need to be developed in this context?

244. We seek comment on whether our proposed radiated PSD limit approach would be appropriate for jamming solutions to address contraband unlicensed devices or should the power limits more closely align with the part 15 rules which in some instances specify an output power and maximum antenna gain[739] and in others specify only a maximum EIRP.[740] Is the proposed per megahertz power spectral density metric compatible with narrowband sweeping signals that may be used by some jamming solutions? If not, parties should make and support specific alternative proposals. Should we establish a maximum total power limit across all bands where unlicensed devices are targeted, or would a PSD limit ensure that jamming solutions use reasonable power levels? What are the trade-offs associated with these approaches and are there other options that may be more appropriate? If commenters support alternate approaches, are there concerns that a jamming solution could deploy a high gain, narrow beam antenna, albeit with lower output power? Does such a deployment pose additional risk of causing harmful interference to authorized users outside of jamming containment area(s)?

245. The Commission's part 15 rules for unlicensed operation in Wi-Fi bands apply different power limits in certain bands depending on whether the device operates indoors or outdoors.[741] We recognize that each jamming solution requires flexibility to custom engineer as necessary, and seek comment on whether jamming solution power limits should also vary across the unlicensed bands based on indoor/outdoor deployment scenarios. We are mindful that custom designed solutions will generally be deployed to use the minimum power necessary to achieve the desired goal, so as to minimize the impact on authorized devices outside of the jamming containment area(s). We also recognize that there are other licensed services in bands used for Wi-Fi (e.g., the 6 GHz band, which includes fixed point-to-point, broadcast auxiliary and temporary fixed news gathering operations, and the 5 GHz bands that accommodate federal radars in various locations), that have primary allocation status and are thus entitled to protection from harmful interference. Each jamming solutions deployment will therefore require careful engineering to ensure that it does not cause harmful interference to authorized users. We seek comment on whether this is the appropriate power limit for jamming solutions to effectively jam contraband wireless devices operating as part 15 devices in the bands discussed above. Should the radiated power limit we propose apply to each of the bands contained in mobile phones that are certified as unlicensed devices? If not, what power limit should be applied in each applicable band? Commenters should provide a thorough justification and technical details for power limits suggested in the record.

246. *Out-of-Band Emission Limits for Jamming Solutions that Target Unlicensed Devices.* We observe that the part 15 OOBE rules were created to accommodate a wide variety of devices, functions, and associated RF characteristics, and therefore vary depending on a number of factors, including the frequencies outside of the authorized channel on which the unwanted emissions fall,

[739] *See*, *e.g.*, *id*. § 15.407(a)(1) – (a)(3).

[740] *See*, *e.g.*, *id*. § 15.407(a)(7) – (a)(7).

[741] *See, e.g.*, *id*. § 15.407(a)(3).

whether the device is indoors or outdoors, and whether the radiated power is measured as peak or average. We also recognize that part 15 devices are designed to communicate using techniques that may not be directly applicable to jamming signals, such as spread spectrum, frequency hopping or digital modulation.[742]

247. We propose that, for the 2.4 GHz, 5 GHz, and 6 GHz unlicensed bands, jamming solution emissions outside the authorized band of operation must be suppressed to a level of at least -27 dBm/MHz EIRP. This OOBE limit currently applies to unlicensed devices operating across the 5 GHz and 6 GHz bands used by Wi-Fi devices, with some exceptions.[743] Regarding the 2.4 GHz band, the existing OOBE rule permits compliance with either a variable suppression requirement based upon in-band power, or a stringent limit of -41.3 dBm/MHz. Although the current variable OOBE rule is less restrictive than the -27 dBm/MHz we propose, depending on the radiated power used, we believe that, in this context, a fixed OOBE limit will provide regulatory certainty for designers of jamming solutions. Further, as jamming signals may take a variety of forms, application of a variable emission mask may have undetermined consequences. We believe the proposed OOBE limit is suitable for the extremely controlled environment of correctional facilities, with less need to account for the variety of Wi-Fi devices in the public domain. We seek comment on the proposed OOBE limit, including costs and benefits. Is this emission suppression level appropriate for jamming part 15 unlicensed operations in the noted bands? Is our assessment correct that current part 15 OOBE limits, with stair step masks and differing suppression levels required based on indoor vs. outdoor usage and device type, would not be appropriate to apply to jamming solutions because of differences in signal characteristics?

248. Recognizing that jamming signals may have to operate across multiple adjacent UNII bands, we believe applying a single OOBE is appropriate in this context, and that requiring licensees to meet differing emission limits for a range of adjacent bands, is unnecessarily complex. We seek comment on whether we should apply a less stringent emission mask in the 5.895-5.925 GHz band, used for cellular vehicle to everything (C-V2X)[744] in vehicles and along roadways, for jamming solutions that are limited to controlled environments. If commenters believe our proposal does not afford adequate protection, what are the appropriate OOBE limits for these solutions aimed at part 15 devices, and should they vary based upon indoor or outdoor applications, or should we apply different emission limits based upon where the unwanted emission falls outside of its authorized band? As an alternative, we seek comment on whether the Commission's OOBE limit of 43+10log(P) (equating to -13 dBm), commonly applied in wireless radio services, would adequately protect authorized operations.[745] Commenting parties should provide a detailed justification for any alternative proposal.

249. *Jamming Solutions in the 6 GHz Band*. We note that unlicensed operations in the 6 GHz band are subject to a range of additional Commission rules to promote sharing with fixed and broadcast auxiliary incumbent operations. In particular, standard power access point and fixed client devices must be equipped with geo-location capabilities and operations must comply with an automated frequency

[742] *See, e.g.*, *id*. §§ 15.247(d), 15.407(b).

[743] *See id*. § 15.407(b). For example, the UNII-3 band (5.725-5.825 GHz) requires -27 dBm/MHz 75 megahertz away from the band edge and includes a stair step mask of lesser suppression up to the band edge; the UNII-3 and the adjacent UNII-4 band (5.850-5.895 MHz) also requires a stair step mask and allows a lower suppression for indoor devices and different masks for client devices, subordinate device and indoor access points depending on the location of operation. *See id.* § 15.407(b)(4)-(5).

[744] C-V2X is defined in our rules as "[t]he use of cellular radio techniques to transfer data between roadside and on-board units or between on-board units to perform operations related to the improvement of traffic flow, traffic safety, and other Intelligent Transportation System applications in a variety of environments. C-V2X systems may also transmit status and instructional messages related to the units involved." *Id*. § 90.7.

[745] *See, e.g.*, *id*. §§ 22.359, 27.53, and 90.543.

coordination (AFC) system that can control the location, channels and power of the operating devices.[746] We tentatively conclude that jamming solutions proposed for authorized operation in the 6 GHz band, pursuant to part 90, subpart Z of the Commission's rules, should not be required to meet similar requirements, because use of an automated coordination system is solely for the purpose of facilitating coordination among multiple users in the 6 GHz band, and is arguably inapplicable to jamming devices deployed as part of a jamming solution to *prevent* contraband wireless device communications in that band in a limited area. We seek comment on this tentative conclusion. In addition, we note that C-V2X, including vehicular safety messages, operates in the lower adjacent band to 6 GHz unlicensed devices. As jamming signals under our framework are not permitted to cause harmful interference beyond the jamming containment area, we do not believe that C-V2X operations, even on roadways near correctional facilities, would be affected by jamming solutions. We seek comment, however, on whether additional protections are necessary in this context. Are there special considerations present in the 6 GHz band, including the presence of C-V2X, that support limiting jamming solutions in that band to indoor use, or alternatively only permitting outdoor use in a portion of the band?[747]

250. *Other Bands that Support Unlicensed Operations*. The record reflects that contraband wireless devices (i.e., mobile phones) are operating in the 2.4 GHz, 5 GHz, and 6 GHz bands with Wi-Fi calling and messaging features, and we therefore propose and seek further comment on technical parameters relating to those bands. We also seek comment on the extent to which contraband wireless devices are being used in correctional facilities that are operating in other bands on an unlicensed basis under part 15, for example, the 902-928 MHz band, the 60 GHz band (57-71 GHz), and the 90 GHz band (92-95 GHz). We seek to further develop the overall record on the types of devices used by inmates for communications, on what frequency bands, and on the appropriate technical limits to adopt, if jamming solutions were extended to such bands.

251. *RF Exposure*. Similar to other bands in which jamming solutions operate, we propose that jamming solutions targeting part 15 devices should be subject to the radio frequency radiation exposure requirements specified in sections 1.1307(b), 1.1310, 2.1091, and 2.1093 of the Commission's rules.[748] We seek comment on this proposal and whether other rules applicable to part 15 devices should also be applicable to jamming solutions that operate in those bands.[749]

B. Satellite Operations Under Part 100

252. In the *Third FNPRM*, the Commission sought comment on whether we should expand our deauthorization approach to enable jamming solutions that might address contraband wireless devices using part 25 satellite communications spectrum.[750] The Commission asked whether devices operating under part 25—not covered by the deauthorization rule—are a substantial problem in correctional facilities, and whether there are technologies that can block part 25 authorized transmissions.[751] The Commission also sought comment on the appropriate framework by which to authorize those technologies, and whether any of those technologies include functions that enable network connections

[746] *See id*. § 15.407(k).

[747] Recognizing that C-V2X operations are in the lower adjacent band, the Commission's 6 GHz device rules require very low power devices and geofenced variable power devices to prioritize operations on frequencies above 6.105 GHz prior to operating on frequencies between 5.925 GHz and 6.105 GHz. *See id*. § 15.407(d)(9).

[748] *Id*. §§ 15.407(f), 1.1307(b), 1.1310, 2.1091, and 2.1093.

[749] *See, e.g., id*. § 15.247(c) (requiring a reduction of power for antenna gains greater than 6 dBi); § 15.249(a) (limiting the field strength created by intentional radiators); § 15.407(d)(3) (restricting certain transmitters to indoor use).

[750] *See Third FNPRM*, 40 FCC Rcd at 8049, paras. 109; 8053, para. 119.

[751] *Id*. at 8053, para. 119.

for authorized devices that might be located in a correctional facility.[752] Regarding interference protection, the Commission asked how these technologies can protect other satellite services, including international satellite systems, from harmful interference.[753] Finally, assuming the deauthorization of contraband wireless device satellite communications authorized under part 25, the Commission sought comment on the appropriate approach to authorizing jamming solutions in the relevant bands.[754]

253. We seek further comment on these issues. As stated, in the *Space Modernization R&O*, the Commission reformed space and earth station licensing and operating rules by replacing part 25 with new part 100 rules.[755] The part 100 rules introduce changes to earth station licensing, and we seek comment on the implications of these rules in the context of the deauthorization of contraband wireless devices in correctional facilities.

254. The record reflects limited comment regarding the scope of inmate use of contraband devices operating on part 100 spectrum. CLA claims that inmates are now using satellite links to communicate using contraband wireless devices.[756] The South Carolina DOC asserts that it has evidence that satellite communications "have been discussed by inmates" as a way to use contraband wireless devices to communicate.[757] The Satellite Industry Association (SIA), in contrast, argues that jamming solutions specifically designed to operate across frequences allocated to satellite services, such as Mobile Satellite Service (MSS) or Fixed Satellite Service (FSS), are unnecessary as satellite phones or terminals have limited indoor coverage.[758] CTIA, while generally opposing jamming solutions, nonetheless contends that excluding non-commercial spectrum, including satellite spectrum, could create loopholes for those seeking to use contraband wireless devices.[759] Likewise, Verizon asserts that any jamming solution should cover all spectrum used for commercial wireless services, including MSS and FSS.[760]

255. We seek to avoid creating spectrum loopholes for inmates to exploit and find it appropriate to develop a robust record on contraband device communications through satellites. We therefore seek further comment on these issues, including the prevalence of satellite communications usage by inmates and current DOC efforts to document and deter any such usage. We ask commenters to specifically describe the nature of the problem and the types of devices inmates are using to communicate via satellite. Where are inmates using these devices, indoors or in outdoor spaces? Are the devices primarily satellite phones or devices using Direct-to-Device (D2D) technology? Is there evidence of other types of terminals operating as a contraband device on satellite frequencies?

256. We also seek further comment regarding the appropriate means to deauthorize the use of contraband wireless devices using satellite networks. In the *Third FNPRM*, the Commission pointed to Supplemental Coverage from Space (SCS) and the ancillary terrestrial component (ATC) of MSS as examples of spectrum that would not be affected by our amendment to section 1.903 (i.e., our deauthorization rule).[761] We seek additional comment on the current or anticipated use of wireless

---

[752] *Id*.

[753] *Id*.; *see* ITU Radio Regulation Nos. 0.4, 0.8, and 15.1 § 1.

[754] *Third FNPRM*, 40 FCC Rcd at 8053, para. 119.

[755] *See generally Space Modernization R&O*.

[756] CLA Comments at 10.

[757] South Carolina DOC Comments at 4.

[758] SIA Comments at 3, n.11.

[759] CTIA Reply at 13.

[760] Verizon Comments at 3.

[761] *Third FNPRM*, 40 FCC Rcd at 8049, para. 109, n.239. *See* 47 CFR §§ 25.115(q), 25.125(e) (licensing by rule as earth stations those terrestrial devices communicating with satellites on SCS bands); *id*. § 1.9005(jj) (ATC authority (continued….)

services provided using SCS and MSS (including ATC)[762] in correctional facilities. SCS bands include certain spectrum bands allocated and licensed exclusively on a terrestrial basis to enable transmissions from space stations to end-user devices.[763] We seek comment generally on how to extend our regulatory framework to address contraband device communications via satellite. How might such devices be deauthorized in this context, and how best to authorize jamming solutions to address this issue?

257. Under the part 100 approach, MSS handset portable devices, terrestrial mobile handset devices acting as earth stations, and hybrid terrestrial/earth station handset devices in certain circumstances are authorized under a license by rule framework.[764] These handset portable devices may communicate with a space station or satellite without the need for a separate earth station license or authorization so long as they meet specified requirements.[765] Devices operating under SCS rules and terrestrial mobile handset devices acting as earth stations,[766] using frequencies allocated primarily for terrestrial wireless services, are also licensed by rule so long as the devices show compliance with at least one of either part 22, 24, or 27 rules to provide SCS within the technical parameters and provisions associated with the device certification, and the device certification shows compliance with the licensed parameters of the terrestrial wireless license(s) and at least one of either part 22, 24, or 27.[767] Given this license by rule framework, we seek comment on the appropriate deauthorization approach to permit jamming operations, consistent with section 333 of the Act, to combat contraband wireless devices operating as earth stations pursuant to SCS authority. Should we amend the earth station licensing rule to exclude contraband wireless devices from the license by rule framework? Under this approach, similar to the deauthorization approach adopted in the *Third R&O*, contraband wireless devices in correctional facilities deemed contraband through a federal, state, or local law, or a correctional facility rule, regulation, or policy that prohibits the possession or operation of contraband wireless devices, would not be licensed by rule and would therefore not be authorized to communicate with satellites on terrestrial bands. Are there other approaches that we should consider?

258. With regard to the Commission's authority to authorize jamming of satellite communications, Public Knowledge argues that the same statutory arguments (including MQD concerns) it raises with regard to authorizing jamming on commercial spectrum apply to satellite spectrum as well.[768] SIA notes that 18 U.S.C. § 1367(a) prohibits causing interference to non-government satellite

(Continued from previous page)
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)). The issues discussed in this section are applicable to the current MSS and SCS rules.

[762] Common MSS bands include the "Big LEO" bands, which refer to low-earth orbit (LEO) MSS above one gigahertz, and "L-band," which refers to the entire frequency range from one to two gigahertz. Big LEO includes the 1610-1626.5 MHz and 2483.5-2500 MHz bands, designated through Commission rulemaking proceedings for use by non-geostationary satellite orbit (NGSO). L-band includes the "upper L-band" (1545-1559 MHz and 1646.5-1660.5 MHz) and "lower L-band" (1525-1544 MHz and 1626.5-1645.5 MHz), which are internationally allocated for MSS.

[763] *See SCS R&O*, 39 FCC Rcd 2622, 2634-35, para. 28. The following bands are available for provision of SCS: 600 MHz (614-652 MHz and 663-698 MHz), 700 MHz (698-769 MHz, 775 MHz-799 MHz, and 805-806 MHz), 800 MHz (824-849 MHz and 869-894 MHz), Broadband PCS (1850-1915 MHz and 1930-1995 MHz), and AWS-H Block (1915-1920 MHz and 1995-2000 MHz).

[764] *See Space Modernization R&O* at 35-37, paras. 93-96; 47 CFR § 100.120.

[765] 47 CFR § 100.120(b)(4)(b).

[766] *See id*. § 100.113.

[767] *See Space Modernization R&O* at 35-36, paras. 93-94; 47 CFR § 100.120(d)(2).

[768] Public Knowledge Comments at 11; *see supra* paras. [X-X].

transmissions without the authority of the satellite operator.[769] As described above, we believe that authorizing jamming solutions in correctional facilities does not rise to the level of economic or political importance that requires application of the major questions doctrine.[770] With respect to 18 U.S.C. § 1367, we recognize that there are limited circumstances under which intentional interference with authorized satellite operations is permitted.[771] We seek comment generally on our legal authority to authorize jamming solutions addressing satellite transmissions to contraband wireless devices. We also seek comment on whether congressional action is required to create an exemption for interference with satellite transmissions to contraband wireless devices in correctional facilities.

259. The record also reflects concern about potential interference from jamming solutions using satellite spectrum to authorized users of the spectrum.[772] SIA cautions that an RF jamming device would pose a greater risk to earth station receivers spread over a large geographic area than a jamming device operating at the same power level on terrestrial frequencies would pose to terrestrial receivers.[773] SIA explains that this is because satellite earth station receivers must "hear" signals that originate in space, so satellite services are particularly sensitive to co- and adjacent- channel interference from terrestrial jamming devices.[774] The GPS Innovation Alliance expresses concern that jamming solutions could introduce interference to public safety, transportation, and PNT applications that rely on MSS and other satellite spectrum.[775] Sirius XM is also concerned about potential interference from jamming operations to satellite transmissions.[776]

260. We seek comment on the specific technical requirements that should apply to jamming solutions intended to prevent contraband wireless device use on satellite spectrum to minimize the risk of harmful interference to authorized communications. We seek further comment on whether additional rules are required for jamming solutions directed at devices using part 100 satellite spectrum. To ensure that jamming solutions adequately protect authorized incumbent users operating on such spectrum from harmful interference, we seek comment on whether and how technical requirements and safeguards might differ from the rules adopted in the *Third R&O*. In addition to the commercial mobile broadband service bands on which we authorize jamming solutions today, on which specific additional bands used for satellite communications should we authorize jamming solutions? All spectrum bands used for satellite communications, or only on specified MSS bands? What technical rules should be implemented to limit the effects of satellite jamming solutions on satellite communications in areas adjacent to correctional facilities, where devices are authorized? Should jamming solution operators be required to meet specific interference protection obligations and what parameters are necessary to protect against harmful interference to authorized users of satellite spectrum bands? Is it viable to only jam the downlink portion of satellite bands that provide service to contraband devices, or is TDD technology prevalent or emerging in satellite-to-consumer services? Should jamming solution operators in satellite bands be required to meet specific interference protection obligations and what parameters such as EIRP, PSD, and/or elevation mask, are necessary to protect against harmful interference? We seek comment on the appropriate technical requirements for potential satellite jamming solutions, including costs and benefits.

[769] SIA Comments at 3-4, n.11.

[770] *See supra* paras. 60-62.

[771] *See* 18 U.S.C. § 1367.

[772] *See, e.g.*, SIA Comments at 3-5; GPSIA Comments at 4-5.

[773] SIA Comments at 3.

[774] *Id*.

[775] GPSIA Comments at 4-5.

[776] Sirius XM Reply at 3.

C. Additional Safeguards for Jamming Solutions

261. In the *Third R&O,* we require relevant wireless providers to notify overlay licensees and lessees of technical changes in the area where a jamming solution is deployed.[777] To facilitate effective jamming solutions and to reduce the risk of causing harmful interference to authorized users, we seek comment on whether to require such wireless providers to coordinate technical changes with overlay licensees at correctional facilities where a jamming solution is deployed. Such a coordination requirement could ensure that any changes are made in harmony with the continuous operation of a jamming solution and could further minimize the risk of harmful interference outside of the jamming containment area at a correctional facility. We seek comment on the extent to which such an approach would promote the contained operation of jamming solutions. Is a 15-mile coordination area, which would align with the area for which mandatory advanced notification is required to solutions providers for wireless provider technical changes, appropriate in this context? Would an alternative distance be more beneficial to the parties? We seek comment on the timing and duration of coordination, so as to facilitate efficient network adjustments and decrease the risk of harmful interference. To what extent should the Commission specify details of the coordination process? We seek comment on this additional safeguard and its implications.

262. The record reflects that jamming solutions are "highly dependent on local RF conditions," and can be more effective if deployed in weaker wireless provider signal strength environments.[778] Accordingly, we also seek comment on whether to apply to wireless providers a signal strength limit surrounding correctional facilities with deployed jamming solutions. Such an approach could result in jamming solutions requiring less radiated power to operate effectively, and could reduce the potential for negative impacts outside of the jamming containment area. We seek comment on what signal level limits would be appropriate in this context, and in what instances a wireless provider should be required to reduce signal levels surrounding a correctional facility. Should a signal strength limit be required only at correctional facilities located in rural areas? Commenters that favor an approach that would impose varying signal strength levels across different locales and RF environments should include technical analysis supporting their preferred solution.

263. Separately, we seek comment on whether we should consider adopting additional safeguards, for example potential compliance or monitoring obligations on lessees and licensees of jamming solutions to reduce the risk of harmful interference to authorized users outside of the jamming containment area, including vital public safety operations. We note that, in addition to FirstNet operations on Band 14, public safety agencies operate across various spectrum bands on Land Mobile Radio (LMR) systems. In the *Third R&O*, the Commission adopts rules implementing a regulatory framework authorizing jamming solutions on certain spectrum bands in correctional facilities, while subjecting the licensee or lessee to strict testing requirements and technical safeguards to ensure that jamming solutions do not cause harmful interference outside of the jamming containment areas. Are there additional protections, beyond those adopted in the *Third R&O*, that we should consider to specifically protect authorized public safety communications operating on LMR systems? If so, what types of additional protections would be effective in this regard? Should we consider specific additional compliance or monitoring obligations to ensure that public safety communications are protected outside of the jamming containment areas? Commenters seeking further safeguards should address the need for enhanced measures beyond the testing requirements, network monitoring requirement, interference resolution procedures, and annual certification rule adopted in the *Third R&O,* and why any suggested measures would further our goal of preventing harmful interference to authorized users, particularly public safety, from the operation of jamming solutions in correctional facilities.

[777] *See supra* paras. 106-07.

[778] *See* VT-ARC Report at 6-8, 91-92.

D. Quiet Zones

264. In the *Third R&O*, the Commission notes that it has, throughout this proceeding, maintained a policy of technology neutrality by seeking comment on a range of interdiction solutions in an effort to provide additional tools to the corrections community to combat contraband wireless devices in correctional facilities.[779] The Commission sought comment in the *Third FNPRM* on whether it could support the development of other device-based interdiction solutions such as geofencing or beacon technology.[780] The Commission also asked generally whether there are other technologies, beyond those identified as "handset-centric," that could be used to combat contraband devices in correctional facilities.[781] In the *Third R&O,* we find it in the public interest to create a regulatory framework to authorize jamming solutions at this time, but we do not preclude stakeholders from exploring market-based solutions under our existing rules.[782] Although we decline at this time to adopt rules or other regulatory changes to support other interdiction technologies, in this *Fourth FNPRM*, we seek to refresh the record on the concept of establishing "quiet zones" in and around correctional facilities, which the Commission has previously raised in this proceeding.[783]

265. The Commission has described "quiet zones" in the correctional facility context as areas in and around correctional facilities in which wireless communications are not authorized such that contraband wireless devices in the area would not receive service from a wireless provider.[784] While some commenters in this proceeding support the concept of quiet zones, others have argued that quiet zones—or "dead zones"—are infeasible to engineer without disrupting authorized users, costly, or otherwise not a complete solution.[785] We seek updated comment on whether there have been technological advancements in the wireless providers' network engineering such that today it may be more feasible to precisely define quiet zones in and around correctional facilities. We seek comment on the complexities involved in wireless provider engineering of quiet zones surrounding correctional facilities. We seek comment on whether such an approach would nonetheless allow inmates to continue to use the features of contraband wireless devices in some capacity. As an alternative to mandating quiet zones in this context, are there other ways in which the Commission could support voluntary wireless provider action to implement quiet zones?

266. We also seek comment on the appropriate technical criteria to use to define a quiet zone (e.g., field strength limit). How would the adoption of technical parameters affect network design to provide service in areas located outside the quiet zone? Beyond the geographical location of the correctional facility, should we consider other features of correctional facilities in determining the parameters of quiet zones? Are additional safeguards required to ensure that authorized users outside of the quiet zones would not experience harmful interference? We seek specific comment on the costs and benefits of establishing quiet zones in and around correctional facilities, including experience in other contexts and technical analyses.

---

[779] *See supra* paras. 212-14.

[780] *Third FNPRM*, 40 FCC Rcd at 8059-61, paras. 134-38.

[781] *Id*. at 8063, para. 144.

[782] *See supra* para. 214.

[783] In the *Second FNPRM*, the Commission sought further comment on an approach suggested by certain commenters whereby the Commission would establish quiet zones in and around correctional facilities. *See Second FNPRM*, 36 FCC Rcd at 11843, para. 77 (citing the *First FNPRM*, 32 Rcd at 2380-81, paras. 123-27).

[784] *See Second FNPRM*, 36 FCC Rcd at 11843-44, para. 77.

[785] *Id*.; s*ee also First FNPRM*, 32 FCC Rcd at 2380-81, paras. 123-27.

V. PROCEDURAL MATTERS

267. *Regulatory Flexibility Act*. The Regulatory Flexibility Act of 1980, as amended (RFA),[786] 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."[787] Accordingly, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule and policy changes contained in this *Third Report and Order* on small entities. The FRFA is set forth in Appendix C.

268. The Commission has also prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the potential impact of rule and policy changes contained in this *Fourth Further Notice of Proposed Rulemaking*. The IRFA is set forth in Appendix D. 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 *Fourth Further Notice of Proposed Rulemaking* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

269. *Paperwork Reduction Act*. This *Third Report and Order* may contain new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. All such requirements will be submitted to the Office of Management and Budget (OMB) for review under section 3507(d) of the PRA. OMB, the general public, and other federal agencies will be invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, we note that, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. § 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. This *Fourth 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.[788] 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.

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

271. *Providing Accountability Through Transparency Act*. Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of *the Fourth Further Notice of Proposed Rulemaking* is available on https://www.fcc.gov/proposed-rulemakings.

272. *Ex Parte Presentations.* The proceeding this *Fourth Further Notice of Proposed Rulemaking* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the

[786] 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).

[787] *Id.* § 605(b).

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

Commission's *ex parte* rules.[789] 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.

273. *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 *Fourth Further Notice of Proposed Rulemaking*.

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

274. *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).

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

[789] 47 CFR § 1.1200 *et seq.*

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

VI. ORDERING CLAUSES

277. 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, that this *Third Report and Order and Fourth Further Notice of Proposed Rulemaking* IS HEREBY ADOPTED.[790]

278. IT IS FURTHER ORDERED that the rules and requirements as adopted herein ARE ADOPTED, effective thirty (30) days after publication in the Federal Register; provided, however, that sections 1.949(e)(5), 1.9041(c), 1.9041(d), 1.9041(e), 1.9041(k), 1.9041(m)(1), 1.9041(n), 1.9041(o), 20.23(c), 20.23(e), 90.1407, 90.1409, 90.1411, 90.1417, 90.1427, 90.1435, and 90.1437 of the Commission's rules, which contain new or modified information collection requirements that require review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act, will not become effective until the effective date for those information collections is announced in a document published in the Federal Register after the Commission receives OMB approval. The Commission directs the Bureau to issue such document and to cause sections 1.949(e)(5), 1.9041(c), 1.9041(d), 1.9041(e), 1.9041(k), 1.9041(m)(1), 1.9041(n), 1.9041(o), 20.23(c), 20.23(e), 90.1407, 90.1409, 90.1411, 90.1417, 90.1427, 90.1435, and 90.1437 to be revised accordingly.

279. IT IS FURTHER ORDERED that the Commission's Office of the Secretary SHALL SEND a copy of this *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, including the Final Regulatory Flexibility Analysis and Initial Regulatory Flexibility Analysis, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[790] Pursuant to Executive Order 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993), as amended by Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 24, 2025), this regulatory action has been determined to be significant under section 3(f)(1) of Executive Order 12866 and has been reviewed by the Office of Management and Budget.

APPENDIX A

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 1, 2, 15, 20, 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 1.929 is amended by adding paragraph (l) to read as follows:

§ **1.929 Classification of filings as major or minor.**

* * * * *

(l) In addition to those changes listed in paragraph (a) of this section, a request by an overlay license of a jamming solution to increase the size of the jamming containment area, as defined in § 90.1401 of this chapter, is a major change.

4. Section 1.949 is amended by adding paragraph (e)(5) to read as follows:

§ 1.949 Application for renewal of authorization.

* * * * *

(e) *Safe harbors*. * * *

(5) An applicant for renewal of an overlay license for a jamming solution must certify that it remains eligible to hold the overlay license at the specified correctional facility, and that it continues to operate consistent with its authorization to provide jamming operations at the specified correctional facility.

* * * * *

5. Section 1.953 is amended by revising paragraph (a) to read as follows:

§ 1.953 Discontinuance of service or operations.

(a) *Termination of authorization*. A licensee's authorization will automatically terminate, without specific Commission action, if the licensee permanently discontinues service or operations under the license during the license term. A licensee is subject to this provision commencing on the date it is required to be providing service or operating. An overlay licensee of a jamming solution, as defined in § 90.1401 of this chapter, is not subject to this provision.

* * * * *

6. Section 1.9003 is amended by revising the definition of "Contraband Interdiction System" to read as follows:

§ 1.9003 Definitions.

* * * * *

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 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. A Contraband Interdiction System does not include a Jamming Solution, as defined in § 90.1401 of this chapter.

* * * * *

7. Section 1.9020 is amended by revising paragraph (a) to read as follows:

§ 1.9020 Spectrum manager leasing arrangements.

(a) *Overview.* Under the provisions of this section, a licensee (in any of the included services) and a spectrum lessee, except for a lessee of a jamming solution as defined in § 90.1401 of this chapter, may enter into a spectrum manager leasing arrangement, without the need for prior Commission approval, provided that the licensee retains *de jure* control of the license and *de facto* control, as defined and explained in this subpart, of the leased spectrum. The licensee must notify the Commission of the spectrum leasing arrangement pursuant to the rules set forth in this section. The term of a spectrum manager leasing arrangement may be no longer than the term of the license authorization.

* * * * *

8. Section 1.9030 is amended by revising paragraph (e) to read as follows:

§ 1.9030 Long-term *de facto* transfer leasing arrangements.

* * * * *

(e) *Applications for long-term de facto transfer leasing arrangements.* Applications for long-term *de facto* transfer leasing arrangements will be processed either pursuant to the general approval procedures or the immediate approval procedures, as discussed herein, except that such applications for a jamming solution, as defined in § 90.1401 of this chapter, must be processed pursuant to the general

approval procedures. Spectrum leasing parties must submit the application by electronic filing using ULS and FCC Form 608, and obtain Commission consent prior to consummating the transfer of *de facto* control of the leased spectrum, except that parties falling within the provisions of § 1.913(d) may file the application either electronically or manually.

* * * * *

9. Section 1.9035 is amended by revising paragraph (e) to read as follows:

§ 1.9035 Short-term de facto transfer leasing arrangements.

* * * * *

(e) *Spectrum leasing application.* Short-term *de facto* transfer leasing arrangements will be processed pursuant to immediate approval procedures, as discussed herein, except that such applications for a jamming solution, as defined in § 90.1401 of this chapter, must be processed pursuant to the general approval procedures described in § 1.9030(e)(1) of this chapter. Parties entering into a short-term *de facto* transfer leasing arrangement are required to file an electronic application with the Commission, using FCC Form 608, and obtain Commission consent prior to consummating the transfer of *de facto* control of the leased spectrum, except that parties falling within the provisions of § 1.913(d) may file the application either electronically or manually.

* * * * *

10. Section 1.9041 is added to read as follows:

§ 1.9041 Special provisions relating to spectrum leasing arrangements involving jamming solutions in correctional facilities.

(a) *Eligibility criteria.* An entity seeking Commission approval as lessee in a *de facto* transfer spectrum leasing arrangement under this section must be either a department of corrections with authority over the correctional facility for which the lease is sought, or an entity that has entered into a contract with a department of corrections with authority over the correctional facility for which the lease is sought.

(b) *Bands available.* The bands available for *de facto* transfer spectrum leasing arrangements for jamming solutions in correctional facilities are the following: 617-652 MHz, 716-728 MHz, 728-746 MHz, 746-757 MHz, 757-758 MHz, 758-769 MHz, 788-799 MHz, 862-869 MHz, 869-894 MHz, 935-940 MHz, 1390-1392 MHz, 1392-1395 MHz, 1432-1435 MHz, 1670-1675 MHz, 1695-1710 MHz, 1930-1990 MHz, 1995-2000 MHz, 2110-2180 MHz, 2180-2200 MHz, 2305-2315 MHz, 2315-2320 MHz, 2345-2350 MHz, 2350-2360 MHz, 2496-2690 MHz, 3450-3550 MHz, 3550-3700 MHz, 3700-4140 MHz, and the frequency bands listed in § 30.4 of this chapter in the Upper Microwave Flexible Use Service.

(c) *Proof of concept test*. Prior to seeking authority to engage in a *de facto* transfer spectrum leasing as a lessee under this section, an eligible entity must successfully complete a proof of concept test at a correctional facility pursuant to an experimental license granted under part 5 of this chapter. The entity must provide seven days' advance notice of the test to the First Responder Network Authority, as defined in 47 U.S.C. 1424, and all relevant wireless providers, as defined in § 20.23(b)(3)(i) of this chapter, and allow them the opportunity to participate.

(d) *Application requirements.* An entity seeking to engage in spectrum leasing as a lessee under this section must include the following as attachments to FCC Form 608:

(1) Proof of concept test results demonstrating that the jamming solution does not cause harmful interference to authorized devices located outside the jamming containment area, and that the test was representative of, and scalable to, the jamming solution to be deployed under the authorization sought;

(2) Proof that advance notification was given to the First Responder Network Authority, as defined in 47 U.S.C. 1424, and the relevant wireless providers regarding the proof of concept test, and identification of any such entities that attended the test;

(3) The name and address of the correctional facility with which it has a contract where the jamming solution will be deployed;

(4) The requested frequency bands of operation;

(5) Certification that it meets the eligibility requirements and seeks to deploy a jamming solution; and

(6) A description of the jamming solution, a shapefile and visual representation of the jamming containment area associated with the proposed operations within which the jamming solution impact will be contained, such that harmful interference will not occur to authorized users located outside of that area, including public safety users, and the methodology as to how the applicant will deploy the jamming solution to not cause harmful interference to authorized devices, including test locations, complete deployed system configuration, technical parameters, and measurable protection criteria.

(e) *Pre-operational test*. After grant of a *de facto* transfer spectrum lease to operate a jamming solution under this section, but prior to commencing operations, a lessee under this section must successfully complete testing at the correctional facility at which the lessee intends to operate using jamming devices that have obtained equipment authorization under part 2 of this chapter prior to commencing jamming operations. The lessee must provide seven days' advance notice of the test to the First Responder Network Authority (FirstNet), as defined in 47 U.S.C. 1424, all relevant wireless providers, as defined in § 20.23(b)(3)(i) of this chapter, the relevant Statewide Interoperability Coordinator (SWIC) or equivalent representative, and the relevant Public Safety Answering Point (PSAP) as defined in § 9.3 of this chapter, or 911 Authority as defined in § 9.28 of this chapter, to allow them the opportunity to participate in the test. This notification must include the anticipated date of commencement of jamming operations and a point of contact capable of deactivating the jamming solution. Following the test, the lessee must file a notification under its lease in the Universal Licensing System that includes:

(1) Certification that on-site, pre-operational testing at the specific correctional facility was complete and successful when applying the selected protection criteria in accordance with the consented to lease application;

(2) Proof that all jamming devices used as part of the jamming solution had appropriate equipment authorizations pursuant to part 2 of this chapter, including applicable FCC IDs.; and

(3) Proof of seven days' advance notification to FirstNet, the relevant wireless providers, relevant SWIC or equivalent representative, and relevant PSAP or 911 Authority, and identification of any of these entities that participated in the pre-operational testing.

(f) *Effective date of spectrum leasing arrangement*. Notwithstanding the provisions of §§ 1.9030(f) and 1.9035(f), a *de facto* transfer spectrum lessee authorized to provide a jamming solution will be authorized to commence operations on the next business day following the filing of the pre-operational test notification.

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

(h) *Construction/performance requirements.* Notwithstanding the provisions of § 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.

(i) *Termination of spectrum leasing arrangement.* Notwithstanding the provisions of §§ 1.9030(g) and 1.9035(h), a *de facto* spectrum leasing arrangement entered into for purpose of the operation of a

jamming solution in a correctional facility will automatically terminate if the lessee has a contract with the department of corrections that expires or is terminated.

(j) *Interference-related rules*. Notwithstanding the provisions of § 1.9030(d)(1), a *de facto* spectrum lessee must comply with the following interference-related and technical rules applicable to spectrum lessees authorized to provide jamming solutions in correctional facilities contained in part 90, subpart Z of this chapter: §§ 90.1421, 90.1423, 90.1425, 90.1427, 90.1431, and 90.1433.

(k) *Community notification requirement*. Ten days prior to deploying a jamming solution, a *de facto* transfer spectrum lessee must notify the community in which the correctional facility is located. The notification must include a description of what the system is intended to do, the date the system is scheduled to begin operating, and the location of the correctional facility. Notification must be tailored to reach the community immediately adjacent to the correctional facility, including through television, radio, Internet news sources, or community groups, as may be appropriate. No notification is required under this subsection when conducting a proof of concept test pursuant to § 1.9041(c), or pre-operational test pursuant to § 1.9041(e), of a jamming solution prior to deployment.

(l) *Lease Modification*. A *de facto* transfer spectrum lessee that deploys a jamming solution, as defined in § 90.1401 of this part, must file a lease modification application if the size of the jamming containment area, as defined in § 90.1401 of this part, increases.

(m) *FirstNet*. The following provisions shall apply to spectrum leasing arrangements for the 758-769/788-799 MHz spectrum band (Band 14) involving the First Responder Network Authority (FirstNet), as defined in 47 U.S.C. 1424:

(1) An entity seeking to engage in spectrum leasing as a lessee under this section and obtain authority to operate on Band 14 must include as an attachment to FCC Form 608, in addition to the information required by § 1.9041(d), a demonstration that it has an agreement with FirstNet to operate on Band 14 to deploy a jamming solution at the specified correctional facility. If the entity is filing more than one lease application for the specified correctional facility, this attachment need only accompany the lead lease application.

(2) A lessee of spectrum to operate a jamming solution that is authorized to operate on Band 14 is subject to the condition that Band 14 may not be jammed if FirstNet otherwise prevents contraband wireless device access to Band 14 in the jamming containment area.

(n) *Notification to jamming solution lessees of wireless provider technical changes*. Wireless providers leasing spectrum to jamming solution operators must provide 90 days' advance notice to jamming solution operator lessees of the following network changes occurring within 15 miles of the correctional facility:

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

(2) Deploying a new air interface technology or changing an existing air interface technology;

(3) Adding, relocating, or removing a site; and/or

(4) Changing a radiated power level at a site.

(o) *Annual certification*. A lessee of a jamming solution deployed at a specific correctional facility must annually file a notification under its lease in the Universal Licensing System, commencing one year after the date the pre-operational test notification, required by § 1.9041(e) of this section, is filed,

certifying that the deployed jamming solution continues to operate as authorized and does not cause harmful interference outside the jamming containment area.

PART 2 – FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

11. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336, unless otherwise noted.

12. Section 2.106 is amended by:

a. Revising pages 30–33, 35-41, 54, 55, 58, and 59 of the Table of Frequency Allocations; and

b. Adding paragraph (c)(XXX).

The revisions and addition read as follows:

§ 2.106 Table of Frequency Allocations.

* * * * *

5.149 5.291A 5.294 5.296 5.300 5.304 5.306 5.312	614-698 BROADCASTING Fixed Mobile 5.293 5.308 5.308A 5.309		614-890	614-698 FIXED MOBILE Mobile-satellite NG33A NG5 NG14 NG33 NG115 NG149 US566	RF Devices (15) Satellite Communications (25) Wireless Communications (27) LPTV, TV Translator/Booster (74G Low Power Auxiliary (74H) Private Land Mobile (90)
694-790 MOBILE except aeronautical mobile 5.312A 5.317A BROADCASTING	698-806 MOBILE 5.317A BROADCASTING Fixed			698-758 FIXED MOBILE Mobile-satellite NG33A NG159 US566	 Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G) Private Land Mobile (90)
				758-775 FIXED MOBILE Mobile-satellite NG33A NG34 NG159 US566	 Satellite Communications (25) Public Safety Land Mobile (90R) Private Land Mobile (90)
				775-788 FIXED MOBILE Mobile-satellite NG33A NG159	 Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G)
5.300 5.312				788-805 FIXED MOBILE Mobile-satellite NG33A NG34 NG159 US566	 Satellite Communications (25) Public Safety Land Mobile (90R) Private Land Mobile (90)
790-862 FIXED MOBILE except aeronautical mobile 5.316B 5.317A BROADCASTING				805-806 FIXED MOBILE Mobile-satellite NG33A NG159	 Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G)
	5.293 5.309				
	806-890 FIXED MOBILE 5.317A BROADCASTING			806-809 LAND MOBILE	 Public Safety Land Mobile (90S)
				809-849 FIXED LAND MOBILE Mobile-satellite NG33A	 Public Mobile (22) Satellite Communications (25) Private Land Mobile (90)
				849-851 AERONAUTICAL MOBILE	 Public Mobile (22)
				851-854 LAND MOBILE	 Public Safety Land Mobile (90S)
5.312 5.319					

862-890 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 5.319 5.323	5.317 5.318	5.149 5.305 5.306 5.307 5.320		854-894 FIXED LAND MOBILE Mobile-satellite NG33A US116 US268 US566	Public Mobile (22) Satellite Communications (25) Private Land Mobile (90)

Table of Frequency Allocations 894-1400 MHz (UHF)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
890-942 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 Radiolocation	890-902 FIXED MOBILE except aeronautical mobile 5.317A Radiolocation 5.318 5.325	890-942 FIXED MOBILE 5.317A BROADCASTING Radiolocation	890-902 US116 US268 G2	(See previous page) 894-896 AERONAUTICAL MOBILE US116 US268 896-901 FIXED MOBILE except aeronautical mobile US116 US268 901-902 FIXED MOBILE US116 US268	 Public Mobile (22) Wireless Communications (27) Private Land Mobile (90) Personal Communications (24)
	902-928 FIXED Amateur Mobile except aeronautical mobile 5.325A Radiolocation 5.150 5.325 5.326		902-928 RADIOLOCATION G59 5.150 US218 US267 US275 G11	902-928 5.150 US218 US267 US275	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Amateur Radio (97)
	928-942 FIXED MOBILE except aeronautical mobile 5.317A Radiolocation		928-932	928-929 FIXED US116 US268 NG35 929-930 FIXED LAND MOBILE US116 US268 930-931 FIXED MOBILE	Public Mobile (22) Private Land Mobile (90) Fixed Microwave (101) Private Land Mobile (90) Personal Communications (24)

				US116 US268	
			US116 US268 G2	931-932 FIXED LAND MOBILE US116 US268	Public Mobile (22)
			932-935 FIXED US268 G2	932-935 FIXED US268 NG35	Public Mobile (22) Fixed Microwave (101)
			935-941	935-940 FIXED MOBILE except aeronautical mobile US116 US268 US566	Wireless Communications (27) Private Land Mobile (90)
			US116 US268 G2	940-941 FIXED MOBILE US116 US268	Personal Communications (24
5.323	5.325	5.327			
942-960 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 5.323	942-960 FIXED MOBILE 5.317A	942-960 FIXED MOBILE 5.317A BROADCASTING 5.320	941-944 FIXED US84 US268 US301 G2 944-960	941-944 FIXED US84 US268 US301 NG30 NG35 944-960 FIXED NG35	Public Mobile (22) Aural Broadcast Auxiliary (74E) Low Power Auxiliary (74H) Fixed Microwave (101)
960-1164 AERONAUTICAL MOBILE (R) 5.327A AERONAUTICAL RADIONAVIGATION 5.328 5.328AA			960-1164 AERONAUTICAL MOBILE (R) 5.327A AERONAUTICAL RADIONAVIGATION 5.328 5.328AA US78 US224		Aviation (87)
1164-1215 AERONAUTICAL RADIONAVIGATION 5.328 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.328A			1164-1215 AERONAUTICAL RADIONAVIGATION 5.328 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328A US224		
1215-1240 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.329 5.329A SPACE RESEARCH (active) 5.330 5.331 5.332			1215-1240 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) G132 SPACE RESEARCH (active) 5.332	1215-1240 Earth exploration-satellite (active) Space research (active)	

1240-1300 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.329 5.329A SPACE RESEARCH (active) Amateur 5.282 5.330 5.331 5.332 5.335 5.335A		1240-1300 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 SPACE RESEARCH (active) AERONAUTICAL RADIONAVIGATION 5.332 5.335	1240-1300 AERONAUTICAL RADIONAVIGATION Amateur Earth exploration-satellite (active) Space research (active) 5.282	Amateur Radio (97)
1300-1350 RADIOLOCATION AERONAUTICAL RADIONAVIGATION 5.337 RADIONAVIGATION-SATELLITE (Earth-to-space) 5.149 5.337A		1300-1350 AERONAUTICAL RADIONAVIGATION 5.337 Radiolocation G2 US342	1300-1350 AERONAUTICAL RADIONAVIGATION 5.337 US342	Aviation (87)
1350-1400 FIXED MOBILE RADIOLOCATION	1350-1400 RADIOLOCATION 5.338A	1350-1390 FIXED MOBILE RADIOLOCATION G2 5.334 5.339 US342 US385 G27 G114	1350-1390 5.334 5.339 US342 US385	
		1390-1395 5.339 US79 US342 US385	1390-1395 FIXED MOBILE except aeronautical mobile 5.339 US79 US342 US385 NG338A US566	Wireless Communications (27) Private Land Mobile (90)
5.149 5.338 5.338A 5.339	5.149 5.334 5.339	1395-1400 LAND MOBILE (medical telemetry and medical telecommand) 5.339 US79 US342 US385		Personal Radio (95)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
1400-1427 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340 5.341			1400-1427 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) 5.341 US246		
1427-1429 SPACE OPERATION (Earth-to-space) FIXED MOBILE except aeronautical mobile 5.341A 5.341B 5.341C 5.338A 5.341			1427-1429.5 LAND MOBILE (medical telemetry and medical telecommand) US350 5.341 US79	1427-1429.5 LAND MOBILE (telemetry and telecommand) Fixed (telemetry) 5.341 US79 US350 NG338A	Private Land Mobile (90) Personal Radio (95)
1429-1452 FIXED MOBILE except aeronautical mobile 5.341A	1429-1452 FIXED MOBILE 5.341B 5.341C 5.343		1429.5-1432 5.341 US79 US350	1429.5-1432 FIXED (telemetry and telecommand) LAND MOBILE (telemetry and telecommand) 5.341 US79 US350 NG338A	

			1432-1435 5.341 US83	1432-1435 FIXED MOBILE except aeronautical mobile 5.341 US83 NG338A US566	Wireless Communications (27) Private Land Mobile (90)
5.338A 5.341 5.342	5.338A 5.341		1435-1525 MOBILE (aeronautical telemetry) US338A		Aviation (87)
1452-1492 FIXED MOBILE except aeronautical mobile 5.346 BROADCASTING BROADCASTING-SATELLITE 5.208B 5.341 5.342 5.345	1452-1492 FIXED MOBILE 5.341B 5.343 5.346A BROADCASTING BROADCASTING-SATELLITE 5.208B 5.341 5.344 5.345				
1492-1518 FIXED MOBILE except aeronautical mobile 5.341A 5.341 5.342	1492-1518 FIXED MOBILE 5.341B 5.343 5.341 5.344	1492-1518 FIXED MOBILE 5.341C 5.341			
1518-1525 FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341 5.342	1518-1525 FIXED MOBILE 5.343 MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341 5.344	1518-1525 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341	5.341 US84 US343		
1525-1530 SPACE OPERATION (space-to-Earth) FIXED MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Mobile except aeronautical mobile 5.349 5.341 5.342 5.350 5.351 5.352A 5.354	1525-1530 SPACE OPERATION (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Fixed Mobile 5.343 5.341 5.351 5.354	1525-1530 SPACE OPERATION (space-to-Earth) FIXED MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Mobile 5.349 5.341 5.351 5.352A 5.354	1525-1535 MOBILE-SATELLITE (space-to-Earth) US315 US380		Satellite Communications (25) Maritime (80)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
1626.5-1660 MOBILE-SATELLITE (Earth-to-space) 5.351A 5.341 5.351 5.353A 5.354 5.355 5.357A 5.359 5.362A 5.374 5.375 5.376			1626.5-1660 MOBILE-SATELLITE (Earth-to-space) US308 US309 US315 US380 5.341 5.351 5.375		Satellite Communications (25) Maritime (80) Aviation (87)
1660-1660.5 MOBILE-SATELLITE (Earth-to-space) 5.351A RADIO ASTRONOMY 5.149 5.341 5.351 5.354 5.362A 5.376A			1660-1660.5 MOBILE-SATELLITE (Earth-to-space) US308 US309 US380 RADIO ASTRONOMY 5.341 5.351 US342		Satellite Communications (25) Aviation (87)
1660.5-1668 RADIO ASTRONOMY SPACE RESEARCH (passive) Fixed Mobile except aeronautical mobile 5.149 5.341 5.379 5.379A			1660.5-1668.4 RADIO ASTRONOMY US74 SPACE RESEARCH (passive)		

1668-1668.4 MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.379C RADIO ASTRONOMY SPACE RESEARCH (passive) Fixed Mobile except aeronautical mobile 5.149 5.341 5.379 5.379A		5.341 US246		
1668.4-1670 METEOROLOGICAL AIDS FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.379C RADIO ASTRONOMY 5.149 5.341 5.379D 5.379E		1668.4-1670 METEOROLOGICAL AIDS (radiosonde) RADIO ASTRONOMY US74 5.341 US99 US342		
1670-1675 METEOROLOGICAL AIDS FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.341 5.379D 5.379E 5.380A		1670-1675 5.341 US211 US362	1670-1675 FIXED MOBILE except aeronautical mobile 5.341 US211 US362 US566	Wireless Communications (27) Private Land Mobile (90)
1675-1690 METEOROLOGICAL AIDS FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.341		1675-1695 METEOROLOGICAL AIDS (radiosonde) METEOROLOGICAL-SATELLITE (space-to-Earth) US88 5.341 US211 US289		
1690-1700 METEOROLOGICAL AIDS METEOROLOGICAL-SATELLITE (space-to-Earth) Fixed Mobile except aeronautical mobile 5.289 5.341 5.382	1690-1700 METEOROLOGICAL AIDS METEOROLOGICAL-SATELLITE (space-to-Earth) 5.289 5.341 5.381	1695-1710 METEOROLOGICAL-SATELLITE (space-to-Earth) US88	1695-1710 FIXED MOBILE except aeronautical mobile	Wireless Communications (27) Private Land Mobile (90)
1700-1710 FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.289 5.341	1700-1710 FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.289 5.341 5.384	5.341	5.341 US88 US566	
1710-1930 FIXED MOBILE 5.384A 5.388A 5.388B 5.149 5.341 5.385 5.386 5.387 5.388		1710-1761 5.341 US91 US378 US385 1761-1780 SPACE OPERATION	1710-1780 FIXED MOBILE 5.341 US91 US378 US385	

			(Earth-to-space) G42 US91		
			1780-1850 FIXED MOBILE SPACE OPERATION (Earth-to-space) G42	1780-1850	
1930-1970 FIXED MOBILE 5.388A 5.388B 5.388	1930-1970 FIXED MOBILE 5.388A 5.388B Mobile-satellite (Earth-to-space) 5.388	1930-1970 FIXED MOBILE 5.388A 5.388B 5.388	1850-2025	1850-2000 FIXED MOBILE Mobile-satellite NG33A US566	RF Devices (15) Personal Communications (24) Satellite Communications (25 Wireless Communications (27) Private Land Mobile (90) Fixed Microwave (101)
1970-1980 FIXED MOBILE 5.388A 5.388B 5.388					
1980-2010 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) 5.351A 5.388 5.389A 5.389B 5.389F				2000-2020 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space)	Satellite Communications (25) Wireless Communications (27)
2010-2025 FIXED MOBILE 5.388A 5.388B 5.388	2010-2025 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) 5.388 5.389C 5.389E	2010-2025 FIXED MOBILE 5.388A 5.388B 5.388		2020-2025 FIXED MOBILE	
2025-2110 SPACE OPERATION (Earth-to-space) (space-to-space) EARTH EXPLORATION-SATELLITE (Earth-to-space) (space-to-space) FIXED MOBILE 5.391 SPACE RESEARCH (Earth-to-space) (space-to-space) 5.392			2025-2110 SPACE OPERATION (Earth-to-space) (space-to-space) EARTH EXPLORATION-SATELLITE (Earth-to-space) (space-to-space) SPACE RESEARCH (Earth-to-space) (space-to-space) FIXED MOBILE 5.391 5.392 US90 US92 US222 US346 US347	2025-2110 FIXED NG118 MOBILE 5.391 Space Operation (Earth-to-space) US94 5.392 US90 US92 US222 US346 US347	Space Launch Services (26) TV Auxiliary Broadcasting (74F) Cable TV Relay (78) Local TV Transmission (101J)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
2110-2120 FIXED MOBILE 5.388A 5.388B SPACE RESEARCH (deep space) (Earth-to-space)			2110-2120	2110-2120 FIXED MOBILE	Public Mobile (22) Wireless Communications (27) Private Land Mobile (90)

<table>
<tr><td colspan="3">5.388</td><td>US252</td><td>US252 US566</td><td>Fixed Microwave (101)</td></tr>
<tr><td>2120-2170
FIXED
MOBILE 5.388A 5.388B

5.388</td><td>2120-2160
FIXED
MOBILE 5.388A 5.388B
Mobile-satellite (space-to-Earth)
5.388
2160-2170
FIXED
MOBILE
MOBILE-SATELLITE (space-to-Earth)
5.388 5.389C 5.389E</td><td>2120-2170
FIXED
MOBILE 5.388A 5.388B

5.388</td><td rowspan="3">2120-2200</td><td>2120-2180
FIXED
MOBILE

NG41 US566</td><td></td></tr>
<tr><td colspan="3">2170-2200
FIXED
MOBILE
MOBILE-SATELLITE (space-to-Earth) 5.351A
5.388 5.389A 5.389F</td><td>2180-2200
FIXED
MOBILE
MOBILE-SATELLITE (space-to-Earth)

US566</td><td>Satellite Communications (25)
Wireless Communications (27)
Private Land Mobile (90)</td></tr>
<tr><td colspan="3">2200-2290
SPACE OPERATION (space-to-Earth) (space-to-space)
EARTH EXPLORATION-SATELLITE (space-to-Earth) (space-to-space)
FIXED
MOBILE 5.391
SPACE RESEARCH (space-to-Earth) (space-to-space)

5.392</td><td>2200-2290
SPACE OPERATION (space-to-Earth) (space-to-space) US96
EARTH EXPLORATION-SATELLITE (space-to-Earth) (space-to-space)
FIXED (line-of-sight only)
MOBILE (line-of-sight only including aeronautical telemetry, but excluding flight testing of manned aircraft) 5.391
SPACE RESEARCH (space-to-Earth) (space-to-space)

5.392 US303</td><td>2200-2290

US96 US303</td><td>Space Launch Services (26)</td></tr>
<tr><td colspan="3">2290-2300
FIXED
MOBILE except aeronautical mobile
SPACE RESEARCH (deep space) (space-to-Earth)</td><td>2290-2300
FIXED
MOBILE except aeronautical mobile
SPACE RESEARCH (deep space) (space-to-Earth)</td><td>2290-2300
SPACE RESEARCH (deep space) (space-to-Earth)</td><td></td></tr>
<tr><td>2300-2450
FIXED
MOBILE 5.384A
Amateur
Radiolocation</td><td>2300-2450
FIXED
MOBILE 5.384A
RADIOLOCATION
Amateur</td><td></td><td>2300-2305

G122</td><td>2300-2305
Amateur</td><td>Amateur Radio (97)</td></tr>
<tr><td colspan="3"></td><td>2305-2310

US97 G122</td><td>2305-2310
FIXED
MOBILE except aeronautical mobile
RADIOLOCATION
Amateur
US97 US566</td><td>Wireless Communications (27)
Private Land Mobile (90)
Amateur Radio (97)</td></tr>
</table>

		2310-2320 Fixed Mobile US100 Radiolocation G2 US97 US327	2310-2320 FIXED MOBILE BROADCASTING-SATELLITE RADIOLOCATION US97 US100 US327 US566	Wireless Communications (27) Private Land Mobile (90)
		2320-2345 Fixed Radiolocation G2 US327	2320-2345 BROADCASTING-SATELLITE US327	Satellite Communications (25)
		2345-2360 Fixed Mobile US100 Radiolocation G2 US327	2345-2360 FIXED MOBILE US100 BROADCASTING-SATELLITE RADIOLOCATION US327 US566	Wireless Communications (27) Private Land Mobile (90)
		2360-2390 MOBILE US276 RADIOLOCATION G2 G120 Fixed US101	2360-2390 MOBILE US276 Space Operation (Earth-to-space) (space-to-Earth) NG42 US101	Space Launch Services (26) Aviation (87) Personal Radio (95)
		2390-2395 MOBILE US276 US101	2390-2395 AMATEUR MOBILE US276 Space Operation (Earth-to-space) (space-to-Earth) NG42 US101	Space Launch Services (26) Aviation (87) Personal Radio (95) Amateur Radio (97)
		2395-2400 US101 G122	2395-2400 AMATEUR US101	Personal Radio (95) Amateur Radio (97)
		2400-2417 5.150 G122	2400-2417 AMATEUR 5.150 5.282	RF Devices (15) ISM Equipment (18) Amateur Radio (97)
		2417-2450 Radiolocation G2 5.150	2417-2450 Amateur 5.150 5.282	
5.150 5.282 5.395	5.150 5.282 5.393 5.394			
2450-2483.5 FIXED MOBILE Radiolocation 5.150	2450-2483.5 FIXED MOBILE RADIOLOCATION 5.150	2450-2483.5 5.150 US41	2450-2483.5 FIXED MOBILE Radiolocation 5.150 US41	RF Devices (15) ISM Equipment (18) TV Auxiliary Broadcasting (74F) Private Land Mobile (90 Fixed Microwave (101)

Table of Frequency Allocations		2483.5-3600 MHz (UHF/SHF)			Page 39
International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 Radiolocation 5.398A 5.150 5.399 5.401 5.402	2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIOLOCATION RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402	2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIOLOCATION RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.401 5.402	2483.5-2500 MOBILE-SATELLITE (space-to-Earth) US319 US380 US391 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402 US41	2483.5-2495 MOBILE-SATELLITE (space-to-Earth) US380 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402 US41 US319 NG147 2495-2500 FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (space-to-Earth) US380 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402 US41 US319 US391 NG147 US566	ISM Equipment (18) Satellite Communications (25) ISM Equipment (18) Satellite Communications (25) Wireless Communications (27) Private Land Mobile (90)
2500-2520 FIXED 5.410 MOBILE except aeronautical mobile 5.384A 5.412	2500-2520 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A 5.404	2500-2520 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A MOBILE-SATELLITE (space-to-Earth) 5.351A 5.407 5.414 5.414A 5.404 5.415A	2500-2655	2500-2655 FIXED US205 MOBILE except aeronautical mobile	Wireless Communications (27) Private Land Mobile (90)
2520-2655 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.412 5.418B 5.418C	2520-2655 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.418B 5.418C	2520-2535 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.403 5.414A 5.415A 2535-2655 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.418 5.418A 5.418B 5.418C	5.339 US205	5.339 US566	

2655-2670 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.208B 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.412	2655-2670 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.208B	2655-2670 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.208B 5.420	2655-2690 Earth exploration-satellite (passive) Radio astronomy US385 Space research (passive)	2655-2690 FIXED US205 MOBILE except aeronautical mobile Earth exploration-satellite (passive) Radio astronomy Space research (passive)	
2670-2690 FIXED 5.410 MOBILE except aeronautical mobile 5.384A Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.412	2670-2690 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.208B 5.415 MOBILE except aeronautical mobile 5.384A Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149	2670-2690 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) 5.415 MOBILE except aeronautical mobile 5.384A MOBILE-SATELLITE (Earth-to-space) 5.351A 5.419 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149	US205	US385 US566	
2690-2700 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340 5.422			2690-2700 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) US246		
2700-2900 AERONAUTICAL RADIONAVIGATION 5.337 Radiolocation 5.423 5.424			2700-2900 METEOROLOGICAL AIDS AERONAUTICAL RADIONAVI-GATION 5.337 US18 Radiolocation G2 5.423 G15	2700-2900 5.423 US18	Aviation (87)
2900-3100 RADIOLOCATION 5.424A RADIONAVIGATION 5.426 5.425 5.427			2900-3100 RADIOLOCATION 5.424A G56 MARITIME RADIONAVIGATION 5.427 US44 US316	2900-3100 MARITIME RADIONAVIGATION Radiolocation US44 5.427 US316	Maritime (80) Private Land Mobile (90)
3100-3300 RADIOLOCATION Earth exploration-satellite (active) Space research (active) 5.149 5.428			3100-3300 RADIOLOCATION G59 Earth exploration-satellite (active) Space research (active) US342	3100-3300 Earth exploration-satellite (active) Space research (active) Radiolocation US342	Private Land Mobile (90)

3300-3400 RADIOLOCATION 5.149 5.429 5.429A 5.429B 5.430	3300-3400 RADIOLOCATION Amateur Fixed Mobile 5.149 5.429C 5.429D	3300-3400 RADIOLOCATION Amateur 5.149 5.429 5.429E 5.429F	3300-3500 RADIOLOCATION US431B G2	3300-3450 US103 US342	
3400-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.430A Radiolocation 5.282 5.431	3400-3500 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.431A 5.431B Amateur Radiolocation 5.433 5.282	3400-3500 FIXED FIXED-SATELLITE (space-to-Earth) Amateur Mobile 5.432 5.432B Radiolocation 5.433 5.282 5.432A	US103 US342	3450-3600 FIXED MOBILE except aeronautical mobile US103 US105 US431B US433 US566	Wireless Communi-cations (27) Citizens Broadband (96) Private Land Mobile (90)

International Table			United States Table		
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	FCC Rule Part(s)
3400-3600 MHz: see previous page	3500-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.431B Radiolocation 5.433	3500-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.433A Radiolocation 5.433	3500-3550 RADIOLOCATION G59 AERONAUTICAL RADIONAVIGATION (ground-based) G110 US103 US431B 3550-3650 RADIOLOCATION G59 AERONAUTICAL RADIONAVIGATION (ground-based) G110 US105 US107 US245 US433 3650-3700 US109 US349	3500-3600 MHz: see previous page 3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) US107 US245 NG169 MOBILE except aeronautical mobile US105 US109 US349 US433 US566	
3600-4200 FIXED FIXED-SATELLITE (space-to-Earth) Mobile	3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.434 Radiolocation 5.433	3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile Radiolocation 5.435			Satellite Communications (25) Private Land Mobile (90) Citizens Broadband (96)
	3700-4200 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile		3700-4200	3700-4160 FIXED MOBILE except aeronautical mobile NG182 NG457A US566 4160-4200 FIXED	Wireless Communications (27) Private Land Mobile (90) Satellite

		FIXED-SATELLITE (space-to-Earth) NG457A NG182	Communications (25)
4200-4400 AERONAUTICAL MOBILE (R) 5.436 AERONAUTICAL RADIONAVIGATION 5.438 5.437 5.439 5.440	4200-4400 AERONAUTICAL RADIONAVIGATION 5.440 US261		Aviation (87)
4400-4500 FIXED MOBILE 5.440A	4400-4940 FIXED MOBILE	4400-4500	
4500-4800 FIXED FIXED-SATELLITE (space-to-Earth) 5.441 MOBILE 5.440A		4500-4800 FIXED-SATELLITE (space-to-Earth) 5.441 US245	
4800-4990 FIXED MOBILE 5.440A 5.441A 5.441B 5.442 Radio astronomy 5.149 5.339 5.443	US113 US245 US342	4800-4940 US113 US342	
	4940-4990 5.339 US342 US385 G122	4940-4990 FIXED MOBILE except aeronautical mobile 5.339 US342 US385	Public Safety Land Mobile (90Y)
4990-5000 FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY Space research (passive) 5.149	4990-5000 RADIO ASTRONOMY US74 Space research (passive) US246		
22-22.21 FIXED MOBILE except aeronautical mobile 5.149	22-22.21 FIXED MOBILE except aeronautical mobile US342		
22.21-22.5 EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY SPACE RESEARCH (passive) 5.149 5.532	22.21-22.5 EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY SPACE RESEARCH (passive) US342 US532		
22.5-22.55 FIXED MOBILE	22.5-22.55 FIXED MOBILE US211		
22.55-23.15 FIXED INTER-SATELLITE 5.338A MOBILE SPACE RESEARCH (Earth-to-space) 5.532A 5.149	22.55-23.15 FIXED INTER-SATELLITE US145 US278 MOBILE SPACE RESEARCH (Earth-to-space) 5.532A US342		Satellite Communications (25) Fixed Microwave (101)
23.15-23.55 FIXED	23.15-23.55 FIXED		

INTER-SATELLITE 5.338A MOBILE			INTER-SATELLITE US145 US278 MOBILE		
23.55-23.6 FIXED MOBILE			23.55-23.6 FIXED MOBILE		Fixed Microwave (101)
23.6-24 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340			23.6-24 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) US246		
24-24.05 AMATEUR AMATEUR-SATELLITE 5.150			24-24.05 5.150 US211	24-24.05 AMATEUR AMATEUR-SATELLITE 5.150 US211	ISM Equipment (18) Amateur Radio (97)
24.05-24.25 RADIOLOCATION Amateur Earth exploration-satellite (active) 5.150			24.05-24.25 RADIOLOCATION G59 Earth exploration-satellite (active) 5.150	24.05-24.25 Amateur Earth exploration-satellite (active) Radiolocation 5.150	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Amateur Radio (97)
24.25-24.45 FIXED MOBILE except aeronautical mobile 5.338A 5.532AB	24.25-24.45 FIXED 5.532AA MOBILE except aeronautical mobile 5.338A 5.532AB RADIONAVIGATION	24.25-24.45 FIXED MOBILE 5.338A 5.532AB RADIONAVIGATION	24.25-24.45	24.25-24.45 FIXED MOBILE US146 US566	RF Devices (15) Upper Microwave Flexible Use (30) Private Land Mobile (90)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
24.45-24.65 FIXED INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB	24.45-24.65 FIXED 5.532AA INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB RADIONAVIGATION 5.533	24.45-24.65 FIXED INTER-SATELLITE MOBILE 5.338A 5.532AB RADIONAVIGATION 5.533	24.45-24.65 INTER-SATELLITE RADIONAVIGATION 5.533		RF Devices (15) Satellite Communications (25)
24.65-24.75 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB	24.65-24.75 FIXED 5.532AA INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB RADIOLOCATION-SATELLITE (Earth-to-space)	24.65-24.75 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B INTER-SATELLITE MOBILE 5.338A 5.532AB	24.65-24.75 INTER-SATELLITE RADIOLOCATION-SATELLITE (Earth-to-space)		
24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B MOBILE except aeronautical mobile 5.338A 5.532AB	24.75-25.25 FIXED 5.532AA FIXED-SATELLITE (Earth-to-space) 5.535 MOBILE except aeronautical mobile 5.338A 5.532AB	24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) 5.535 MOBILE 5.338A 5.532AB	24.75-25.25	24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE US146 NG65 US566	RF Devices (15) Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile

					(90)
25.25-25.5 FIXED 5.534A INTER-SATELLITE 5.536 MOBILE 5.338A 5.532AB Standard frequency and time signal-satellite (Earth-to-space)			25.25-25.5 FIXED INTER-SATELLITE 5.536 MOBILE Standard frequency and time signal-satellite (Earth-to-space)	25.25-25.5 Inter-satellite 5.536 Standard frequency and time signal-satellite (Earth-to-space)	RF Devices (15)
25.5-27 EARTH EXPLORATION-SATELLITE (space-to-Earth) 5.536B FIXED 5.534A INTER-SATELLITE 5.536 MOBILE 5.338A 5.532AB SPACE RESEARCH (space-to-Earth) 5.536C Standard frequency and time signal-satellite (Earth-to-space) 5.536A			25.5-27 EARTH EXPLORATION-SATELLITE (space-to-Earth) FIXED INTER-SATELLITE 5.536 MOBILE SPACE RESEARCH (space-to-Earth) Standard frequency and time signal-satellite (Earth-to-space) 5.536A US258	25.5-27 SPACE RESEARCH (space-to-Earth) Inter-satellite 5.536 Standard frequency and time signal-satellite (Earth-to-space) 5.536A US258	
27-27.5 FIXED INTER-SATELLITE 5.536 MOBILE 5.338A 5.532AB	27-27.5 FIXED 5.534A FIXED-SATELLITE (Earth-to-space) INTER-SATELLITE 5.536 5.537 MOBILE 5.338A 5.532AB		27-27.5 FIXED INTER-SATELLITE 5.536 MOBILE	27-27.5 Inter-satellite 5.536	
27.5-28.5 FIXED 5.537A FIXED-SATELLITE (Earth-to-space) 5.484A 5.516B 5.517A 5.539 MOBILE 5.538 5.540			27.5-30	27.5-28.35 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE US566	RF Devices (15) Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile (90) Fixed Microwave (101)
				28.35-29.1 FIXED-SATELLITE (Earth-to-space) NG165 NG527A	RF Devices (15) Satellite Communications (25)
37-37.5 FIXED MOBILE except aeronautical mobile 5.550B SPACE RESEARCH (space-to-Earth) 5.547			37-38 FIXED MOBILE except aeronautical mobile SPACE RESEARCH (space-to-Earth)	37-37.5 FIXED MOBILE except aeronautical mobile US151 US566	Upper Microwave Flexible Use (30) Private Land Mobile (90)
37.5-38 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C MOBILE except aeronautical mobile 5.550B SPACE RESEARCH (space-to-Earth) Earth exploration-satellite (space-to-Earth) 5.547			US151	37.5-38 FIXED FIXED-SATELLITE (space-to-Earth) NG63 MOBILE except aeronautical mobile US151 US566	Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile (90)
38-39.5 FIXED 5.550D FIXED-SATELLITE (space-to-Earth) 5.550C			38-38.6 FIXED MOBILE	38-39.5 FIXED FIXED-SATELLITE (space-to-Earth)	

MOBILE 5.550B Earth exploration-satellite (space-to-Earth) 5.547			38.6-39.5	NG63 MOBILE NG175 US566	
39.5-40 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C MOBILE 5.550B MOBILE-SATELLITE (space-to-Earth) Earth exploration-satellite (space-to-Earth) 5.547 5.550E			39.5-40 FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) US382 G117	39.5-40 FIXED FIXED-SATELLITE (space-to-Earth) NG63 MOBILE NG175 US382 US566	
40-40.5 EARTH EXPLORATION-SATELLITE (Earth-to-space) FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C MOBILE 5.550B MOBILE-SATELLITE (space-to-Earth) SPACE RESEARCH (Earth-to-space) Earth exploration-satellite (space-to-Earth) 5.550E			40-40.5 EARTH EXPLORATION-SATELLITE (Earth-to-space) FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) SPACE RESEARCH (Earth-to-space) Earth exploration-satellite (space-to-Earth) G117	40-40.5 FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth)	Satellite Communications (25)
40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547	40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile Mobile-satellite (space-to-Earth) 5.547	40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547	40.5-41 FIXED-SATELLITE (space-to-Earth) Mobile-satellite (space-to-Earth) US211 G117	40.5-41 FIXED-SATELLITE (space-to-Earth) BROADCASTING BROADCASTING-SATELLITE Fixed Mobile Mobile-satellite (space-to-Earth) US211	
41-42.5 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547 5.551F 5.551H 5.551I			41-42.5 US211	41-42 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE BROADCASTING BROADCASTING-SATELLITE US211	Page 58

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
41-42.5 GHz: see previous page			41-42.5 GHz: see previous page	42-42.5 FIXED MOBILE US211	

42.5-43.5 FIXED FIXED-SATELLITE (Earth-to-space) 5.552 MOBILE except aeronautical mobile 5.550B RADIO ASTRONOMY 5.149 5.547	42.5-43.5 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE except aeronautical mobile RADIO ASTRONOMY US342	42.5-43.5 RADIO ASTRONOMY US342	
43.5-47 MOBILE 5.553 5.553A MOBILE-SATELLITE RADIONAVIGATION RADIONAVIGATION-SATELLITE	43.5-45.5 FIXED-SATELLITE (Earth-to-space) MOBILE-SATELLITE (Earth-to-space) G117	43.5-45.5	
	45.5-46.9 MOBILE MOBILE-SATELLITE (Earth-to-space) RADIONAVIGATION-SATELLITE 5.554		
5.554	46.9-47 MOBILE MOBILE-SATELLITE (Earth-to-space) RADIONAVIGATION-SATELLITE 5.554	46.9-47 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) RADIONAVIGATION-SATELLITE 5.554	
47-47.2 AMATEUR AMATEUR-SATELLITE	47-48.2	47-47.2 AMATEUR AMATEUR-SATELLITE	Amateur Radio (97)
47.2-47.5 FIXED FIXED-SATELLITE (Earth-to-space) 5.550C 5.552 MOBILE 5.553B 5.552A		47.2-48.2 FIXED FIXED-SATELLITE (Earth-to-space) US297 MOBILE	Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile (90)
47.5-47.9 FIXED FIXED-SATELLITE (Earth-to-space) 5.550C 5.552 (space-to-Earth) 5.516B 5.554A MOBILE 5.553B	47.5-47.9 FIXED FIXED-SATELLITE (Earth-to-space) 5.550C 5.552 MOBILE 5.553B		
47.9-48.2 FIXED FIXED-SATELLITE (Earth-to-space) 5.550C 5.552 MOBILE 5.553B 5.552A		NG65 US566	

* * * * *

(c) * * *

(XXX) USXXX A jamming solution may be authorized subject to part 90, subpart Z of this chapter to prevent the operation of wireless devices in correctional facilities deemed contraband through a federal, state, or local law, or a correctional facility rule, regulation, or policy. Jamming solution operation is permitted under a primary allocation in the fixed and land mobile services, limited to an authorized jamming containment area within a correctional facility. Operation beyond the authorized jamming containment area is strictly prohibited, is on a non-interference basis, and shall not cause harmful interference to authorized services or devices.

* * * * *

PART 5 – EXPERIMENTAL RADIO SERVICE

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

Authority: 47 U.S.C. 154, 301, 302, 303, 307, 336.

14. Section 5.3 is amended by redesignating paragraph (m) to paragraph (n), adding a new paragraph (m) and revising redesignated paragraph (m) to read as follows:

§ 5.3 Scope of service.

* * * * *

(m) Proof of concept testing for jamming devices used in jamming solutions as defined in § 90.1401 of this chapter and conducted pursuant to § 90.1407 of this chapter.

(n) Types of experiments that are not specifically covered under paragraphs (a) through (m) of this section will be considered upon demonstration of need for such additional types of experiments.

15. Section 5.84 is revised to read as follows:

§ 5.84 Non-interference criterion.

Operation of an experimental radio station is permitted only on the condition that harmful interference is not caused to any authorized station operating in accordance with the Table of Frequency Allocation of part 2 of this chapter. If harmful interference to authorized stations within an established radio service occurs, upon becoming aware of such harmful interference the Experimental Radio Service licensee shall immediately cease transmissions. Furthermore, the licensee shall not resume transmissions until the licensee establishes to the satisfaction of the Commission that further harmful interference will not be caused to any established radio service.

PART 15 – RADIO FREQUENCY DEVICES

16. 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.

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

§ 15.5 General conditions of operation.

* * * * *

(e) Operation of a jamming device as part of a jamming solution, as defined in § 90.1401 of this chapter, is prohibited under this part, even under a power level that complies with the limits set forth in this part. A jamming solution must be authorized pursuant to §§ 1.9041 or part 90, subpart Z of this chapter, or a combination thereof.

18. 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 § 90.1401 of this chapter, is not eligible for certification under part 15 pursuant to the Commission's part 2, subpart J Equipment Authorization Procedures, and must be so authorized pursuant to part 90, subpart Z of this chapter.

PART 20 – COMMERCIAL MOBILE SERVICES

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

Authority: 47 U.S.C. 47 U.S.C. 151, 152(a), 154(i), 155, 157, 160, 201, 214, 222, 251(e), 301, 302a, 303, 303(b), 303(r), 307, 307(a), 309, 309(j)(3), 316, 316(a), 332, 610, 615, 615a, 615b, and 615c, unless otherwise noted.

20. Section 20.23 is amended by revising paragraph (c) and adding paragraph (e) to read as follows:

§ 20.23 Contraband wireless devices in correctional facilities.

* * * * *

(c) *Disabling contraband wireless devices*. A DCFO may request that a CMRS licensee disable a contraband wireless device that has been detected in a correctional facility by a CIS that has been certified in accordance with paragraph (b) of this section. Absent objections from a wireless provider, as described under paragraph (b)(4) of this section, the DCFO may submit a qualifying request to a wireless provider beginning on the date the Wireless Telecommunications Bureau updates the Commission's website to reflect certification of the CIS at the correctional facility subject of the self-certification filing described in paragraph (b)(3)(ii) of this section or recertification of the CIS through the filing described in paragraph (b)(5) of this section.

* * * * *

(e) *Notification to jamming solution licensees of wireless provider technical changes.*

(1) All relevant wireless providers must provide 90 days' advance notice to jamming solution licensees, as defined in § 90.1401 of this chapter, of the following network changes occurring within 15 miles of a correctional facility where a jamming solution has been deployed:

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

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

(iii) Adding, relocating, or removing a site; and/or

(iv) Changing a radiated power level at a site.

(2) For purposes of this rule, relevant wireless providers include any wireless provider holding a license that:

(i) Authorizes operation on the frequencies on which a jamming solution overlay licensee seeks to operate a jamming solution; and

(ii) Authorizes service in the geographic area (e.g., census tract, county, Partial Economic Area (PEA), Economic Area (EA), Cellular Market Area (CMA), Regional Economic Area Grouping (REAG)) within which a correctional facility is located where a department of corrections or solutions provider seeks to deploy a jamming solution.

PART 90 – PRIVATE LAND MOBILE RADIO SERVICES

21. 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.

22. Section 90.155 is amended by revising paragraph (a) to read as follows:

§ 90.155 Time in which station must be placed in operation.

(a) All stations authorized under this part, except as provided in §§ 90.528, 90.529, 90.629, 90.631(f), 90.655, 90.685, and subpart Z of this part, must be placed in operation within twelve (12) months from the date of grant or the authorization cancels automatically and must be returned to the Commission.

23. Section 90.217 is amended by revising the introductory paragraph to read as follows:

§ 90.217 Exemption from technical standards.

Except as noted herein, jamming solutions, as defined in § 90.1401 of this part, are exempt from the technical requirements of this subpart, but are subject to the technical requirements set forth in subpart Z of this part. Except as noted herein, transmitters used at stations licensed below 800 MHz on any frequency listed in subparts B and C of this part or licensed on a business category channel above 800 MHz which have an output power not exceeding 120 milliwatts are exempt from the technical requirements set out this subpart, but must instead comply with the following:

* * * * *

24. Subpart Z is added to read as follows:

Subpart Z Regulations Governing Overlay Licensing of Jamming Solutions.

§ 90.1401 Definitions.

Terms used in this subpart have the following meanings:

Jamming Containment Area. The geographic area(s) of a correctional facility within which possession of a contraband wireless devices is a violation of federal, state, or local law, or a correctional facility rule, regulation, or policy; where a jamming solution is authorized; and outside of which the jamming solution must not cause harmful interference to authorized devices.

Jamming Device. A transmitter within a correctional facility (as defined in § 1.9003 of this chapter) that prevents a contraband wireless device (as defined in § 1.9003 of this chapter) from establishing or maintaining a radio link by overwhelming the contraband wireless device with RF energy.

Jamming Solution. A system authorized for use only at a correctional facility that is comprised of one or more Jamming Device(s), as defined in this section, and associated elements.

§ 90.1403 Eligibility.

An entity is eligible to apply for an overlay license for the provision of a jamming solution under this subpart if it is a department of corrections with authority over the correctional facility for which the license is sought, or an entity that has entered into a contract with a department of corrections with authority over the correctional facility for which the license is sought.

§ 90.1405 Bands available.

The bands available for overlay licensing for jamming solutions in correctional facilities are the following: 617-652 MHz, 716-728 MHz, 728-746 MHz, 746-757 MHz, 757-758 MHz, 758-769 MHz, 788-799 MHz, 862-869 MHz, 869-894 MHz, 935-940 MHz, 1390-1392 MHz, 1392-1395 MHz, 1432-1435 MHz, 1670-1675 MHz, 1695-1710 MHz, 1930-1990 MHz, 1995-2000 MHz, 2110-2180 MHz, 2180-2200 MHz, 2305-2315 MHz, 2315-2320 MHz, 2345-2350 MHz, 2350-2360 MHz, 2496-2690 MHz, 3450-3550 MHz, 3550-3700 MHz, 3700-4140 MHz, and the frequency bands listed in § 30.4 of this chapter in the Upper Microwave Flexible Use Service.

§ 90.1407 Proof of concept test.

Prior to seeking authorization for an overlay license to operate a jamming solution under this section, an eligible entity must successfully complete a proof of concept test at a correctional facility pursuant to an experimental license granted under part 5 of this chapter. The entity must provide seven days' advance notice of the test to the First Responder Network Authority, as defined in 47 U.S.C. 1424, and all relevant wireless providers, as defined in § 20.23(b)(3)(i) of this chapter, and allow them the opportunity to participate.

§ 90.1409 Application requirements.

An overlay license applicant seeking authority to provide a jamming solution in a correctional facility must apply using FCC Form 601 in 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 the following as attachments to its FCC Form 601:

(1) Proof of concept test results demonstrating that the jamming solution does not cause harmful interference to authorized devices located outside the jamming containment area, and that the test was representative of, and scalable to, the jamming solution to be deployed under the authorization sought;

(2) Proof that advance notification was given to the First Responder Network Authority, as defined in 47 U.S.C. 1424, and the relevant wireless providers regarding the proof of concept test, and identification of any such entities that attended the test;

(3) The name and address of the correctional facility with which it has a contract where the jamming solution will be deployed;

(4) The requested frequency bands of operation;

(5) Certification that it meets the eligibility requirements and seeks to deploy a jamming solution; and

(6) A description of the jamming solution, a shapefile and visual representation of the jamming containment area associated with the proposed operations within which the jamming solution impact will be contained, such that harmful interference will not occur to authorized users located outside of that area, including public safety users, and the methodology as to how the applicant will deploy the jamming solution to not cause harmful interference to authorized devices, including the complete deployed system configuration, technical parameters, test locations, and measurable protection criteria.

§ 90.1411 Authorization of jamming solutions.

(a) *Pre-operational test*. After a licensee is granted an overlay license to operate a jamming solution under this section, but prior to commencing operations, a licensee under this section must successfully complete testing at the correctional facility at which the licensee intends to operate using jamming devices that have obtained equipment authorization under part 2 of this chapter prior to commencing jamming operations. The licensee must provide seven days' advance notice of the test to the First Responder Network Authority (FirstNet), as defined in 47 U.S.C. 1424, to all relevant wireless providers, as defined in § 20.23(b)(3)(i) of this chapter, the relevant Statewide Interoperability Coordinator (SWIC) or equivalent representative, and the relevant PSAP as defined in § 9.3 of this chapter or 911 Authority, as defined in § 9.28 of this chapter, to allow them the opportunity to participate in the test. This notification must include the anticipated date of commencement of jamming operations and a point of contact capable of deactivating the jamming solution. Following the test, the licensee must file a notification under its license in the Universal Licensing System that includes:

(1) Certification that on-site, pre-operational testing at the specific correctional facility was complete and successful when applying the selected protection criteria in accordance with the granted license application;

(2) Proof that all jamming devices used as part of the jamming solution had appropriate equipment authorizations pursuant to part 2 of this chapter, including applicable FCC IDs.; and

(3) Proof of seven days' advance notification to FirstNet, the relevant wireless providers, relevant SWIC or equivalent representative, and relevant PSAP or 911 Authority, and identification of any of these entities that participated in the pre-operational testing.

(b) *Effectiveness of authorization*. The licensee of a jamming solution will be authorized to commence operations on the next business day following the filing of the pre-operational test notification.

(c) *FirstNet*. The licensee of a jamming solution that is authorized to operate on the 758-769/788-799 MHz band is subject to the condition that these bands may not be jammed if the First Responder Network Authority (FirstNet), as defined in 47 U.S.C. 1424, otherwise prevents contraband wireless device access to these bands in the jamming containment area.

§ 90.1413 License term.

An initial authorization for a jamming solution license will have a term not to exceed ten years from the date of initial issuance or renewal. The license will automatically terminate if the licensee has a contract with a department of corrections for the relevant correctional facility that expires or is terminated by the parties.

§ 90.1415 Special limitation on applications for assignment of license.

Notwithstanding § 1.948 of this chapter, a license to operate a jamming solution may not be assigned, unless the assignment is non-substantial (*pro forma*). Notwithstanding § 1.950 of this chapter, a

license to operate a jamming solution may not be partitioned or disaggregated to another party. A licensee may seek approval to transfer control of its license by filing FCC Form 603 in the Commission's Universal Licensing System (ULS) in accordance with part 1, subpart F.

§ 90.1417 Community notification requirement.

Ten days prior to deploying a jamming solution, a licensee must notify the community in which the correctional facility is located. The notification must include a description of what the system is intended to do, the date the system is scheduled to begin operating, and the location of the correctional facility. Notification must be tailored to reach the community immediately adjacent to the correctional facility, including through television, radio, Internet news sources, or community groups, as may be appropriate. No notification is required under this subsection when conducting a proof of concept test pursuant to § 90.1407, or pre-operational test pursuant to § 90.1411, of a jamming solution prior to deployment.

§ 90.1419 Power limits.

(a) Jamming solutions operating in the bands listed in § 90.1405 of this part shall not exceed the following power spectral density (PSD) limits:

(1) In bands below 1 GHz, the maximum radiated PSD shall not exceed 18 dBm/MHz Equivalent Isotropic Radiated Power (EIRP).

(2) In bands above 1 GHz, the maximum radiated PSD shall not exceed 24 dBm/MHz EIRP.

(b) Jamming solution providers shall use the minimum power necessary to effectively prevent communications solely within the licensed jamming containment area.

(c) *Power measurement*. Measurement of the EIRP of jamming solution transmitters may be performed using peak or average measurement techniques. Average power measurements shall not exceed a peak-to-average ratio (PAR) of 13 dB.

(1) For guidance on proper average measurement techniques, parties should consult a Commission-approved measurement technique (see FCC Laboratory's Knowledge Database); and

(2) For purposes of this section, peak transmit power must be measured over an interval of continuous transmission using instrumentation calibrated in terms of an rms-equivalent voltage. The measurement results shall be properly adjusted for any instrument limitations, such as detector response times, limited resolution bandwidth capability when compared to the emission bandwidth, sensitivity, etc., so as to obtain a true peak measurement for the emission in question over the full bandwidth of the channel.

§ 90.1421 Emission limits.

(a) In the bands listed in § 90.1405 of this part, the power of any emission outside a jamming solution frequency band(s) of operation shall be attenuated in accordance with the corresponding rule governing the target band for jamming:

(1) For jamming solutions operating in 600 MHz, 700 MHz (with the exception of 758-769 MHz and 788-799 MHz), 2100 MHz, 2300 MHz, 2500 MHz, 3450 MHz, and 3700 MHz, refer to the corresponding requirements and measurement procedures in § 27.53 of this chapter for applicable Miscellaneous Wireless Radio Services. For mobile services operating in 758-769 MHz and 788-799 MHz, refer to the corresponding requirement and measurement procedure in § 90.543(e) of this chapter.

(2) For jamming solutions operating in 860 MHz range, refer to the corresponding requirements and measurement procedures in § 22.917 of this chapter for cellular services and § 90.691 of this chapter for Enhanced Specialized Mobile Radio services.

(3) For jamming solutions operating in the 1900 MHz range, refer to the corresponding requirements and measurement procedures in § 24.238 of this chapter for Personal Communications Services.

(4) For jamming solutions in the 3550 MHz range, refer to the corresponding requirements and measurement procedures in § 96.41 of this chapter for Citizens Broadband Radio Services.

(5) For jamming solutions operating in bands set forth in § 30.4 of this chapter, refer to the corresponding requirements and measurement procedures in § 30.203 of this chapter.

(b) For jamming solutions operating across multiple license blocks within the same service band, or across a contiguous band of two adjacent services, the out-of-band emission limits may be applied at the outer frequencies of the combined frequency range over which the jamming solution is permitted to operate, rather than applied to each channel within the service blocks or at the edge of each individual service band or allocation, if the jamming solution's operation spans across the adjacent band.

§ 90.1423 Locking mechanism requirement.

A jamming solution deployment must implement a geofencing feature that will cause any jamming device or devices to automatically cease operating if removed from the licensed jamming containment area(s) and a feature to enable the determination of the location of the jamming device or devices.

§ 90.1425 Network monitoring requirement.

A licensee of a jamming solution must: (1) monitor the RF environment for the bands in which jamming operations are active at a correctional facility; (2) detect a material change in the power level (e.g., a significant decrease) of a particular carrier's signals at the correctional facility; and (3) automatically modify the jamming solution architecture, such as by changing the power of the relevant jamming signal, adjusting antennas, or implementing other mitigations sufficient to maintain the protection criteria upon which its application was granted to not cause harmful interference to authorized users, or else immediately cease jamming operations in that band.

§ 90.1427 Interference resolution procedures.

The following requirements apply to a licensee authorized to provide a jamming solution pursuant to an overlay license issued pursuant to part 90, subpart Z, of this chapter:

(a) Jamming solution licensees shall establish a single point of contact that will be available at all times to receive complaints from the Commission, and credible complaints from the First Responder Network Authority, as defined in 47 U.S.C. 1424, and wireless providers, of harmful interference to authorized users resulting from jamming operations and shall update the contact information, as necessary.

(b) A complaint of harmful interference must come directly from the Commission, the First Responder Network Authority (FirstNet), as defined in 47 U.S.C. 1424, or a wireless provider, not an individual user. Complaints from FirstNet or a wireless provider must be credible, i.e., contain sufficient information to establish the contention that the jamming solution is the source of the harmful interference to an authorized user.

(c) Upon receipt of a credible complaint of harmful interference from the First Responder Network Authority, as defined in 47 U.S.C. 1424, or a wireless provider, or a complaint from the Commission, an overlay licensee must immediately cease jamming operations until the complaint is investigated and resolved. The overlay licensee is required to expeditiously investigate and such complaints of harmful interference.

§ 90.1429 Other technical/operational limits.

Jamming solution providers operating on spectrum bands deployed using frequency division duplex (FDD) technology shall only transmit on the downlink band to minimize impact on base station receivers.

§ 90.1431 Equipment authorization.

(a) Each transmitter utilized for operation under this part and each transmitter marketed, as set forth in § 2.803 of this chapter, must be of a type that has been authorized by the Commission under its certification procedure for use under this part. A modular transmitter may not be certified as a jamming device.

(b) Any manufacturer of radio transmitting equipment to be used in this service may request equipment authorization following the procedures set forth in subpart J of part 2 of this chapter. Equipment authorization for an individual transmitter may be requested by an applicant for a station authorization by following the procedures set forth in part 2 of this chapter.

§ 90.1433 Marketing limitation for jamming devices.

Jamming devices, as defined in § 90.1401 of this part, are subject to the provisions of § 2.803 of this chapter where applicable, but may only be marketed to a department of corrections for use at a correctional facility as part of a jamming solution or to a jamming solutions provider that has a contract with such a department of corrections.

§ 90.1435 Jamming device labeling requirements.

Jamming device manufacturers, distributors, and retailers must ensure that all jamming devices include the following advisories, in a conspicuous location, when marketed pursuant to § 90.1435 of this part:

(1) On the outside packaging of a jamming device; and

(2) On a label permanently affixed to a jamming device:

WARNING: This is NOT a CONSUMER device. You can ONLY PURCHASE AND/OR OPERATE this device if you have an FCC LICENSE authorizing the operation of a jamming solution in a correctional facility; and

(3) The information listed in (2) of this subsection may not be conveyed using the electronic labeling procedures contained in § 2.935 of this chapter.

§ 90.1437 Annual certification.

A licensee of a jamming solution deployed at a specific correctional facility must annually file a notification under its license in the Universal Licensing System, commencing one year after the date the pre-operational test notification, required by § 90.1411(a) of this part, is filed, certifying that the deployed jamming solution continues to operate as authorized and does not cause harmful interference outside the jamming containment area.

APPENDIX B

Proposed Rules

The Federal Communications Commission proposes to amend 47 CFR parts 2, 15, and 90 as follows:

PART 2 – FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

1. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336, unless otherwise noted.

2. Section 2.106 is amended by:

a. Revising pages 30–33, 35–42, 44, 54, 55, 58, and 59 of the Table of Frequency Allocations; and

b. Revising paragraph (c)(XXX).

The revisions read as follows:

§ 2.106 Table of Frequency Allocations.

* * * * *

5.149 5.291A 5.294 5.296 5.300 5.304 5.306 5.312 694-790 MOBILE except aeronautical mobile 5.312A 5.317A BROADCASTING	614-698 BROADCASTING Fixed Mobile 5.293 5.308 5.308A 5.309	
	698-806 MOBILE 5.317A BROADCASTING Fixed	
5.300 5.312 790-862 FIXED MOBILE except aeronautical mobile 5.316B 5.317A BROADCASTING	5.293 5.309	
	806-890 FIXED MOBILE 5.317A BROADCASTING	
5.312 5.319		

614-890	614-698 FIXED MOBILE Mobile-satellite NG33A NG5 NG14 NG33 NG115 NG149 US566	RF Devices (15) Satellite Communications (25) Wireless Communications (27) LPTV, TV Translator/Booster (74G Low Power Auxiliary (74H) Private Land Mobile (90)
	698-758 FIXED MOBILE Mobile-satellite NG33A NG159 US566	Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G) Private Land Mobile (90)
	758-775 FIXED MOBILE Mobile-satellite NG33A NG34 NG159 US566	Satellite Communications (25) Public Safety Land Mobile (90R) Private Land Mobile (90)
	775-788 FIXED MOBILE Mobile-satellite NG33A NG159	Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G)
	788-805 FIXED MOBILE Mobile-satellite NG33A NG34 NG159 US566	Satellite Communications (25) Public Safety Land Mobile (90R) Private Land Mobile (90)
	805-806 FIXED MOBILE Mobile-satellite NG33A NG159	Satellite Communications (25) Wireless Communications (27) LPTV and TV Translator (74G)
	806-809 LAND MOBILE	Public Safety Land Mobile (90S)
	809-849 FIXED LAND MOBILE Mobile-satellite NG33A	Public Mobile (22) Satellite Communications (25) Private Land Mobile (90)
	849-851 AERONAUTICAL MOBILE	Public Mobile (22)
	851-854 LAND MOBILE	Public Safety Land Mobile (90S)
	854-894 FIXED	Public Mobile (22)

862-890 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 5.319 5.323	5.317 5.318	5.149 5.305 5.306 5.307 5.320		LAND MOBILE Mobile-satellite NG33A US116 US268 US566	Satellite Communications (25) Private Land Mobile (90) Page 30

Page 31

Table of Frequency Allocations 894-1400 MHz (UHF)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
890-942 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 Radiolocation	890-902 FIXED MOBILE except aeronautical mobile 5.317A Radiolocation 5.318 5.325	890-942 FIXED MOBILE 5.317A BROADCASTING Radiolocation	890-902 US116 US268 G2	(See previous page) 894-896 AERONAUTICAL MOBILE US116 US268 896-901 FIXED MOBILE except aeronautical mobile US116 US268 901-902 FIXED MOBILE US116 US268	 Public Mobile (22) Wireless Communications (27) Private Land Mobile (90) Personal Communications (24)
	902-928 FIXED Amateur Mobile except aeronautical mobile 5.325A Radiolocation 5.150 5.325 5.326		902-928 RADIOLOCATION G59 5.150 US218 US267 US275 G11	902-928 5.150 US218 US267 US275	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Amateur Radio (97)
	928-942 FIXED MOBILE except aeronautical mobile 5.317A Radiolocation		928-932 US116 US268 G2	928-929 FIXED US116 US268 NG35 929-930 FIXED LAND MOBILE US116 US268 930-931 FIXED MOBILE US116 US268 931-932 FIXED LAND MOBILE US116 US268	Public Mobile (22) Private Land Mobile (90) Fixed Microwave (101) Private Land Mobile (90) Personal Communications (24) Public Mobile (22)

			932-935 FIXED US268 G2	932-935 FIXED US268 NG35	Public Mobile (22) Fixed Microwave (101)
			935-941	935-940 FIXED MOBILE except aeronautical mobile US116 US268 US566	Wireless Communications (27) Private Land Mobile (90)
				940-941 FIXED MOBILE	Personal Communications (24
5.323	5.325	5.327	US116 US268 G2	US116 US268	
942-960 FIXED MOBILE except aeronautical mobile 5.317A BROADCASTING 5.322 5.323	942-960 FIXED MOBILE 5.317A	942-960 FIXED MOBILE 5.317A BROADCASTING 5.320	941-944 FIXED US84 US268 US301 G2	941-944 FIXED US84 US268 US301 NG30 NG35	Public Mobile (22) Aural Broadcast Auxiliary (74E) Low Power Auxiliary (74H) Fixed Microwave (101)
			944-960	944-960 FIXED NG35	
960-1164 AERONAUTICAL MOBILE (R) 5.327A AERONAUTICAL RADIONAVIGATION 5.328 5.328AA			960-1164 AERONAUTICAL MOBILE (R) 5.327A AERONAUTICAL RADIONAVIGATION 5.328 5.328AA US78 US224		Aviation (87)
1164-1215 AERONAUTICAL RADIONAVIGATION 5.328 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.328A			1164-1215 AERONAUTICAL RADIONAVIGATION 5.328 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328A US224		
1215-1240 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.329 5.329A SPACE RESEARCH (active) 5.330 5.331 5.332			1215-1240 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) G132 SPACE RESEARCH (active) 5.332	1215-1240 Earth exploration-satellite (active) Space research (active)	
1240-1300 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.329 5.329A SPACE RESEARCH (active) Amateur 5.282 5.330 5.331 5.332 5.335 5.335A			1240-1300 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 SPACE RESEARCH (active) AERONAUTICAL RADIONAVIGATION 5.332 5.335	1240-1300 AERONAUTICAL RADIONAVIGATION Amateur Earth exploration-satellite (active) Space research (active) 5.282	Amateur Radio (97)

1300-1350 RADIOLOCATION AERONAUTICAL RADIONAVIGATION 5.337 RADIONAVIGATION-SATELLITE (Earth-to-space) 5.149 5.337A		1300-1350 AERONAUTICAL RADIONAVIGATION 5.337 Radiolocation G2 US342	1300-1350 AERONAUTICAL RADIONAVIGATION 5.337 US342	Aviation (87)
1350-1400 FIXED MOBILE RADIOLOCATION	1350-1400 RADIOLOCATION 5.338A	1350-1390 FIXED MOBILE RADIOLOCATION G2 5.334 5.339 US342 US385 G27 G114	1350-1390 5.334 5.339 US342 US385	
		1390-1395 5.339 US79 US342 US385	1390-1395 FIXED MOBILE except aeronautical mobile 5.339 US79 US342 US385 NG338A US566	Wireless Communications (27) Private Land Mobile (90)
5.149 5.338 5.338A 5.339	5.149 5.334 5.339	1395-1400 LAND MOBILE (medical telemetry and medical telecommand) 5.339 US79 US342 US385		Personal Radio (95)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
1400-1427 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340 5.341			1400-1427 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) 5.341 US246		
1427-1429 SPACE OPERATION (Earth-to-space) FIXED MOBILE except aeronautical mobile 5.341A 5.341B 5.341C 5.338A 5.341			1427-1429.5 LAND MOBILE (medical telemetry and medical telecommand) US350 5.341 US79	1427-1429.5 LAND MOBILE (telemetry and telecommand) Fixed (telemetry) 5.341 US79 US350 NG338A	Private Land Mobile (90) Personal Radio (95)
1429-1452 FIXED MOBILE except aeronautical mobile 5.341A 5.338A 5.341 5.342	1429-1452 FIXED MOBILE 5.341B 5.341C 5.343 5.338A 5.341		1429.5-1432 5.341 US79 US350	1429.5-1432 FIXED (telemetry and telecommand) LAND MOBILE (telemetry and telecommand) 5.341 US79 US350 NG338A	
			1432-1435 5.341 US83	1432-1435 FIXED MOBILE except aeronautical mobile 5.341 US83 NG338A US566	Wireless Communications (27) Private Land Mobile (90)
1452-1492 FIXED MOBILE except aeronautical mobile 5.346 BROADCASTING BROADCASTING-SATELLITE 5.208B 5.341 5.342 5.345	1452-1492 FIXED MOBILE 5.341B 5.343 5.346A BROADCASTING BROADCASTING-SATELLITE 5.208B 5.341 5.344 5.345		1435-1525 MOBILE (aeronautical telemetry) US338A		Aviation (87)

1492-1518 FIXED MOBILE except aeronautical mobile 5.341A 5.341 5.342	1492-1518 FIXED MOBILE 5.341B 5.343 5.341 5.344	1492-1518 FIXED MOBILE 5.341C 5.341		
1518-1525 FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341 5.342	1518-1525 FIXED MOBILE 5.343 MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341 5.344	1518-1525 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.348 5.348A 5.348B 5.351A 5.341	5.341 US84 US343	
1525-1530 SPACE OPERATION (space-to-Earth) FIXED MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Mobile except aeronautical mobile 5.349 5.341 5.342 5.350 5.351 5.352A 5.354	1525-1530 SPACE OPERATION (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Fixed Mobile 5.343 5.341 5.351 5.354	1525-1530 SPACE OPERATION (space-to-Earth) FIXED MOBILE-SATELLITE (space-to-Earth) 5.208B 5.351A Earth exploration-satellite Mobile 5.349 5.341 5.351 5.352A 5.354	1525-1535 MOBILE-SATELLITE (space-to-Earth) US315 US380	Satellite Communications (25) Maritime (80)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
1626.5-1660 MOBILE-SATELLITE (Earth-to-space) 5.351A 5.341 5.351 5.353A 5.354 5.355 5.357A 5.359 5.362A 5.374 5.375 5.376			1626.5-1660 MOBILE-SATELLITE (Earth-to-space) US308 US309 US315 US380 5.341 5.351 5.375		Satellite Communications (25) Maritime (80) Aviation (87)
1660-1660.5 MOBILE-SATELLITE (Earth-to-space) 5.351A RADIO ASTRONOMY 5.149 5.341 5.351 5.354 5.362A 5.376A			1660-1660.5 MOBILE-SATELLITE (Earth-to-space) US308 US309 US380 RADIO ASTRONOMY 5.341 5.351 US342		Satellite Communications (25) Aviation (87)
1660.5-1668 RADIO ASTRONOMY SPACE RESEARCH (passive) Fixed Mobile except aeronautical mobile 5.149 5.341 5.379 5.379A			1660.5-1668.4 RADIO ASTRONOMY US74 SPACE RESEARCH (passive)		
1668-1668.4 MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.379C RADIO ASTRONOMY SPACE RESEARCH (passive) Fixed Mobile except aeronautical mobile 5.149 5.341 5.379 5.379A			5.341 US246		
1668.4-1670 METEOROLOGICAL AIDS FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.379C RADIO ASTRONOMY			1668.4-1670 METEOROLOGICAL AIDS (radiosonde) RADIO ASTRONOMY US74		

5.149 5.341 5.379D 5.379E			5.341 US99 US342		
1670-1675 METEOROLOGICAL AIDS FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE MOBILE-SATELLITE (Earth-to-space) 5.351A 5.379B 5.341 5.379D 5.379E 5.380A			1670-1675 5.341 US211 US362	1670-1675 FIXED MOBILE except aeronautical mobile 5.341 US211 US362 US566	Wireless Communications (27 Private Land Mobile (90)
1675-1690 METEOROLOGICAL AIDS FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.341			1675-1695 METEOROLOGICAL AIDS (radiosonde) METEOROLOGICAL-SATELLITE (space-to-Earth) US88 5.341 US211 US289		
1690-1700 METEOROLOGICAL AIDS METEOROLOGICAL-SATELLITE (space-to-Earth) Fixed Mobile except aeronautical mobile 5.289 5.341 5.382	1690-1700 METEOROLOGICAL AIDS METEOROLOGICAL-SATELLITE (space-to-Earth) 5.289 5.341 5.381		1695-1710 METEOROLOGICAL-SATELLITE (space-to-Earth) US88 5.341	1695-1710 FIXED MOBILE except aeronautical mobile 5.341 US88 US566	Wireless Communications (27 Private Land Mobile (90)
1700-1710 FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.289 5.341		1700-1710 FIXED METEOROLOGICAL-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.289 5.341 5.384			
1710-1930 FIXED MOBILE 5.384A 5.388A 5.388B 5.149 5.341 5.385 5.386 5.387 5.388			1710-1761 5.341 US91 US378 US385 1761-1780 SPACE OPERATION (Earth-to-space) G42 US91	1710-1780 FIXED MOBILE 5.341 US91 US378 US385	
1930-1970 FIXED MOBILE 5.388A 5.388B 5.388	1930-1970 FIXED MOBILE 5.388A 5.388B Mobile-satellite (Earth-to-space) 5.388	1930-1970 FIXED MOBILE 5.388A 5.388B 5.388	1780-1850 FIXED MOBILE SPACE OPERATION (Earth-to-space) G42	1780-1850	
			1850-2025	1850-2000 FIXED MOBILE Mobile-satellite NG33A	RF Devices (15) Personal Communications (24) Satellite Communications (25 Wireless Communications

1970-1980 FIXED MOBILE 5.388A 5.388B 5.388					(27) Private Land Mobile (90) Fixed Microwave (101)
1980-2010 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) 5.351A 5.388 5.389A 5.389B 5.389F				US566	
2010-2025 FIXED MOBILE 5.388A 5.388B 5.388	2010-2025 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) 5.388 5.389C 5.389E	2010-2025 FIXED MOBILE 5.388A 5.388B 5.388		2000-2020 FIXED MOBILE MOBILE-SATELLITE (Earth-to-space) 2020-2025 FIXED MOBILE	Satellite Communications (25) Wireless Communications (27)
2025-2110 SPACE OPERATION (Earth-to-space) (space-to-space) EARTH EXPLORATION-SATELLITE (Earth-to-space) (space-to-space) FIXED MOBILE 5.391 SPACE RESEARCH (Earth-to-space) (space-to-space) 5.392			2025-2110 SPACE OPERATION (Earth-to-space) (space-to-space) EARTH EXPLORATION-SATELLITE (Earth-to-space) (space-to-space) SPACE RESEARCH (Earth-to-space) (space-to-space) FIXED MOBILE 5.391 5.392 US90 US92 US222 US346 US347	2025-2110 FIXED NG118 MOBILE 5.391 Space Operation (Earth-to-space) US94 5.392 US90 US92 US222 US346 US347	Space Launch Services (26) TV Auxiliary Broadcasting (74F) Cable TV Relay (78) Local TV Transmission (101J)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
2110-2120 FIXED MOBILE 5.388A 5.388B SPACE RESEARCH (deep space) (Earth-to-space) 5.388			2110-2120 US252	2110-2120 FIXED MOBILE US252 US566	Public Mobile (22) Wireless Communications (27) Private Land Mobile (90 Fixed Microwave (101)
2120-2170 FIXED MOBILE 5.388A 5.388B 5.388	2120-2160 FIXED MOBILE 5.388A 5.388B Mobile-satellite (space-to-Earth) 5.388 2160-2170 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.388 5.389C 5.389E	2120-2170 FIXED MOBILE 5.388A 5.388B 5.388	2120-2200	2120-2180 FIXED MOBILE NG41 US566	

2170-2200 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A 5.388 5.389A 5.389F			2180-2200 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) US566	Satellite Communications (25) Wireless Communications (27) Private Land Mobile (90)
2200-2290 SPACE OPERATION (space-to-Earth) (space-to-space) EARTH EXPLORATION-SATELLITE (space-to-Earth) (space-to-space) FIXED MOBILE 5.391 SPACE RESEARCH (space-to-Earth) (space-to-space) 5.392		2200-2290 SPACE OPERATION (space-to-Earth) (space-to-space) US96 EARTH EXPLORATION-SATELLITE (space-to-Earth) (space-to-space) FIXED (line-of-sight only) MOBILE (line-of-sight only including aeronautical telemetry, but excluding flight testing of manned aircraft) 5.391 SPACE RESEARCH (space-to-Earth) (space-to-space) 5.392 US303	2200-2290 US96 US303	Space Launch Services (26)
2290-2300 FIXED MOBILE except aeronautical mobile SPACE RESEARCH (deep space) (space-to-Earth)		2290-2300 FIXED MOBILE except aeronautical mobile SPACE RESEARCH (deep space) (space-to-Earth)	2290-2300 SPACE RESEARCH (deep space) (space-to-Earth)	
2300-2450 FIXED MOBILE 5.384A Amateur Radiolocation	2300-2450 FIXED MOBILE 5.384A RADIOLOCATION Amateur	2300-2305 G122	2300-2305 Amateur	Amateur Radio (97)
		2305-2310 US97 G122	2305-2310 FIXED MOBILE except aeronautical mobile RADIOLOCATION Amateur US97 US566	Wireless Communications (27) Private Land Mobile (90) Amateur Radio (97)
		2310-2320 Fixed Mobile US100 Radiolocation G2 US97 US327	2310-2320 FIXED MOBILE BROADCASTING-SATELLITE RADIOLOCATION US97 US100 US327 US566	Wireless Communications (27) Private Land Mobile (90)
		2320-2345 Fixed Radiolocation G2 US327	2320-2345 BROADCASTING-SATELLITE US327	Satellite Communications (25)
		2345-2360 Fixed Mobile US100 Radiolocation G2	2345-2360 FIXED MOBILE US100 BROADCASTING-SATELLITE RADIOLOCATION	Wireless Communications (27) Private Land Mobile (90)
5.150 5.282 5.395	5.150 5.282 5.393 5.394			

		US327	US327 US566	
		2360-2390 MOBILE US276 RADIOLOCATION G2 G120 Fixed US101	2360-2390 MOBILE US276 Space Operation (Earth-to-space) (space-to-Earth) NG42 US101	Space Launch Services (26) Aviation (87) Personal Radio (95)
		2390-2395 MOBILE US276 US101	2390-2395 AMATEUR MOBILE US276 Space Operation (Earth-to-space) (space-to-Earth) NG42 US101	Space Launch Services (26) Aviation (87) Personal Radio (95) Amateur Radio (97)
		2395-2400 US101 G122	2395-2400 AMATEUR US101	Personal Radio (95) Amateur Radio (97)
		2400-2417 5.150 G122	2400-2417 AMATEUR 5.150 5.282 US566	RF Devices (15) ISM Equipment (18) Amateur Radio (97)
		2417-2450 Radiolocation G2 5.150	2417-2450 Amateur 5.150 5.282 US566	
2450-2483.5 FIXED MOBILE Radiolocation 5.150	2450-2483.5 FIXED MOBILE RADIOLOCATION 5.150	2450-2483.5 5.150 US41	2450-2483.5 FIXED MOBILE Radiolocation 5.150 US41 US566	RF Devices (15) ISM Equipment (18) TV Auxiliary Broadcasting (74F) Private Land Mobile (90 Fixed Microwave (101)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIODETERMINATION-	2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIOLOCATION	2483.5-2500 FIXED MOBILE MOBILE-SATELLITE (space-to-Earth) 5.351A RADIOLOCATION	2483.5-2500 MOBILE-SATELLITE (space-to-Earth) US319 US380 US391 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398	2483.5-2495 MOBILE-SATELLITE (space-to-Earth) US380 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402 US41 US319 NG147	ISM Equipment (18) Satellite Communications (25)

SATELLITE (space-to-Earth) 5.398 Radiolocation 5.398A 5.150 5.399 5.401 5.402	RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402	RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.401 5.402	5.150 5.402 US41	2495-2500 FIXED MOBILE except aeronautical mobile MOBILE-SATELLITE (space-to-Earth) US380 RADIODETERMINATION-SATELLITE (space-to-Earth) 5.398 5.150 5.402 US41 US319 US391 NG147 US566	ISM Equipment (18) Satellite Communications (25) Wireless Communications (27) Private Land Mobile (90)
2500-2520 FIXED 5.410 MOBILE except aeronautical mobile 5.384A 5.412	2500-2520 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A 5.404	2500-2520 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A MOBILE-SATELLITE (space-to-Earth) 5.351A 5.407 5.414 5.414A 5.404 5.415A	2500-2655	2500-2655 FIXED US205 MOBILE except aeronautical mobile	Wireless Communications (27) Private Land Mobile (90)
2520-2655 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.412 5.418B 5.418C	2520-2655 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.418B 5.418C	2520-2535 FIXED 5.410 FIXED-SATELLITE (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.403 5.414A 5.415A 2535-2655 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 5.339 5.418 5.418A 5.418B 5.418C	5.339 US205	5.339 US566	
2655-2670 FIXED 5.410 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.208B 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.412	2655-2670 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.208B	2655-2670 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) 5.415 MOBILE except aeronautical mobile 5.384A BROADCASTING-SATELLITE 5.413 5.416 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.208B 5.420	2655-2690 Earth exploration-satellite (passive) Radio astronomy US385 Space research (passive)	2655-2690 FIXED US205 MOBILE except aeronautical mobile Earth exploration-satellite (passive) Radio astronomy Space research (passive)	

2670-2690 FIXED 5.410 MOBILE except aeronautical mobile 5.384A Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149 5.412	2670-2690 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.208B 5.415 MOBILE except aeronautical mobile 5.384A Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149	2670-2690 FIXED 5.410 FIXED-SATELLITE (Earth-to-space) 5.415 MOBILE except aeronautical mobile 5.384A MOBILE-SATELLITE (Earth-to-space) 5.351A 5.419 Earth exploration-satellite (passive) Radio astronomy Space research (passive) 5.149	US205 US566	US385 US566	
2690-2700 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340 5.422			2690-2700 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) US246		
2700-2900 AERONAUTICAL RADIONAVIGATION 5.337 Radiolocation 5.423 5.424			2700-2900 METEOROLOGICAL AIDS AERONAUTICAL RADIONAVI-GATION 5.337 US18 Radiolocation G2 5.423 G15	2700-2900 5.423 US18	Aviation (87)
2900-3100 RADIOLOCATION 5.424A RADIONAVIGATION 5.426 5.425 5.427			2900-3100 RADIOLOCATION 5.424A G56 MARITIME RADIONAVIGATION 5.427 US44 US316	2900-3100 MARITIME RADIONAVIGATION Radiolocation US44 5.427 US316	Maritime (80) Private Land Mobile (90)
3100-3300 RADIOLOCATION Earth exploration-satellite (active) Space research (active) 5.149 5.428			3100-3300 RADIOLOCATION G59 Earth exploration-satellite (active) Space research (active) US342	3100-3300 Earth exploration-satellite (active) Space research (active) Radiolocation US342	Private Land Mobile (90)
3300-3400 RADIOLOCATION 5.149 5.429 5.429A 5.429B 5.430	3300-3400 RADIOLOCATION Amateur Fixed Mobile 5.149 5.429C 5.429D	3300-3400 RADIOLOCATION Amateur 5.149 5.429 5.429E 5.429F	3300-3500 RADIOLOCATION US431B G2	3300-3450 US103 US342	
3400-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.430A Radiolocation	3400-3500 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.431A 5.431B Amateur Radiolocation 5.433	3400-3500 FIXED FIXED-SATELLITE (space-to-Earth) Amateur Mobile 5.432 5.432B Radiolocation 5.433		3450-3600 FIXED MOBILE except aeronautical mobile	Wireless Communi-cations (27) Private Land Mobile (90) Citizens Broadband (96)

5.431	5.282	5.282 5.432A	US103 US342	US103 US105 US431B US433 US566	Page 40

Table of Frequency Allocations	3600-5460 MHz (SHF)				Page 41
International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
3400-3600 MHz: see previous page	3500-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.431B Radiolocation 5.433	3500-3600 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.433A Radiolocation 5.433	3500-3550 RADIOLOCATION G59 AERONAUTICAL RADIONAVIGATION (ground-based) G110 US103 US431B	3500-3600 MHz: see previous page	
			3550-3650 RADIOLOCATION G59 AERONAUTICAL RADIONAVIGATION (ground-based) G110 US105 US107 US245 US433	3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) US107 US245 NG169 MOBILE except aeronautical mobile	Satellite Communications (25) Private Land Mobile 90) Citizens Broadband (96)
3600-4200 FIXED FIXED-SATELLITE (space-to-Earth) Mobile	3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile 5.434 Radiolocation 5.433	3600-3700 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile Radiolocation 5.435	3650-3700 US109 US349	US105 US109 US349 US433 US566	
	3700-4200 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE except aeronautical mobile		3700-4200	3700-4160 FIXED MOBILE except aeronautical mobile NG182 NG457A US566	Wireless Communications (27) Private Land Mobile (9(
				4160-4200 FIXED FIXED-SATELLITE (space-to-Earth) NG457A NG182	Satellite Communications (25)
4200-4400 AERONAUTICAL MOBILE (R) 5.436 AERONAUTICAL RADIONAVIGATION 5.438 5.437 5.439 5.440			4200-4400 AERONAUTICAL RADIONAVIGATION 5.440 US261		Aviation (87)
4400-4500 FIXED MOBILE 5.440A			4400-4940 FIXED MOBILE	4400-4500	
4500-4800 FIXED FIXED-SATELLITE (space-to-Earth) 5.441 MOBILE 5.440A				4500-4800 FIXED-SATELLITE (space-to-Earth) 5.441 US245	
4800-4990 FIXED MOBILE 5.440A 5.441A 5.441B 5.442			US113 US245 US342	4800-4940 US113 US342	
			4940-4990	4940-4990	

Radio astronomy 5.149 5.339 5.443		FIXED MOBILE except aeronautical mobile 5.339 US342 US385	Public Safety Land Mobile (90Y)
4990-5000 FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY Space research (passive) 5.149	4990-5000 RADIO ASTRONOMY US74 Space research (passive) US246		
5000-5010 AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION RADIONAVIGATION-SATELLITE (Earth-to-space)	5000-5010 AERONAUTICAL MOBILE (R) US115 AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION US260 RADIONAVIGATION-SATELLITE (Earth-to-space) US211		Aviation (87)
5010-5030 AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.328B 5.443B	5010-5030 AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION US260 RADIONAVIGATION-SATELLITE (space-to-Earth) (space-to-space) 5.443B US115 US211		
5030-5091 AERONAUTICAL MOBILE (R) 5.443C AERONAUTICAL MOBILE-SATELLITE (R) 5.443D AERONAUTICAL RADIONAVIGATION 5.444	5030-5091 AERONAUTICAL MOBILE (R) 5.443C AERONAUTICAL MOBILE-SATELLITE (R) 5.443D AERONAUTICAL RADIONAVIGATION US260 US211 US444		
5091-5150 FIXED-SATELLITE (Earth-to-space) 5.444A AERONAUTICAL MOBILE 5.444B AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION 5.444	5091-5150 AERONAUTICAL MOBILE US111 US444B AERONAUTICAL MOBILE-SATELLITE (R) 5.443AA AERONAUTICAL RADIONAVIGATION US260 US211 US344 US444 US444A		Satellite Communications (25) Aviation (87)
5150-5250 FIXED-SATELLITE (Earth-to-space) 5.447A MOBILE except aeronautical mobile 5.446A 5.446B AERONAUTICAL RADIONAVIGATION 5.446 5.446C 5.446D 5.447 5.447B 5.447C	5150-5250 AERONAUTICAL RADIONAVIGATION US260 US211 US307 US344	5150-5250 FIXED-SATELLITE (Earth-to-space) 5.447A US344 AERONAUTICAL RADIONAVIGATION US260 5.447C US211 US307 US566	RF Devices (15) Satellite Communications (25) Private Land Mobile (90) Aviation (87)
5250-5255 EARTH EXPLORATION-SATELLITE (active) MOBILE except aeronautical mobile 5.446A 5.447F RADIOLOCATION SPACE RESEARCH 5.447D 5.447E 5.448 5.448A	5250-5255 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G59 SPACE RESEARCH (active) 5.447D 5.448A	5250-5255 Earth exploration-satellite (active) Radiolocation Space research US566	RF Devices (15) Private Land Mobile (90)

5255-5350 EARTH EXPLORATION-SATELLITE (active) MOBILE except aeronautical mobile 5.446A 5.447F RADIOLOCATION SPACE RESEARCH (active) 5.447E 5.448 5.448A			5255-5350 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G59 SPACE RESEARCH (active) 5.448A	5255-5350 Earth exploration-satellite (active) Radiolocation Space research (active) 5.448A US566	
5350-5460 EARTH EXPLORATION-SATELLITE (active) 5.448B RADIOLOCATION 5.448D AERONAUTICAL RADIONAVIGATION 5.449 SPACE RESEARCH (active) 5.448C			5350-5460 EARTH EXPLORATION-SATELLITE (active) 5.448B RADIOLOCATION G56 AERONAUTICAL RADIONAVIGATION 5.449 SPACE RESEARCH (active) US390 G130	5350-5460 AERONAUTICAL RADIONAVIGATION 5.449 Earth exploration-satellite (active) 5.448B Radiolocation Space research (active) US390	Aviation (87) Private Land Mobile (90)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
5460-5470 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION 5.448D RADIONAVIGATION 5.449 SPACE RESEARCH (active) 5.448B			5460-5470 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 RADIONAVIGATION 5.449 US65 SPACE RESEARCH (active) 5.448B US49 G130	5460-5470 RADIONAVIGATION 5.449 US65 Earth exploration-satellite (active) Radiolocation Space research (active) 5.448B US49 US566	Maritime (80) Aviation (87) Private Land Mobile (90)
5470-5570 EARTH EXPLORATION-SATELLITE (active) MOBILE except aeronautical mobile 5.446A 5.450A RADIOLOCATION 5.450B MARITIME RADIONAVIGATION SPACE RESEARCH (active) 5.448B 5.450 5.451			5470-5570 EARTH EXPLORATION-SATELLITE (active) RADIOLOCATION G56 MARITIME RADIONAVIGATION US65 SPACE RESEARCH (active) 5.448B US50 G131	5470-5570 RADIOLOCATION MARITIME RADIONAVIGATION US65 Earth exploration-satellite (active) Space research (active) US50 US566	RF Devices (15) Maritime (80) Private Land Mobile (90)
5570-5650 MOBILE except aeronautical mobile 5.446A 5.450A RADIOLOCATION 5.450B MARITIME RADIONAVIGATION 5.450 5.451 5.452			5570-5600 RADIOLOCATION G56 MARITIME RADIONAVIGATION US65 US50 G131 5600-5650 METEOROLOGICAL AIDS RADIOLOCATION G56 MARITIME RADIONAVIGATION US65 5.452 US50 G131	5570-5600 RADIOLOCATION MARITIME RADIONAVIGATION US65 US50 US566 5600-5650 METEOROLOGICAL AIDS RADIOLOCATION MARITIME RADIONAVIGATION US65 5.452 US50 US566	
5650-5725 MOBILE except aeronautical mobile 5.446A 5.450A RADIOLOCATION Amateur Space research (deep space) 5.282 5.451 5.453 5.454 5.455			5650-5925 RADIOLOCATION G2	5650-5830 Amateur	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Amateur Radio (97)

5725-5830 FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur 5.150 5.451 5.453 5.455	5725-5830 RADIOLOCATION Amateur 5.150 5.453 5.455			5.150 5.282 US566	
5830-5850 FIXED-SATELLITE (Earth-to-space) RADIOLOCATION Amateur Amateur-satellite (space-to-Earth) 5.150 5.451 5.453 5.455	5830-5850 RADIOLOCATION Amateur Amateur-satellite (space-to-Earth) 5.150 5.453 5.455			5830-5850 Amateur Amateur-satellite (space-to-Earth) 5.150 US566	
5850-5925 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE 5.150	5850-5925 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE Amateur Radiolocation 5.150	5850-5925 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE Radiolocation 5.150	5.150 US245	5850-5925 FIXED-SATELLITE (Earth-to-space) US245 MOBILE NG160 Amateur 5.150 US566	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Personal Radio (95) Amateur Radio (97)
5925-6700 FIXED 5.457 FIXED-SATELLITE (Earth-to-space) 5.457A 5.457B MOBILE 5.457C 5.149 5.440 5.458			5925-6425 5.440 5.458	5925-6425 FIXED FIXED-SATELLITE (Earth-to-space) NG457A US566	RF Devices (15) Satellite Communications (25 Private Land Mobile (90) Fixed Microwave (101)
			6425-6525 5.440 5.458	6425-6525 FIXED-SATELLITE (Earth-to-space) MOBILE 5.440 5.458 US566	RF Devices (15) Satellite Communications (25 TV Broadcast Auxiliary (74F) Cable TV Relay (78) Private Land Mobile (90) Fixed Microwave (101)
			6525-6700 5.458 US342	6525-6700 FIXED FIXED-SATELLITE (Earth-to-space) 5.458 US342 US566	RF Devices (15) Satellite Communications (25 Private Land Mobile (90) Fixed Microwave (101)
6700-7075 FIXED FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.441 MOBILE			6700-7125	6700-6875 FIXED FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.441 5.458 5.458A 5.458B US566	

		6875-7025 FIXED NG118 FIXED-SATELLITE (Earth-to-space) (space-to-Earth) 5.441 MOBILE NG171 5.458 5.458A 5.458B US566	RF Devices (15) Satellite Communications (25 TV Broadcast Auxiliary (74F) Cable TV Relay (78) Private Land Mobile (90)
5.458 5.458A 5.458B		7025-7075 FIXED NG118 FIXED-SATELLITE (Earth-to-space) NG172 MOBILE NG171 5.458 5.458A 5.458B US566	RF Devices (15) TV Broadcast Auxiliary (74F) Cable TV Relay (78) Private Land Mobile (90)
7075-7145 FIXED MOBILE	5.458	7075-7125 FIXED NG118 MOBILE NG171 5.458 US566	
	7125-7145 FIXED 5.458 G116	7125-7145 5.458	RF Devices (15)
5.458 5.459			Page 44

22-22.21 FIXED MOBILE except aeronautical mobile 5.149	22-22.21 FIXED MOBILE except aeronautical mobile US342	
22.21-22.5 EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY SPACE RESEARCH (passive) 5.149 5.532	22.21-22.5 EARTH EXPLORATION-SATELLITE (passive) FIXED MOBILE except aeronautical mobile RADIO ASTRONOMY SPACE RESEARCH (passive) US342 US532	
22.5-22.55 FIXED MOBILE	22.5-22.55 FIXED MOBILE US211	
22.55-23.15 FIXED INTER-SATELLITE 5.338A MOBILE SPACE RESEARCH (Earth-to-space) 5.532A 5.149	22.55-23.15 FIXED INTER-SATELLITE US145 US278 MOBILE SPACE RESEARCH (Earth-to-space) 5.532A US342	Satellite Communications (25) Fixed Microwave (101)
23.15-23.55 FIXED INTER-SATELLITE 5.338A MOBILE	23.15-23.55 FIXED INTER-SATELLITE US145 US278 MOBILE	
23.55-23.6	23.55-23.6	Fixed Microwave (101)

FIXED MOBILE			FIXED MOBILE		
23.6-24 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY SPACE RESEARCH (passive) 5.340			23.6-24 EARTH EXPLORATION-SATELLITE (passive) RADIO ASTRONOMY US74 SPACE RESEARCH (passive) US246		
24-24.05 AMATEUR AMATEUR-SATELLITE 5.150			24-24.05 5.150 US211	24-24.05 AMATEUR AMATEUR-SATELLITE 5.150 US211	ISM Equipment (18) Amateur Radio (97)
24.05-24.25 RADIOLOCATION Amateur Earth exploration-satellite (active) 5.150			24.05-24.25 RADIOLOCATION G59 Earth exploration-satellite (active) 5.150	24.05-24.25 Amateur Earth exploration-satellite (active) Radiolocation 5.150	RF Devices (15) ISM Equipment (18) Private Land Mobile (90) Amateur Radio (97)
24.25-24.45 FIXED MOBILE except aeronautical mobile 5.338A 5.532AB	24.25-24.45 FIXED 5.532AA MOBILE except aeronautical mobile 5.338A 5.532AB RADIONAVIGATION	24.25-24.45 FIXED MOBILE 5.338A 5.532AB RADIONAVIGATION	24.25-24.45	24.25-24.45 FIXED MOBILE US146 US566	RF Devices (15) Upper Microwave Flexible Use (30) Private Land Mobile (90)

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
24.45-24.65 FIXED INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB	24.45-24.65 FIXED 5.532AA INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB RADIONAVIGATION 5.533	24.45-24.65 FIXED INTER-SATELLITE MOBILE 5.338A 5.532AB RADIONAVIGATION 5.533	24.45-24.65 INTER-SATELLITE RADIONAVIGATION 5.533		RF Devices (15) Satellite Communications (25)
24.65-24.75 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB	24.65-24.75 FIXED 5.532AA INTER-SATELLITE MOBILE except aeronautical mobile 5.338A 5.532AB RADIOLOCATION-SATELLITE (Earth-to-space)	24.65-24.75 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B INTER-SATELLITE MOBILE 5.338A 5.532AB	24.65-24.75 INTER-SATELLITE RADIOLOCATION-SATELLITE (Earth-to-space)		
24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) 5.532B MOBILE except aeronautical mobile 5.338A 5.532AB	24.75-25.25 FIXED 5.532AA FIXED-SATELLITE (Earth-to-space) 5.535 MOBILE except aeronautical mobile 5.338A 5.532AB	24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) 5.535 MOBILE 5.338A 5.532AB	24.75-25.25	24.75-25.25 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE US146 NG65 US566	RF Devices (15) Satellite Communications (25) Upper Microwave Flexible Use (30)
25.25-25.5 FIXED 5.534A INTER-SATELLITE 5.536			25.25-25.5 FIXED INTER-SATELLITE 5.536	25.25-25.5 Inter-satellite 5.536 Standard frequency and time	RF Devices (15)

MOBILE 5.338A 5.532AB Standard frequency and time signal-satellite (Earth-to-space)		MOBILE Standard frequency and time signal-satellite (Earth-to-space)	signal-satellite (Earth-to-space)	
25.5-27 EARTH EXPLORATION-SATELLITE (space-to-Earth) 5.536B FIXED 5.534A INTER-SATELLITE 5.536 MOBILE 5.338A 5.532AB SPACE RESEARCH (space-to-Earth) 5.536C Standard frequency and time signal-satellite (Earth-to-space) 5.536A		25.5-27 EARTH EXPLORATION-SATELLITE (space-to-Earth) FIXED INTER-SATELLITE 5.536 MOBILE SPACE RESEARCH (space-to-Earth) Standard frequency and time signal-satellite (Earth-to-space) 5.536A US258	25.5-27 SPACE RESEARCH (space-to-Earth) Inter-satellite 5.536 Standard frequency and time signal-satellite (Earth-to-space) 5.536A US258	
27-27.5 FIXED INTER-SATELLITE 5.536 MOBILE 5.338A 5.532AB	27-27.5 FIXED 5.534A FIXED-SATELLITE (Earth-to-space) INTER-SATELLITE 5.536 5.537 MOBILE 5.338A 5.532AB	27-27.5 FIXED INTER-SATELLITE 5.536 MOBILE	27-27.5 Inter-satellite 5.536	
27.5-28.5 FIXED 5.537A FIXED-SATELLITE (Earth-to-space) 5.484A 5.516B 5.517A 5.539 MOBILE 5.538 5.540		27.5-30	27.5-28.35 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE US566	RF Devices (15) Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile (90) Fixed Microwave (101)
			28.35-29.1 FIXED-SATELLITE (Earth-to-space) NG165 NG527A	RF Devices (15) Satellite Communications (25)
37-37.5 FIXED MOBILE except aeronautical mobile 5.550B SPACE RESEARCH (space-to-Earth) 5.547		37-38 FIXED MOBILE except aeronautical mobile SPACE RESEARCH (space-to-Earth)	37-37.5 FIXED MOBILE except aeronautical mobile US151 US566	Upper Microwave Flexible Use (30) Private Land Mobile (90)
37.5-38 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C MOBILE except aeronautical mobile 5.550B SPACE RESEARCH (space-to-Earth) Earth exploration-satellite (space-to-Earth) 5.547		US151	37.5-38 FIXED FIXED-SATELLITE (space-to-Earth) NG63 MOBILE except aeronautical mobile US151 US566	Satellite Communications (25) Upper Microwave Flexible Use (30) Private Land Mobile (90)
38-39.5 FIXED 5.550D FIXED-SATELLITE (space-to-Earth) 5.550C MOBILE 5.550B Earth exploration-satellite (space-to-Earth) 5.547		38-38.6 FIXED MOBILE 38.6-39.5	38-39.5 FIXED FIXED-SATELLITE (space-to-Earth) NG63 MOBILE NG175 US566	

39.5-40 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C MOBILE 5.550B MOBILE-SATELLITE (space-to-Earth) Earth exploration-satellite (space-to-Earth) 5.547 5.550E			39.5-40 FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) US382 G117	39.5-40 FIXED FIXED-SATELLITE (space-to-Earth) NG63 MOBILE NG175 US382 US566	
40-40.5 EARTH EXPLORATION-SATELLITE (Earth-to-space) FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C MOBILE 5.550B MOBILE-SATELLITE (space-to-Earth) SPACE RESEARCH (Earth-to-space) Earth exploration-satellite (space-to-Earth) 5.550E			40-40.5 EARTH EXPLORATION-SATELLITE (Earth-to-space) FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth) SPACE RESEARCH (Earth-to-space) Earth exploration-satellite (space-to-Earth) G117	40-40.5 FIXED-SATELLITE (space-to-Earth) MOBILE-SATELLITE (space-to-Earth)	Satellite Communications (25)
40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547	40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile Mobile-satellite (space-to-Earth) 5.547	40.5-41 FIXED FIXED-SATELLITE (space-to-Earth) 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547	40.5-41 FIXED-SATELLITE (space-to-Earth) Mobile-satellite (space-to-Earth) US211 G117	40.5-41 FIXED-SATELLITE (space-to-Earth) BROADCASTING BROADCASTING-SATELLITE Fixed Mobile Mobile-satellite (space-to-Earth) US211	
41-42.5 FIXED FIXED-SATELLITE (space-to-Earth) 5.516B 5.550C LAND MOBILE 5.550B BROADCASTING BROADCASTING-SATELLITE Aeronautical mobile Maritime mobile 5.547 5.551F 5.551H 5.551I			41-42.5 US211	41-42 FIXED FIXED-SATELLITE (space-to-Earth) MOBILE BROADCASTING BROADCASTING-SATELLITE US211	Page 58

International Table			United States Table		FCC Rule Part(s)
Region 1 Table	Region 2 Table	Region 3 Table	Federal Table	Non-Federal Table	
41-42.5 GHz: see previous page			41-42.5 GHz: see previous page	42-42.5 FIXED MOBILE US211	
42.5-43.5 FIXED FIXED-SATELLITE (Earth-to-space) 5.552 MOBILE except aeronautical mobile 5.550B RADIO ASTRONOMY 5.149 5.547			42.5-43.5 FIXED FIXED-SATELLITE (Earth-to-space) MOBILE except aeronautical mobile RADIO ASTRONOMY US342	42.5-43.5 RADIO ASTRONOMY US342	

<table>
<tr><td colspan="2">43.5-47
MOBILE 5.553 5.553A
MOBILE-SATELLITE
RADIONAVIGATION
RADIONAVIGATION-SATELLITE

5.554</td><td>43.5-45.5
FIXED-SATELLITE (Earth-to-space)
MOBILE-SATELLITE (Earth-to-space)
G117</td><td>43.5-45.5</td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2">45.5-46.9
MOBILE
MOBILE-SATELLITE (Earth-to-space)
RADIONAVIGATION-SATELLITE
5.554</td><td></td></tr>
<tr><td colspan="2"></td><td>46.9-47
MOBILE
MOBILE-SATELLITE (Earth-to-space)
RADIONAVIGATION-SATELLITE

5.554</td><td>46.9-47
FIXED
MOBILE
MOBILE-SATELLITE (Earth-to-space)
RADIONAVIGATION-SATELLITE

5.554</td><td></td></tr>
<tr><td colspan="2">47-47.2
AMATEUR
AMATEUR-SATELLITE</td><td rowspan="4">47-48.2</td><td>47-47.2
AMATEUR
AMATEUR-SATELLITE</td><td>Amateur Radio (97)</td></tr>
<tr><td colspan="2">47.2-47.5
FIXED
FIXED-SATELLITE (Earth-to-space) 5.550C 5.552
MOBILE 5.553B

5.552A</td><td>47.2-48.2
FIXED
FIXED-SATELLITE (Earth-to-space)
US297
MOBILE</td><td>Satellite
Communications (25)
Upper Microwave
Flexible Use (30)
Private Land Mobile(90)</td></tr>
<tr><td>47.5-47.9
FIXED
FIXED-SATELLITE (Earth-to-space)
5.550C 5.552 (space-to-Earth)
5.516B 5.554A
MOBILE 5.553B</td><td>47.5-47.9
FIXED
FIXED-SATELLITE (Earth-to-space) 5.550C 5.552
MOBILE 5.553B</td><td></td><td></td></tr>
<tr><td colspan="2">47.9-48.2
FIXED
FIXED-SATELLITE (Earth-to-space) 5.550C 5.552
MOBILE 5.553B

5.552A</td><td>NG65 US566</td><td></td></tr>
</table>

* * * * *

(c) * * *

(XXX) USXXX A jamming solution may be authorized subject to part 90, subpart Z of this chapter to prevent the operation of wireless devices in correctional facilities deemed contraband through a federal, state, or local law, or a correctional facility rule, regulation, or policy. Jamming solution operation is permitted under a primary allocation in the fixed and land mobile services, limited to an authorized jamming containment area within a correctional facility. Operation beyond the authorized jamming containment area is strictly prohibited, is on a non-interference basis, and shall not cause harmful interference to authorized services or devices.

* * * * *

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 15.1 is amended by revising paragraph (b) to read as follows:

§ 15.1 Scope of this part.

* * * * *

(b) The operation of an intentional or unintentional radiator that is not in accordance with the regulations in this part, and the operation of any jamming solution, as defined in § 90.1401 of this chapter, must be licensed pursuant to the provisions of section 301 of the Communications Act of 1934, as amended, unless otherwise exempted from the licensing requirements elsewhere in the chapter. The operation of an intentional radiator that is a contraband wireless device, as defined in § 1.9003 of this chapter, is not permitted.

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. Section 90.1405 is revised to read as follows:

§ 90.1405 Bands available.

The bands available for overlay licensing for jamming solutions in correctional facilities are 617-652 MHz, 716-728 MHz, 728-746 MHz, 746-757 MHz, 757-758 MHz, 758-769 MHz, 788-799 MHz, 862-869 MHz, 869-894 MHz, 935-940 MHz, 1390-1392 MHz, 1392-1395 MHz, 1432-1435 MHz, 1670-1675 MHz, 1695-1710 MHz, 1930-1990 MHz, 1995-2000 MHz, 2110-2180 MHz, 2180-2200 MHz, 2305-2315 MHz, 2315-2320 MHz, 2345-2350 MHz, 2350-2360 MHz, 2400-2483.5 MHz, 2496-2690 MHz, 3450-3550 MHz, 3550-3700 MHz, 3700-4140 MHz, 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz, 5850-5895 MHz, 5925-6425 MHz, 6425-6525 MHz, 6525-6875 MHz, 6875-7125 MHz, and the frequency bands listed in § 30.4 of this chapter in the Upper Microwave Flexible Use Service.

7. Section 90.1421 is amended by adding paragraph (X) to read as follows:

§ 90.1421 Emission limits.

* * * * *

(X) Jamming solutions authorized pursuant to part 90, subpart Z and operating in bands that are also specified in part 15 of this chapter as permitting unlicensed device use shall not exceed the following power spectral density (PSD) limits:

(1) In 2400-2483.5 MHz, 5150-5250 MHz, 5725-5895 MHz, and 6 GHz unlicensed bands, a radiated power of 200 mW/MHz (23 dBm/MHz) Equivalent Isotropic Radiated Power (EIRP).

(2) Jamming solution providers shall use the minimum power necessary to achieve goals within the authorized jamming containment area to minimize signal leakage beyond that area.

(3) *Power measurement*. Measurement of the EIRP of jamming solution transmitters may be performed using peak or average measurement techniques. Average power measurements shall not exceed a peak-to-average ratio (PAR) of 13 dB. For guidance on proper average measurement techniques, parties should consult a Commission-approved measurement technique (see FCC Laboratory's Knowledge Database).

(a) For purposes of this section, peak transmit power must be measured over an interval of continuous transmission using instrumentation calibrated in terms of an rms-equivalent voltage. The measurement results shall be properly adjusted for any instrument limitations, such as detector response times, limited resolution bandwidth capability when compared to the emission bandwidth, sensitivity, etc., so as to obtain a true peak measurement for the emission in question over the full bandwidth of the channel.

8. Section 90.1423 is amended by adding paragraph (X) to read as follows:

* * * * *

(X) Jamming solutions authorized pursuant to part 90, subpart Z and operating in bands that are also specified in part 15 of this chapter as permitting unlicensed device use, shall attenuate the power of any emission outside a jamming solution frequency band(s) of operation in accordance with the following:

(1) In the 2.4 GHz, 5.15-5.35 GHz, 5.47-5.895 GHz, and 6 GHz unlicensed bands, emissions outside the authorized band of operation must be suppressed at least to a level of -27 dBm/MHz.

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) incorporated an Initial Regulatory Flexibility Analysis (IRFA) in the *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, Third Further Notice of Proposed Rulemaking* (*Third FNPRM*), released in September 2025.[2] The Commission sought written public comment on the proposals in the *Third FNPRM*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA and it (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Rules

2. With today's *Third Report and Order* (*Third R&O*), the Commission takes a further step to address the public safety issue of contraband wireless device use in correctional facilities. We increase the availability of technical options for departments of correction (DOCs) by legalizing non-federal operation of radio frequency (RF) jamming solutions in the narrow context of correctional facilities, in compliance with applicable congressional statutes. We take a cue from congressional leaders who have proposed legislation in this area and continue to highlight the need for alternatives to address this public safety challenge. To achieve our goal, we adopt a regulatory framework for the authorization of jamming solutions, with appropriate technical safeguards and rules to reduce the risk that jamming operations will cause harmful interference to authorized communications or be used for unauthorized purposes. We aim to provide this additional tool to the corrections community as expeditiously as possible, while also imposing testing requirements in real-world correctional facility environments. Our new rules also take into account the differences in functionality between jamming solutions and other contraband interdiction systems (CISs), with an awareness that some of these technologies are operated by small entities.

3. In the *Third R&O*, to achieve our goals, we deauthorize subscriber operation of contraband wireless devices in correctional facilities that are deemed contraband through a federal, state, or local statute, or a correctional facility rule, regulation, or policy that prohibits the possession or operation of contraband wireless devices. This deauthorization rule facilitates jamming in accordance with section 333 of the Communications Act of 1934, as amended (the Act).[4] It also ensures that contraband wireless devices located in correctional facilities 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. We apply our deauthorization approach to traditional commercial bands at this time, as well as Band 14 spectrum licensed to FirstNet, and adopt rules to enable authorization of jamming solutions through non-exclusive overlay licensing, while retaining leasing as an available option where parties reach mutual agreement. To ensure that our 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, we adopt rules prohibiting the certification of

[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] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, GN Docket No. 13-111, Third Further Notice of Proposed Rulemaking, 40 FCC Rcd 8001, Appendix (2025) (*Third FNPRM*).

[3] 5 U.S.C. § 604.

[4] 47 U.S.C. § 333.

[5] *Id*. § 301.

[6] *Id*. § 333.

jamming devices pursuant to part 15 to prevent operation of such equipment under part 15 rules. We adopt testing requirements and technical parameters for jamming solutions, additional safety features for jamming devices, and marketing, labeling, and importation rules, to ensure that jamming is limited to targeted use in correctional facilities. Lastly, we also adopt a rule amendment to increase flexibility for the authorization of CIS technologies.

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

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

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

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA,[7] the Commission is required to respond to any comments filed by the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy, and also provide a detailed statement of any change made to the proposed rules as a result of those comments.[8] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

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

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the adopted rules.[9] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[10] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[11] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[12] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[13]

7. 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.[14] In general, a small business is an independent business having fewer than 500 employees.[15] These types

[7] Small Business Jobs Act of 2010, Pub. L. No. 111-240, 124 Stat. 2504 (2010).

[8] 5 U.S.C. § 604 (a)(3).

[9] 5 U.S.C. § 604.

[10] *Id*. § 601(6).

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

[12] 15 U.S.C. § 632.

[13] 13 CFR § 121.903.

[14] 5 U.S.C. § 601(3)-(6).

[15] *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.

of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[16] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and are not dominant in their field.[17] 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.[18] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[19] Based on the 2022 U.S. 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.[20]

8. The rules adopted in the *Third R&O* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[21] codes and corresponding SBA size standard.[22] Where available, we also provide additional information regarding the number of potentially affected entities in the identified industries below.

[16] *Id*.

[17] 5 U.S.C. § 601(4).

[18] *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/.

[19] 5 U.S.C. § 601(5).

[20] *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.

[21] 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.

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

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[23]	Total Small Firms[24]	% Small Firms
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	155	136	87.74%
Other Communications Equipment Manufacturing	334290	800 employees	310	294	94.84%
Wireless Telecommunications Carriers (except Satellite)[25]	517112	1,500 employees	1,184	1,081	91.30%
Telecommunications Resellers[26]	517121	1,500 employees	955	847	88.69%
All Other Telecommunications	517810	$40 million	1,673	1,007	60.19%
Engineering Services	541330	$25.5 million	47,367	37,363	78.88%
Facilities Support Service	561210	$47 million	2,941	2,402	81.67%
Security Guards and Patrol Services	561612	$29 million	7,676	6,052	78.84%
All Other Support Services	561990	$16.5 million	10,554	7,571	71.74%
Correctional Institutions	922140	499 prisoners[27]	1,677[28]	813	48.48%

[23] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[24] *Id.*

[25] 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, Wireless Communications Services, Wireless Telephony.

[26] 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.

[27] The SBA does not have a size standard for this industry. Based on facility characteristics information for these entities, in the 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, the smallest group of correctional facilities had 499 prisoners or less. Therefore, for purposes of assessing the number of small entities in this industry, we will consider a facility as small if it has 499 prisoners or less.

[28] *Id.*

Table 2. Telecommunications Service Provider Data

2025 Universal Service Monitoring Report Telecommunications Service Provider Data [29] (Data as of December 2024)	SBA Size Standard (1500 Employees)		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Toll Resellers	402	388	96.52
Wireless Telecommunications Carriers (except Satellite)[30]	608	522	85.86

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

9. The RFA directs agencies to describe the economic impact of adopted 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 requirement and the type of professional skills necessary for preparation of the report or record.[31]

10. The *Third R&O* adopts a regulatory framework that increases the RF options that DOCs can utilize to combat contraband wireless devices in correctional facilities. The new or additional reporting, recordkeeping, and compliance obligations apply to small entities as well as other applicants and licensees. There are two paths for the authorization of jamming solutions: spectrum leasing using the Commission's existing part 1 leasing rules, with amendments and additional rules for jamming solutions, and overlay licensing, using a new part 90 subpart. Many of the new rules, discussed below, regarding testing and operation of jamming solutions apply to both paths and are required for all lessees and licensee regardless of size to prevent the proliferation of jamming devices outside of the correctional facility context and harmful interference from jamming solutions to authorized communications outside of the targeted jamming containment area. That said, for eligible entities seeking authority to operate a jamming solution using a spectrum leasing arrangement, we continue to leverage existing leasing rules to the extent possible to reduce regulatory burdens. In our jamming authorization framework, we also apply some existing definitions applicable in the CIS context to the authorization of jamming solutions for consistency.

11. The rules adopted in the *Third R&O* may require small entities, as well as other applicants and licensees, to hire attorneys, engineers, consultants, or other professionals to comply, however, the Commission cannot quantify the cost of compliance at this time. We note, however, that several of the adopted rules are consistent with and mirror existing policies and requirements used for other part 90 licenses or part 1 spectrum leasing arrangements. Therefore, small entities may already be familiar with such policies and requirements and may already have the processes and procedures in place to facilitate compliance. To minimize burdens, we have adopted processes and procedures where possible, such as the proof of concept testing and the pre-operational testing, to allow direct interaction between wireless providers, solutions providers, and DOCs, and have avoided interjecting the Commission and additional regulations into the processes. Although we apply strict eligibility

[29] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 25, Table 1.12 (2025), https://docs.fcc.gov/public/attachments/DOC-418505A1.pdf.

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

[31] 5 U.S.C. § 604(a)(5).

requirements, we do not require overly burdensome marketing, importation, and labeling requirements for jamming devices beyond necessary limitations to prevent the misuse of jamming devices outside the correctional facility context. With regard to CISs, we maintain our existing streamlined processes currently in place. In our approach to the authorization of jamming solutions, we sought to provide flexibility for eligible applicants to comply with our rules and requirements in a variety of ways, and intend to assess applications on a case-by-case basis. Below is an overview of areas discussed in the *Third R&O* that may lead to modified or additional reporting, recordkeeping, or compliance requirements for small entities.

12. *Proof of Concept Testing*. To conduct the required proof of concept (POC) test as an initial step in either the overlay approach or the leasing approach, an eligible solutions provider seeking to deploy a jamming solution at a correctional facility must obtain an experimental radio service license from the Office of Engineering and Technology (OET) under part 5 of the Commission's rules. We require that experimental licensees provide seven days advance notification of the POC test to FirstNet and all relevant wireless providers, sufficient to allow them the opportunity to attend and participate in the test. Successful testing should demonstrate that the jamming system will function as described in the part 5 application, including that the jamming solution can be configured to only cause harmful interference to contraband devices located within the intended jamming containment area. Following the POC test, we require that the licensee file the results with the Wireless Telecommunications Bureau (WTB), including proof of advance notification of the POC test provided to FirstNet and the relevant wireless providers, and identification of any entities that attended or participated in the test.

13. *Non-Exclusive Overlay Licensing.* We adopt rules in a new part 90 subpart applicable only to jamming solutions in the correctional facility context to best serve the public interest as the most clear and administratively efficient approach. To be eligible to apply for a non-exclusive overlay license for a jamming solution, an applicant must be a DOC with authority over the correctional facility for which authority to operate a jamming solution is sought, or a solutions provider that has entered into a contract with such a DOC. After POC testing, we require an eligible entity seeking an overlay license to operate a jamming solution in a correctional facility to submit an FCC Form 601 in our Universal Licensing System (ULS), including administrative information, a certification regarding eligibility, a certification that it seeks to deploy jamming devices as part of a jamming solution, a brief description of the solution, confirmation of a successful POC test, the requested bands of operation and associated technical parameters (in compliance with the technical requirements adopted herein), the proposed containment area (license area), and the technical basis for how the system as deployed will not interfere with authorized communications outside of the jamming containment area. Although an applicant has the choice to have a part 2 equipment authorization in place for the jamming devices to be used as part of a jamming solution at the time it files an application, we do not require equipment authorization until prior to site-specific testing at the specific correctional facility. Following submission of the application, WTB will place the application on an informational public notice.

14. *Pre-operational Testing.* We require that overlay licensees provide seven days' advance notification of the pre-operational testing at a specific correctional facility to all relevant wireless providers, FirstNet, the relevant Statewide Interoperability Coordinator (SWIC) or equivalent representative, and the relevant Public Safety Answering Point (PSAP) or 911 Authority serving the facility, to allow them the opportunity to attend. The record reflects that wireless carriers seek involvement in the testing process, and we afford that opportunity, while finding it unnecessary to mandate their participation. The licensee must file a certification with WTB that its pre-operational test was successful when applying the selected protection criteria in accordance with the granted license; specifically, that it was able to demonstrate that the jamming system functions as described in the overlay license application, and that its RF signal causes harmful interference only within the identified licensed jamming containment area(s). The certification must include the following: proof that all jamming devices used as part of the jamming solution have appropriate equipment authorizations pursuant to part 2 of the Commission's rules, and identification of any entities that participated in the testing and proof of notification to the required entities.

15. A jamming solution licensee will be authorized to begin operations no earlier than the next business day after filing the notification of pre-operational testing. We expect a licensee to continue to operate in accordance with its established interference protection criteria and verify that the authorized jamming solution is not causing harmful interference outside of the licensed jamming containment area. To ensure the ongoing accuracy and reliability of a jamming solution at a specific facility, we require the licensee to file an annual certification that the deployed jamming solution is operating as authorized and not causing harmful interference outside the targeted jamming containment area. This requirement will protect public safety communications and other authorized communications from harmful interference going forward. Following license grant, although we anticipate that a licensee may need to make modifications to its system to account for changes in the RF environment, e.g., shielding or antenna placement changes, we will not require the filing of a license modification application unless the size of the containment area increases and/or the licensee seeks to add more spectrum bands to the authorization.

16. *Leasing Arrangements.* As a second path for the authorization of jamming solutions, we provide a market-based option whereby parties can mutually agree to enter into a spectrum leasing arrangement for a jamming solution in a correctional facility. However, because of heightened concern regarding the initiation of jamming solution deployments and the need for careful Commission review of applications and time for testing processes, we prohibit parties from entering into spectrum manager lease arrangements or using immediate approval procedures. We adopt the same eligibility restrictions applicable to applicants for jamming solution overlay licenses to be applicable to applicants for spectrum leasing arrangements for jamming solutions. In the same way that an overlay license applicant must complete POC testing prior to the submission of a jamming solution application, eligible parties that wish to submit a lease application for a jamming solution must successfully complete a POC test prior to submission of an application. After POC testing, parties seeking a *de facto* transfer lease to operate a jamming solution in a correctional facility will be required to submit an FCC Form 608 in ULS. We believe that the use of our existing Form 608, with attachments, adequately serves the purpose of authorizing leases for jamming solutions. Similar to overlay license applicants, lease applicants must include administrative information, a certification regarding eligibility, a certification that it seeks to deploy jamming devices as part of a jamming solution, a brief description of the solution, confirmation of a successful POC test, and the proposed containment area (lease area), showing how the system will not cause harmful interference outside of the containment area. As with overlay license applications, although the leased area will be based on the applicant's underlying contract with the relevant DOC, we do not require the applicant to file that contract with the Commission. Instead, we require that the applicant include a certification that a contract with that DOC has been executed to provide jamming at the specific facility. We also require an applicant to include the name and address of the correctional facility, a shapefile or visual representation of the geographic area within which the jamming solution impact will be contained such that harmful interference will not occur outside of that containment area, and the frequency bands requested, and the requisite protection criteria that will be maintained at the licensed boundary.

17. Because applications for *de facto* transfer spectrum lease arrangements for jamming solutions will not be subject to immediate approval procedures under our revised leasing rules, following submission of the application and acceptance for filing, WTB will place the application on public notice for public comment and will review each application individually to ensure that the applicant has satisfied all requirements. Following grant of consent to the lease arrangement, the lessee must follow the same on-site, pre-operational testing procedures as we adopt for overlay licensees to demonstrate that the jamming system will function as expected and within the boundaries of the leased containment area, while not causing harmful interference to authorized communications. We conclude that, whether a jamming solution is authorized through an overlay license or a lease, the same considerations are relevant with regard to the need to ensure that the jamming solution is restricted to the approved jamming containment area. We therefore require that lessees provide seven days' advance notice to all relevant wireless providers, FirstNet, the SWIC or equivalent representative, and the relevant PSAP or 911 Authority serving the facility of the pre-operational testing at the specific correctional facility, sufficient to allow them the opportunity to attend.

18. Following site-specific testing, the lessee is required to submit the following: a certification that the testing was complete and successful, in accordance with the system described in the application; proof that all jamming devices used as part of the jamming solution have appropriate equipment authorizations pursuant to part 2 of the Commission's rules; and identification of any entities that participated in the testing and proof of notification to the required entities. Following this submission regarding the on-site testing, the lessee will be authorized to initiate jamming operations at the specific correctional facility. More specifically, the lessee will be authorized to begin operations on the next business day. We expect a lessee to continue to operate in accordance with its established interference protection criteria and verify that the authorized jamming solution is not causing harmful interference outside of the leased jamming containment area. To ensure the ongoing accuracy and reliability of a jamming solution at a specific facility, we require the lessee to file an annual certification that the deployed jamming solution is operating as authorized and not causing harmful interference outside the targeted jamming containment area. This requirement will protect public safety communications and other authorized communications from harmful interference going forward. Following lease approval, although we anticipate that a lessee may need to make modifications to its system to account for changes in the RF environment, e.g., shielding or antenna placement changes, we will not require the filing of a lease modification application unless the size of the containment area increases and/or the lessee seeks to add more spectrum bands to the authorization that are licensed to the lessor wireless provider.

19. *Technical Parameters.* In the *Third R&O*, we adopt rules setting basic technical parameters to govern jamming devices and the deployment of jamming solutions in correctional facilities, while allowing flexibility regarding how solutions providers can meet these rules and requirements. After review of the record, we find it in the public interest to adopt power limits for jamming solutions in the form of a maximum power spectral density (PSD) and to adopt discrete radiated power limits for jamming solutions operating in bands above and below 1 GHz, respectively, rather than adopt a power limit for each specific band. This approach reduces burdens, provides regulatory certainty, and avoids unnecessary complexity. To provide manufacturers and solutions providers certainty and to facilitate near-term deployment of jamming solutions, we adopt the following radiated power limits for jamming solutions: jamming operations in frequency bands below 1 GHz are subject to a radiated power limit of 18 dBm/MHz (63.1 mW/MHz) Equivalent Isotropic Radiated Power (EIRP); and jamming operations in frequency bands above 1 GHz are subject to a radiated power limit of 24 dBm/MHz (251.2 mW/MHz) EIRP. We anticipate that these limits will afford solutions providers the flexibility to design effective jamming solutions across varying configurations in environments with strong base station wireless provider signals, including deploying a series of antennas that can limit the jamming signal impact to a targeted area, as required under our approach.

20. We also find it in the public interest to apply to jamming solutions the existing out of band emission (OOBE) limits applicable to commercial wireless systems operating in the same commercial bands. To further minimize the risk that deployment of a jamming solution will impact authorized communications, we also prohibit jamming solutions from transmitting on the uplink portion of frequency division duplexing (FDD) frequencies where the wireless provider base stations receive signals transmitted from end users. We anticipate that each jamming solution will be engineered for the conditions present at a given correctional facility and will be subject to Commission review, therefore, we do not adopt overly prescriptive requirements.

21. To protect authorized communications from harmful interference as a result of the deployment of a jamming solution, we require a jamming solution to: (1) monitor the RF environment of the bands in operation at a correctional facility; (2) detect a material change in the power level (e.g., a significant decrease) of a particular carrier's signals at the correctional facility; and (3) modify the power of the relevant jamming signal sufficient to maintain the protection criteria upon which its application was granted to not cause harmful interference to authorized users, or else immediately cease jamming operations in that band. In addition, we find it in the public interest to require jamming solution providers to include a geofencing feature in the design and operation of their systems, such that any of the jamming devices will automatically shut down if removed from the licensed jamming containment area(s). We

also require overlay licensees and lessees to maintain a single point of contact to receive complaints from the Commission and credible complaints from FirstNet and wireless providers of harmful interference to users resulting from jamming operations, and update the contact information as necessary by filing a ULS administrative update. An overlay licensee or lessee must cease jamming operations until the complaint is investigated and resolved in an expeditious manner.

22. *Part 15 Prohibition.* To guard against the unwanted proliferation of jamming devices outside of correctional facilities, we require that jamming operators apply for either a part 90 overlay license or a part 1 lease for a jamming solution and comply with the core technical rules in part 90, and we prohibit jamming operations under part 15. Combined with a prohibition against part 15 equipment authorization for jamming solutions, we believe that this will ensure that the authorization of jamming solutions does not lead to the production, marketing, or sale of unlicensed low-power jamming devices.

23. *Part 2 Equipment Authorization.* We find that certification under part 2 to ensure compliance with our part 90 core technical rules for jamming devices is necessary to protect against harmful interference to authorized communications. We require jamming devices to be used as part of a jamming solution to be certified under our part 2 equipment authorization procedures, whether the jamming solution is licensed under our overlay or leasing processes. We also require all jamming devices used as part of a jamming solution to obtain equipment certification under part 90. We take this approach as the core technical rules for jamming devices used as part of a jamming solution are located in a new part 90 subpart, applicable solely to jamming solutions authorized through either overlay licensing or leasing.

24. In addition, we specifically prohibit the certification of jamming devices under part 15 from an equipment authorization perspective. Consistent with our decision to require equipment certification for jamming devices, we find it appropriate to apply the procedures contained in rule sections 2.911 and 2.1033, which specify the process for obtaining equipment certification, including what information must be included in an application. Additionally, as specified in these rules, equipment on the Commission's Covered List is not eligible for certification and cannot be used as part of a jamming solution. Because the Commission is authorizing jamming solutions for the first time, such equipment will be subject to pre-approval guidance procedures until such time as the Commission determines that jamming devices have reached a sufficiently mature stage and equipment certification procedures for such devices are well established. Finally, we permit proof of concept testing of jamming solutions prior to equipment authorization through a part 5 experimental license granted by OET under current Commission rules.

25. *Marketing of Jamming Devices.* Under either a leasing or overlay licensing scenario, applicants for authority to operate a jamming solution in a correctional facility must be either a DOC with authority over the correctional facility for which authority to operate is sought or a solutions provider that has entered into a contract with such a DOC. To reinforce this eligibility restriction and guard against the spread of jamming devices to unauthorized users, we find it in the public interest to adopt a part 90 rule that restricts marketing of jamming devices to only those entities eligible to operate a jamming solution. Consistent with this restriction, we note that because marketing under the Commission's definition includes sales, jamming devices cannot be re-sold by a DOC or jamming solutions provider except to another DOC or jamming solutions provider that has a contract with a DOC.

26. *Labeling of Jamming Devices.* To enforce the restrictions on marketing and operation of jamming devices, and to guard against the spread of jamming devices to unauthorized users, we adopt a rule requiring a physical label on jamming devices and their packaging warning that only users authorized to operate jamming devices may purchase or operate such devices. We prohibit the use of e-labeling to satisfy this requirement.

27. *Importation of Jamming Devices.* We find it necessary and in the public interest to permit equipment intended for use in a jamming solution to be imported prior to receiving equipment authorization. This will allow jamming equipment to be available for the required POC test conducted at the outset of the authorization process pursuant to a part 5 experimental license. Under existing rules,

parties may import a limited number of devices prior to receiving equipment authorization if the devices are for testing and evaluation to determine compliance with FCC rules, product development, or suitability for marketing.

28. *Further Facilitating and Streamlining the Authorization of CIS Technology.* To solve the problem of delay in the posting of a correctional facility as approved for contraband wireless device disabling on the CIS status tracker located on the Commission's website, we adopt a rule change to clarify that a designated correctional facility officer (DCFO) can submit a qualifying request, provided there are no wireless provider objections received within five business days, on the date WTB updates the Commission's website to reflect certification of a specific facility. We amend section 20.23(c) to permit a DCFO to submit a qualifying request, absent wireless provider objections, beginning on the date WTB updates the Commission's website to reflect Phase II certification, or recertification following mandatory retesting every three years, of that specific facility.

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

29. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[32]

30. The *Third R&O* establishes rules to authorize RF jamming solutions in the narrow context of correctional facilities. We have taken steps to minimize the impact on small entities and other impacted entities with the rules we adopt by generally providing flexibility in how stakeholders can meet our minimum technical and testing requirements, and continuing to permit negotiations among stakeholders subject to our requirements. To assist stakeholders, including small entities, in navigating our leasing and licensing processes, we directed WTB to issue a public notice and related materials as necessary to guide compliance with our requirements. We also noted that staff, including the Contraband Ombudsperson, will be available to help explain and clarify concepts and requirements.

31. *Authorization of Jamming Solutions*. We considered, as a primary method of authorization, an approach to licensing that sought to leverage our current licensing process and spectrum leasing rules applicable to CISs, which small entities and other correctional facilities and/or solutions providers have used for many years, rather than creating a new paradigm. Based on the record, however, we concluded that leasing arrangements for jamming solutions are unlikely, given the wireless providers' opposition, together with a DOC preference for overlay licensing. Therefore, we adopted a framework to support a non-exclusive overlay licensing approach as the most direct and efficient way to achieve the goal of enhancing public safety. Although we adopted an overlay licensing framework, we provided flexibility to stakeholders, including small entities, to enter into spectrum leasing negotiations where appropriate on a case-by-case basis for particular correctional facilities.

32. In order to authorize jamming in accordance with statutory limitations, we deauthorized subscriber operation of contraband wireless devices in correctional facilities and applied this deauthorization rule to traditional commercial bands and, to close spectrum gaps in a jamming solution, to 700 MHz FirstNet spectrum accessed by AT&T commercial users on a secondary basis. We considered the extension of our framework to unlicensed part 15 operations and satellite communications, but we believe that a more robust record is needed regarding how best to extend our deauthorization rule to this type of spectrum. Therefore, we seek further comment on this issue in an accompanying *Fourth FNPRM*.

33. *Proof of Concept Test*. In the *Third R&O*, we considered, as an alternative to the adoption of a rules framework, a phased implementation of jamming solutions, such as a pilot program in

[32] 5 U.S.C. § 604(a)(6).

controlled environments, or initial restrictions for eligibility for the deployment of jamming solutions at particular types of correctional facilities. We rejected these approaches in favor of the requirement that eligible entities seeking to be authorized to deploy jamming solutions in correctional facilities conduct an initial real-world proof of concept (POC) test to expedite the authorization of jamming solutions and to demonstrate that the jamming system works as intended to contain harmful interference to a targeted jamming containment area. We found that the POC test will serve the same purpose as a pilot program and will be more expeditious. By giving solutions providers, including small entities, the choice of where to conduct the POC test, we aimed to reduce burdens and maintain flexibility, while also ensuring the ultimate containment of jamming solutions in accordance with our technical rules. We also avoided unnecessary delay in the process by not injecting the Commission as a required participant in the POC testing process.

34. *Non-exclusive Overlay Licensing.* We adopted rules in a new part 90 subpart applicable only to jamming solutions in the correctional facility context to best serve the public interest as the most clear and administratively efficient approach, rather than authorizing jamming solution licensees by spectrum band through many Commission rule parts, such as parts 22, 24, 27, 30, 90, and 96. By adopting a substantial number of our rules applicable to jamming solutions in a new subpart, we simplify the application and compliance process for applicants and licensees, making it easier for small entities to understand.

35. In adopting licensing rules, as a general matter, while we considered existing CIS leasing and certification rules, we aimed to create a firm divide between CISs and jamming solutions due to the differences in RF approach, functionality, and intended purpose. For example, we did not impose additional eligibility restrictions on jamming solution applicants, and we did not adopt a requirement of compliance with our 911 and E911 rules due to the technical limitations of jamming solutions. However, because we did not find evidence that the existing community notification requirement for CISs has been burdensome or ineffective, we found it in the public interest to adopt a similar community notification requirement for the deployment of jamming solutions. We continue to believe that the minimal burden on small entities and wireless providers of compliance with this notification requirement is outweighed by its significant public interest benefits, particularly in the jamming context. We also found it in the public interest to adopt a rule requiring relevant wireless providers to notify jamming solution providers in advance of certain technical changes to their networks to assist the operators in maintaining the effectiveness of systems deployed in correctional facilities.

36. With regard to the overlay licensing application requirements, we provided flexibility to applicants in terms of how they describe their interference protection criteria and method of verification used to confirm the lack of harmful interference for their specific jamming solutions to be deployed at particular correctional facilities. We gave small entities and other applicants the discretion to demonstrate compliance with our technical rules in whatever way works for their particular jamming solution. This flexibility promotes technological neutrality and will allow applicants to account for differences across correctional facility deployments, such as quality of service, density of nearby wireless users, and the surrounding RF environment and geographic features. We also took a flexible approach by giving DOCs the flexibility to contract with more than one solutions provider at a specific facility.

37. *Pre-operational Testing*. The on-site testing requirements that we adopted purposely do not inject the Commission into the testing process which could cause unnecessary delay. We adopted an approach that is administratively efficient, as it requires testing at the particular correctional facility where the jamming solution will be deployed following license grant, but prior to commencement of operations. The requirements we adopted for site-specific testing will serve the public interest by ensuring the effectiveness of jamming solutions without being overly prescriptive or causing undue delay. We found that prescribing detailed testing parameters or criteria would reduce flexibility and be potentially burdensome for small entities and other licensees, so we only required a certification from the licensee to satisfy the Commission that the system will operate as approved at the specific correctional facility.

38. Although we did not find it necessary to require a licensee to re-test its jamming solution at any correctional facility at which it is authorized to operate, we expect a licensee to continue to operate in accordance with its established interference protection criteria and continue to verify that the authorized jamming solution is not causing harmful interference outside of the license area. Following license grant, we anticipated that a licensee may need to modify its system to account for changes in the RF environment, for example, shielding or antenna placement changes, and we found that we will consider such changes minor modifications that do not require the filing of a modification application for Commission approval. This way, we reduced burdens on small entities. However, if a licensee seeks to increase the size of the licensed jamming containment area, we will consider that change to be a major modification that requires the filing of a modification application for Commission approval.

39. *Leasing Arrangements*. Because the record showed that voluntary wireless provider participation in the deployment of jamming solutions is remote, and we did not mandate participation through good faith leasing, we adopted an overlay licensing framework as the primary option to ensure that jamming solutions are available in the near term, but also made available leasing arrangements for jamming where desired by stakeholders. For both technical and administrative reasons, we excluded jamming solutions from our definition of CIS, recognizing that jamming solutions are functionally distinct from CIS authorizations and therefore require special rules. Although we applied our core jamming technical rules and testing requirements in both the overlay and leasing context, where relevant and necessary in the public interest, we leveraged to the extent possible our existing leasing regime for jamming solution lease arrangements. Where required, we adjusted our leasing rules for jamming solutions. For example, we prohibited spectrum manager leases and required that all leasing applications for jamming solutions be reviewed and approved by the Commission. We found that any additional burden imposed on small entities or other applicants seeking a spectrum lease arrangement for a jamming solution is outweighed by the need to ensure that any authorized jamming solution complies with our new technical rules and contains the jamming solution within the licensed area of a correctional facility.

40. After review of the record, we also concluded that it is unlikely that existing CIS lessees will be interested in modifying their leases to reflect authorization of a newly proposed jamming solution, and that it would be duplicative and more complicated to describe in a new rule the information and certifications we would require to be filed with a modification application as opposed to simply requiring the solutions provider to file a new lease application with the same required information and certifications, and most likely equally as burdensome. Additionally, in the leasing context for jamming solutions, we took the same approach regarding 911 call transmission requirements, community notification requirement, and relevant wireless provider advance notification of certain technical changes, as we did in the overlay licensing framework.

41. Finally, while we did not find it necessary to require the lessee to re-test its jamming solution at regular intervals following authorized deployment at any correctional facility, we noted our expectation that a lessee continue to operate in accordance with its established interference protection criteria and continue to verify that the authorized jamming solution is not causing harmful interference outside of the leased containment area. Following lease approval, although we anticipate that a lessee may need to make modifications to its system to account for changes in the RF environment, e.g., shielding or antenna placement changes, we did not require the filing of a lease modification application unless the size of the containment area increases and/or the lessee seeks to add more spectrum bands to the authorization that are licensed to the lessor wireless provider. This way, we minimize the burden on small entities and other lessees of jamming solutions.

42. *Technical Parameters*. After review of the record, we determined that no single type of jamming solution will best meet the needs of the wide variety of correctional facilities that exist across the country. Therefore, we did not adopt a rigid one-size-fits-all interference protection criteria so as to maintain a technologically neutral approach, reduce regulatory burdens, and prevent unnecessary implementation challenges. Instead, we required a demonstration from the jamming solutions provider describing the criteria it must meet to protect authorized users from harmful interference outside of the targeted jamming containment area. In line with our case-by-case approach to interference protection

criteria, we found it in the public interest to establish basic technical criteria, including radiated power limits, OOBE limits, restrictions on method of jamming based on wireless provider technology deployed, RF sending capability, and a jamming solution locking mechanism. We recognized the wide array of techniques available in jamming solutions, so we considered but rejected rules adopting limitations on certain design features or various other technical limits, such as field strength limit, PFD limit, or duty cycle, thereby promoting innovation and flexibility. Because we sought to provide regulatory certainly for stakeholders and clarity for small entities, we did not find it appropriate to adopt differing technical rules for jamming solutions based on the licensing mechanism. We applied a single set of technical limits applicable to all jamming solutions, whether authorized through overlay licensing or leasing, located in part 90. This approach is administratively more efficient, reduces burdens, and achieves regulatory parity where possible.

43. To further protect authorized communications from harmful interference as a result of the deployment of a jamming solution, we adopted a network monitoring requirement that requires power modification or the cessation of jamming operations in the event of a material change in the RF environment, and a locking mechanism to prevent jamming devices from being used outside of correctional facilities. To be technologically neutral and flexible, we declined to mandate how the licensee must meet these requirements. We also required overlay licensees and lessees to maintain a single point of contact to receive complaints from the Commission and credible complaints from FirstNet and wireless providers of harmful interference to users resulting from jamming operations, and to update the contact information as necessary by filing a ULS administrative update. An overlay licensee or lessee must cease jamming operations until the complaint is investigated and resolved in an expeditious manner. Because we recognized that the length of time required to investigate and resolve complaints of harmful interference will vary on a case-by-case basis, we declined to adopt a required timeframe for resolution. We also considered, but declined to adopt, reporting requirements in this regard to limit regulatory burdens on small entities and other licensees.

44. *Part 2 Equipment Authorization.* We found that certification under part 2 to ensure compliance with our part 90 core technical rules for jamming devices was necessary to protect against harmful interference to authorized communications from deployed jamming solutions. We required jamming devices to be used as part of a jamming solution to be certified under our part 2 equipment authorization procedures, whether the jamming solution is licensed under our overlay or leasing processes. Typically, RF equipment must comply with various Commission rule parts, depending on the spectrum to be used, and equipment certification approvals list the specific applicable rule parts. Here, however, we did not require jamming equipment to be certified under each distinct commercial wireless rule part, even when seeking ultimately to operate in those bands. Rather, for administrative certainty and ease of administration, we required all jamming devices used as part of a jamming solution to obtain equipment certification under only part 90.

45. *Marketing, Labeling, and Importation of Jamming Devices.* Under either a leasing or overlay licensing scenario, applicants for authority to operate a jamming solution in a correctional facility must be either a DOC with authority over the correctional facility for which authority to operate is sought or a solutions provider that has entered into a contract with such a DOC. To reinforce this eligibility restriction and guard against the spread of jamming devices to unauthorized users, we adopted a part 90 rule that restricts marketing of jamming devices to only those entities eligible to operate a jamming solution. We declined to adopt additional rules restricting marketing of jamming devices, however, in light of the strict technical requirements and safety features we adopted for jamming devices.

46. In addition, we found it in the public interest to permit equipment intended for use in a jamming solution to be imported prior to receiving equipment authorization. This will allow jamming equipment to be available for the required POC test conducted at the outset of the authorization process pursuant to a part 5 experimental license. This approach also provides flexibility to small entities and other solutions providers as they seek to develop effective jamming solutions that comply with our requirements. We found that current rules provide the necessary flexibility for manufacturers of jamming equipment to import their devices for the required POC testing, compliance testing, and other activities

that will need to be performed prior to receiving equipment authorization. In the interest of fostering an open playing field and allowing for the testing of a wide variety of jamming equipment that will best be able to comply with our technical requirements, we considered but did not adopt a requirement that jamming devices be manufactured or assembled in the United States, which could stifle innovation and impede our goal of promoting effective jamming solutions as a tool to help the correctional community in their efforts to combat contraband wireless device use in correctional facilities.

47. *Facilitating Other Interdiction Technologies.* We were not persuaded by the record that our current regulations prohibit the introduction of other solutions that industry might seek to develop and implement, so we did not adopt rules applicable to other interdiction technologies. For example, we support market-based industry solutions, and DOCs, in collaboration with solutions providers, are encouraged to work with the wireless providers and equipment manufacturers to explore geofencing solutions where wireless handsets can be equipped with hardware or software upgrades as necessary and, after interacting with base stations deployed at a correctional facility, the handset would not maintain a connection to the wireless provider network upon entering the correctional facility.

48. *Further Facilitating and Streamlining the Authorization of CIS Technology.* To avoid delay in the posting of a correctional facility as approved for disabling on the CIS status tracker located on the Commission's website, and for administrative clarity, we adopted a rule amendment to permit a DCFO to submit a qualifying request, absent wireless provider objections, beginning on the date WTB updates the Commission's website to reflect Phase II certification, or recertification following mandatory retesting every three years, of that specific facility. With regard to the CIS certification and disabling process, we considered but declined to adopt any additional requirements or changes to the existing CIS framework. We declined to make any sweeping changes to our current CIS authorization framework, as we continue to believe that our CIS disabling process is not unduly burdensome to small entities or other stakeholders. We also found it in the public interest to maintain our existing rules based on wireless provider participation in leasing arrangements, given the need for wireless provider cooperation in the contraband wireless device disabling process. Numerous solutions providers have successfully relied on this process following our adoption of the CIS certification and disabling process.

49. In the *Third R&O*, in authorizing jamming solutions, we found an overriding public interest in preventing the use of contraband wireless devices in correctional facilities by inmates to perpetuate criminal activity and therefore did not adopt exemptions for small entities from the regulatory framework. If small entities were exempted, it is likely that the effectiveness of the solution would be reduced, which is contrary to our goal in this proceeding.

G. Report to Congress

50. The Commission will send a copy of the *Third R&O*, including this Final Regulatory Flexibility Analysis, in a report to Congress pursuant to the Congressional Review Act.[33] In addition, the Commission will send a copy of the *Third R&O*, including this Final Regulatory Flexibility Analysis, to the Chief Counsel for the SBA Office of Advocacy and will publish a copy of the *Third R&O*, and this Final Regulatory Flexibility Analysis (or summaries thereof) in the Federal Register.[34]

[33] 5 U.S.C. § 801(a)(1)(A).

[34] *Id.* § 604(b).

APPENDIX D

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 *Fourth Further Notice of Proposed Rulemaking* (*Fourth FNPRM*) 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 *Fourth FNPRM*. The Commission will send a copy of the *Fourth FNPRM*, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.[2] In addition, the *Fourth FNPRM* 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 R&O*, we adopt rules to authorize non-federal operation of RF jamming solutions to provide the corrections community an additional tool to address the public safety challenges associated with contraband device usage in correctional facilities. The regulatory framework permits jamming solutions through a revision of section 1.903 of our rules, which only applies to fixed and mobile stations in the Wireless Radio Service (WRS). This approach does not affect the authority of wireless devices using unlicensed Wi-Fi or other part 15 spectrum, or those using spectrum separately licensed for satellite communications under part 100 of the Commission's rules. Accordingly, we propose and seek further comment on an approach that expands our adopted framework to unlicensed part 15 operations consistent with section 333 of the Act. We also seek additional comment on the scope of inmate use of contraband wireless devices communicating via satellite networks and an appropriate means to authorize jamming of satellite communications. Finally, we seek comment on additional safeguards for jamming solution deployments, as well as an approach whereby the Commission would establish "quiet zones" in and around certain correctional facilities.

3. Commenters in response to the *Third FNPRM* indicated that inmates are exploiting unlicensed spectrum for contraband wireless device use, including use of Wi-Fi and Bluetooth. Other commenters claimed that unlicensed spectrum use is not problem where commercial spectrum is jammed because there would be no functional devices connected to networks available for tethering and because the use of Wi-Fi is under the control of correctional facilities. The *Fourth FNPRM* seeks comment on these assertions, including the extent to which inmates are using unlicensed spectrum to communicate with contraband wireless devices.

4. The *Fourth FNPRM* ultimately seeks to avoid creating loopholes that inmates could exploit to perpetuate contraband wireless devices use. If inmates can circumvent jamming solutions by using unlicensed spectrum, then jamming could become less effective. We therefore seek additional comment on the scope of the problem of contraband devices operating on unlicensed spectrum and propose a framework to authorize jamming of unlicensed operations under part 15 to address potential gaps. We propose to deauthorize contraband part 15 devices by amending 47 CFR § 15.1 to indicate that, where an intentional or unintentional radiator meets the definition of a contraband wireless device in section 1.9003 of the Commission's rules (i.e., where possession or operation within a correctional facility is prohibited by federal, state, or local law, or a correctional facility rule, regulation, or policy),

[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*.

operation of such devices is not permitted and therefore they may be subject to jamming solutions consistent with section 333 of the Act.

5. We propose that, to receive authorization for a jamming solution in a correctional facility intended to prevent unlicensed contraband wireless device use, a solutions provider must obtain a part 90 overlay license and fully comply with the adopted part 90 rules governing proof of concept (POC) testing, overlay license application requirements, and core technical rules and safeguards, in the same manner as applicants seeking to deploy jamming solutions on licensed commercial spectrum. We propose to license jamming solutions for operation on the following bands currently available for part 15 unlicensed operation: 2400-2483.5 MHz, 5150-5250 MHz, 5250-5350 MHz, 5470-5725 MHz, 5725-5850 MHz, 5850-5895 MHz, 5925-6425 MHz, 6425-6525 MHz, 6525-6875 MHz, and 6875-7125 MHz.

6. The *Fourth FNPRM* also seeks further comment on the authorization of jamming solutions to address contraband wireless devices using satellite networks. In the *Third FNPRM*, the Commission sought comment on the extent of the problem of contraband wireless devices using satellite communications and on approaches to authorizing jamming solutions to address the potential problem. Satellite communications are not included in the framework adopted in the *Third R&O*, and the Commission therefore seeks further comment to develop the record on these issues. We seek further comment on the extent to which inmates use satellite networks to communicate with contraband wireless devices and on the appropriate approach to authorizing jamming solutions in the relevant bands. In addition, we seek comment on the implications of the Commission's *Space Modernization R&O* on potential jamming solutions and the deauthorization of contraband wireless devices in correctional facilities. In the *Space Modernization R&O*, the Commission reformed space and earth station licensing and operating rules by replacing part 25 with new part 100 rules. We seek further comment regarding the appropriate means to deauthorize the use of contraband wireless devices using satellite networks in light of the new part 100 rules, including those operating using Mobile Satellite Service (MSS) spectrum and operating under the Commission's current Supplemental Coverage from Space (SCS) rules. We note that the Commission is exploring changes to the SCS framework to modernize the rules and promote D2D connectivity, recognizing the convergence of terrestrial- and satellite-based networks. The issues discussed in the *Fourth NPRM* are generally applicable to the current MSS and SCS rules, as well as the rules being considered in the ongoing SCS proceeding. The *Fourth FNPRM* also seeks comment on whether and how technical requirements and safeguards might differ from the rules adopted in the *Third R&O* to ensure that jamming solutions adequately protect authorized incumbent users from harmful interference.

7. Finally, the *Fourth NPRM* seeks comment on additional safeguards for the deployment of jamming solutions, as well as an approach that would establish "quiet zones" in and around certain correctional facilities. The additional safeguards, including a requirement that wireless providers coordinate technical changes with overlay licensees at correctional facilities where a jamming solution is deployed and a requirement that wireless providers reduce signal strength levels surrounding correctional facilities, could serve to facilitate effective jamming solutions and reduce the risk of causing harmful interference to authorized users. The *Fourth NPRM* also seeks comment on additional compliance or monitoring obligations on lessees and licensees of jamming solutions to reduce the risk of harmful interference to authorized users outside of the jamming containment area, including authorized communications using Land Mobile Radio (LMR) systems to support vital public safety operations. An approach whereby the Commission establishes "quiet zones" in and around certain correctional facilities could further advance our policy of technological neutrality, providing another solution to the issue of contraband wireless device use in correctional facilities.

B. Legal Basis

8. 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.

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

9. 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 proposed rules, if adopted.[4] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[5] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[6] 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.[7] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[8]

10. 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.[9] In general, a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[11] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant in their field.[12] 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.[13] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[14] Based on the 2022 U.S. 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.[15]

---

[4] 5 U.S.C. § 603(b)(3).

[5] *Id*. § 601(6).

[6] *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."

[7] 15 U.S.C. § 632.

[8] 13 CFR § 121.903.

[9] 5 U.S.C. § 601(3)-(6).

[10] *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.

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] *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/.

[14] 5 U.S.C. § 601(5).

[15] *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.

11. The rules proposed in the *Fourth FNPRM* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[16] codes and corresponding SBA size standard.[17] Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[18]	Total Small Firms[19]	% Small Firms
Radio and Television Broadcasting and Wireless Communications Equip Manufacturing	334220	1,250 employees	155	136	87.74%
Other Communications Equipment Manufacturing	334290	800 employees	310	294	94.84%
Wireless Telecommunications Carriers (except Satellite)[20]	517112	1,500 employees	1,184	1,081	91.30%
Telecommunications Resellers[21]	517121	1,500 employees	955	847	88.69%
Satellite Telecommunications[22]	517410	$44 million	332	195	58.73%
All Other Telecommunications	517810	$40 million	1,673	1,007	60.19%
Engineering Services	541330	$25.5 million	47,367	37,363	78.88%
Facilities Support Service	561210	$47 million	2,941	2,402	81.67%

[16] 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.

[17] The size standards in this chart are set forth in 13 CFR § 121.201, by six digit North American Industrial Classification System (NAICS) code.

[18] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[19] *Id.*

[20] 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, Wireless Communications Services, Wireless Telephony.

[21] 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.

[22] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations, Fixed Satellite Very Small Aperture Terminal (VSAT) Systems, Mobile Satellite Earth Stations.

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[18]	Total Small Firms[19]	% Small Firms
Security Guards and Patrol Services	561612	$29 million	7,676	6,052	78.84%
All Other Support Services	561990	$16.5 million	10,554	7,571	71.74%
Correctional Institutions	922140	499 prisoners[23]	1,677[24]	813	48.48%

Table 2. Telecommunications Service Provider Data

2025 Universal Service Monitoring Report Telecommunications Service Provider Data [25] (Data as of December 2024)	SBA Size Standard (1500 Employees)		
Affected Entity	Total # FCC Form 499A Filers	Small Firms	% Small Entities
Toll Resellers	402	388	96.52
Wireless Telecommunications Carriers (except Satellite)[26]	608	522	85.86

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

12. 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.[27]

13. The proposed changes in the *Fourth FNPRM*, if adopted, may require small entities to hire attorneys, engineers, consultants, or other professionals to comply. Although the Commission cannot quantify the cost of compliance at this time, the proposed rule changes are similar to existing licensing and authorization processes, and small entities familiar with the Commission's existing rules may already have processes and procedures in place to facilitate compliance. We also anticipate that the comments we receive from small and other entities will assist the Commission in identifying and evaluating the extent

[23] The SBA does not have a size standard for this industry. Based on facility characteristics information for these entities, in the 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, the smallest group of correctional facilities had 499 prisoners or less. Therefore, for purposes of assessing the number of small entities in this industry, we will consider a facility as small if it has 499 prisoners or less.

[24] *Id.*

[25] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 25, Table 1.12 (2025), https://docs.fcc.gov/public/attachments/DOC-418505A1.pdf.

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

[27] 5 U.S.C. § 603(b)(4).

of potential burdens on small entities, including compliance costs and other economic or administrative burdens that may result from the inquiries we make in the *Fourth FNPRM*.

14. In the *Fourth FNPRM*, the Commission proposes to amend part 15 of the Commission's rules to permit operation of jamming solutions on certain part 15 spectrum bands. We propose to require a Commission license under the new part 90 overlay licensing rules for jamming of part 15 unlicensed spectrum in correctional facilities.[28] The part 1 leasing approach to authorizing jamming solutions, available in licensed commercial wireless bands as reflected in part 90, would not be an option for an applicant seeking an authorization to operate a jamming solution in a correctional facility on unlicensed part 15 spectrum. Applicants seeking authorization for a jamming solution in a correctional facility must apply for an overlay license under our new part 90 rules adopted in the *Third R&O*. We further propose and seek comment on requiring applicants seeking a part 90 overlay authorization to operate jamming solutions on part 15 unlicensed spectrum to include in their application a certification that they have entered into a contract that requires the solutions provider to block or otherwise deny access to unlicensed part 15 transmissions.

15. The *Fourth FNPRM* proposes technical rules for jamming solutions on unlicensed spectrum, including power limits and out-of-band emissions (OOBE) limits. Specifically, the Commission proposes to apply radiated PSD limits for jamming solutions in unlicensed bands that correspond with the power limits typically used for part 15 Wi-Fi operations. The proposed PSD limits are equivalent, on a per megahertz basis, to those of a Wi-Fi transmitter operating at a typical bandwidth at maximum power. We seek comment on this approach, and on whether jamming solution power limits should also vary across the unlicensed bands based on indoor/outdoor deployment scenarios. With respect to OOBE limits, the Commission proposes that for the 2.4 GHz, 5 GHz and 6 GHz unlicensed bands, jamming solution emissions outside the authorized band of operation must be suppressed to a level of at least -27 dBm/MHz EIRP. While this limit is more restrictive than the current variable OOBE rule, we believe that a fixed OOBE limit in this context will provide regulatory certainty for designers of jamming solutions. We seek comment on this approach to establishing an OOBE limit. Similar to other bands in which jamming solutions operate, we also propose that jamming solutions operating in part 15 bands should be subject to the radio frequency radiation exposure requirements specified in sections 1.1307(b), 1.1310, 2.1091, and 2.1093 of the Commission's rules and seek comment on this proposal.[29]

16. We also seek comment on the extent to which contraband wireless devices are operating in other unlicensed bands, beyond the 2.4 GHz, 5 GHz and 6 GHz unlicensed bands and whether there is any evidence that contraband wireless device use might expand to other unlicensed bands in the future. We encourage commenters supporting further expansion of jamming solutions to additional unlicensed bands to specify appropriate technical limits sought for each subject band. We similarly seek comment on authorizing the jamming of communications between satellite and contraband wireless devices and seek comment on any specific technical limits and requirements in that context.

17. We seek comment on additional matters related to facilitating effective jamming solutions and combatting contraband wireless devices in correctional facilities. The *Fourth NPRM* seeks comment on prohibiting wireless providers from increasing or decreasing the power level or making other adjustments at a transmitter site within 15 miles of a correctional facility where a jamming system is deployed without prior coordination with the correctional facility. We also seek comment on the alternative approach of applying a signal strength limit surrounding correctional facilities that is substantially lower than the level wireless providers currently afford commercial customers. We seek comment on additional compliance or monitoring obligations on lessees and licensees of jamming solutions, as well, to reduce the risk of harmful interference to authorized users outside of the jamming containment area. Finally, we seek comment on whether the Commission should establish "quiet zones"

[28] *See* 47 U.S.C.§ 301 (requiring a license for the "transmission of energy or communications or signals by radio").

[29] 47 CFR §§ 15.407(f), 1.1307(b), 1.1310, 2.1091, and 2.1093.

in and around certain correctional facilities. In these areas, wireless communications would not be authorized to provide signal coverage, such that devices in the area would not receive service from a wireless provider.

18. We encourage small and other entities, including correctional facilities, solutions providers, and providers of wireless services, 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 additional reporting, recordkeeping, or other compliance requirements for small entities, while ensuring that all parties meet the desired goals of providing an addition tool to address contraband wireless device use.

19. We expect the information received in comments, including, where requested, costs and benefit analyses, to help the Commission identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result if the proposals and associated requirements discussed in the *Fourth FNPRM* are adopted.

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

20. 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]

21. In developing the proposals outlined in the *Fourth FNPRM*, the Commission considered the impact of its proposals on small entities, if adopted. We expect that the impact of the proposals will be consistent with those of the rules adopted in the *Third R&O*, since the proposed framework largely aligns with the regulatory framework adopted to permit jamming of WRS bands. For example, if the proposal to permit jamming of part 15 operations using contraband wireless devices in correctional facilities is adopted, we propose that overlay license applicants can apply for whichever spectrum bands they seek authority to jam, including a mix of licensed bands and bands currently used for unlicensed operations. This approach ensures administrative efficiency and reduces regulatory burdens on small and other entities that seek to provide jamming solutions. By adopting a framework that is consistent with the approach in the WRS context, small entities, including solutions providers and departments of correction (DOCs), will already be familiar with the processes, minimizing the economic impact on such entities.

22. In the *Fourth FNPRM*, the Commission also considers and seeks comment on alternative approaches, including associated costs and benefits. For example, we seek comment on whether there are other preferred alternatives to license jamming operations on unlicensed bands, including specific changes that would be required to our part 15 rules and the part 90 rules adopted in the *Third R&O*. In addition, the Commission seeks comment on technical limits and requirements for the authorization of jamming solutions in correctional facilities for both unlicensed operations under part 15 and satellite communications, including alternatives to the proposals in the *Fourth FNPRM*. By seeking comment on these issues and the public interest concerns relevant to the proposals, the Commission will obtain the information required to consider the most appropriate approach to authorizing jamming of contraband wireless devices operating in unlicensed bands and using satellite communications.

[30] 5 U.S.C. § 603(c).

[31] *Id.* § 603(c)(1)-(4).

23. The Commission expects to more fully consider the economic impact and alternatives for small entities following the review of comments and costs and benefits analyses filed in response to the *Fourth FNPRM*. Alternative proposals and approaches from commenters could also help the Commission further minimize the economic impact on small entities. The Commission's evaluation of this information will shape the final alternatives it considers, the final conclusions it reaches, and any final actions it ultimately takes in this proceeding to minimize any significant economic impact of its actions on small entities.

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

24. None.