Administrative Code are incorporated by reference.

(A) R336.1802 Applicability under oxides of nitrogen budget trading program, effective May 20, 2004.

(B) R336.1803 Definitions for oxides of nitrogen budget trading program, effective December 4, 2002.

(C) R336.1804 Retired unit exemption from oxides of nitrogen budget trading program, effective May 20, 2004.

(D) R336.1805 Standard requirements of oxides of nitrogen budget trading program, effective December 4, 2002.

(E) R336.1806 Computation of time under oxides of nitrogen budget trading program, effective December 4, 2002.

(F) R336.1807 Authorized account representative under oxides of nitrogen budget trading program, effective December 4, 2002.

(G) R336.1808 Permit requirements under oxides of nitrogen budget trading program, effective December 4, 2002.

(H) R336.1809 Compliance certification under oxides of nitrogen budget trading program, effective December 4, 2002.

(I) R336.1810 Allowance allocations under oxides of nitrogen budget trading program, effective December 4, 2002.

(J) R336.1811 New source set-aside under oxides of nitrogen budget trading program, effective May 20, 2004.

(K) R336.1812 Allowance tracking system and transfers under oxides of nitrogen budget trading program, effective December 4, 2002.

(L) R336.1813 Monitoring and reporting requirements under oxides of nitrogen budget trading, effective December 4, 2002.

(M) R336.1814 Individual opt-ins under oxides of nitrogen budget trading program, effective December 4, 2002.

(N) R336.1815 Allowance banking under oxides of nitrogen budget trading program, effective December 4, 2002.

(O) R336.1816 Compliance supplement pool under oxides of nitrogen budget trading program, effective December 4, 2002.

(P) R336.1817 Emission limitations and restrictions for Portland cement kilns, effective December 4, 2002.

§ 52.1218 [Removed]

3. Section 52.1218 is removed.

[FR Doc. 05–8787 Filed 5–3–05; 8:45 am]

BILLING CODE 6560–50–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0, 2, and 15

[ET Docket No. 03–108; FCC 05–57]

Cognitive Radio Technologies and Software Defined Radios

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: This document modifies the Commission's rules to reflect ongoing technical developments in cognitive radio technologies. In light of the Commission's experience with these rules, the Commission is modifying and clarifying the equipment rules to further facilitate the development and deployment of software defined and cognitive radios. These actions are taken to facilitate opportunities for flexible, efficient, and reliable spectrum use by radio equipment employing cognitive radio technologies and enable a full realization of their potential benefits.

DATES: Effective August 2, 2005.

FOR FURTHER INFORMATION CONTACT: Hugh Van Tuyl, Office of Engineering and Technology, (202) 418–7506, e-mail: *Hugh.VanTuyl@fcc.gov*.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order, ET Docket No. 03–108, FCC 05–57, adopted March 10, 2005 and released March 11, 2005. The full text of this document is available on the Commission's Internet site at *http://www.fcc.gov*. It is also available for inspection and copying during regular business hours in the FCC Reference Center (Room CY–A257), 445 12th Street, SW., Washington, DC 20554. The full text of this document also may be purchased from the Commission's duplication contractor, Best Copy and Printing Inc., Portals II, 445 12th St., SW., Room CY–B402, Washington, DC 20554; telephone (202) 488–5300; fax (202) 488–5563; e-mail *FCC@BCPIWEB.COM*.

Summary of the Report and Order

1. An accelerating trend in radio technologies has been the use of software in radios to define their transmission characteristics. The incorporation of cognitive radio technologies to allow the more efficient use of spectrum is also becoming increasingly common. As demonstrated in this and earlier proceedings, this Commission has a continuing commitment to recognize these important new technologies and make any necessary changes to its rules and processes to facilitate their development in the public interest.

2. Over the past several years, manufacturers have increased the computer processing capabilities of radio system technologies. As a result, radio systems are increasingly incorporating software into their operating design. Incorporating software programming capabilities into radios can make basic functions easier to implement and more flexible. As the capabilities have advanced, radio systems have been gaining increased abilities to be ''cognitive''—to adapt their behavior based on external factors. This ''ability to adapt'' is opening up a vast potential for more flexible and intensive use of spectrum.

3. On December 17, 2003, we adopted a *Notice of Proposed Rule Making and Order,* 69 FR 7397, February 17, 2004, (''NPRM'') in this proceeding to explore the uses of cognitive radio technology to facilitate improved spectrum access. The *NPRM* addressed: (1) The capabilities of cognitive radios, (2) permitting higher power by unlicensed devices in rural or other areas of limited spectrum use, (3) enabling the development of secondary markets in spectrum use, including interruptible spectrum leasing, (4) applications of cognitive radio technology to dynamically coordinated spectrum sharing, and (5) software defined radio and cognitive radio equipment authorization rule changes. A total of 56 parties filed comments and 14 parties filed reply comments in response to the *NPRM.*

Discussion

4. The development of cognitive radio technology has been and will continue to be evolutionary in nature. As the technology evolves, our intent is to delete, change, or adopt rules in phases so as to ensure that our rules facilitate the market-based development and deployment of these technologies. In this *Report and Order,* we first cover in some detail various wide-ranging efforts being undertaken today by both government and industry to further in the near term the development of cognitive capabilities in software-based radio systems and in the longer term the evolution into fully capable cognitive radio systems.

5. To facilitate the market-based development and introduction of new technologies into the market, we addressed certain issues in the *Report and Order* that have arisen with respect to the certification of software-based radio equipment. Based on our experience and the comments in the record, we modify and clarify certain of

our rules that address software defined radios to facilitate the market based development of this technology. Specifically, we require radios in which the software that controls the RF operating parameters is designed or expected to be modified by a party other than the manufacturer to comply with the rules for software defined radios, including the requirement to incorporate security features to prevent unauthorized modifications to the software. We also modify the definition of software defined radio to include devices where a software change could make the device non-compliant with the Commission's radio frequency emission rules. We are eliminating the rule that the manufacturer supply radio software (source code) to the Commission upon request for certification because such software is generally not useful for certification review and may have become an unnecessary barrier to entry. We always retain the right to request and examine any component (whether software or hardware) of a specific radio system when needed for certification under Commission rules. We are requiring that the manufacturer supply a functional description of the radio software that controls its RF characteristics and a description of the means that will be used to protect that software from unauthorized tampering. Furthermore, since these descriptions are apt to involve proprietary intellectual property, we will make provisions to keep these specific items confidential, for Commission use only.

6. The *Report and Order* also considered the technical measures that a cognitive radio could incorporate to enable secondary use of spectrum, yet allow the use of such spectrum to quickly and reliably revert back to the licensee when necessary. We conclude that such measures are, or will be, technically feasible, but see no need to adopt any particular technical model for interruptible spectrum leasing.

Cognitive Radio Technology Developments

7. The efforts being undertaken by industry, often working with governmental agencies, standards bodies, and others to research, develop, and implement various software-defined radio and cognitive radio capabilities have been striking. These accomplishments were made possible through various advanced radio technologies such as those of the Department of Defense Joint Tactical Radio System (JTRS) in development of a common software architecture and the first actual software defined radios. Industry, working in conjunction with the military, is also taking a lead in developing and implementing new technologies and is serving as the impetus for further technical developments that should spur the commercial deployment of SDRs and cognitive radios. In addition, efforts are underway within industry forums and standards organizations to adopt internationally accepted standards for software defined radios and cognitive radios. These efforts and the resultant technical developments undoubtedly will lead to even greater flexibility in the future, with some touting the ultimate adoption of radios incorporating a cognition cycle as the foundation for a fully flexible cognitive radio.

8. The advent of cognitive radios and associated technologies has the potential to initiate a new era in radio frequency spectrum utilization. With radios that are able to recognize spectrum availability and able to negotiate protocols for rapid reconfiguration, these radios will employ software defined radio technologies to change their operational characteristics and open new opportunities for spectrum use. As highlighted in our NPRM, applications such as dynamic spectrum sharing, interruptible spectrum sharing, and rapidly reconfigurable secondary markets in spectrum use will be attainable with cognitive radios.

Enabling Cognitive and Software Defined Radio

9. In this section, we are making certain changes to our current rules and clarifying them in other respects. First we are modifying the definition of software defined radio to include radios that employ software that determines not just the operating parameters, but also the circumstances under which the radio transmits pursuant to those parameters. We clarify that equipment that is designed or expected to be modified by a party other than the manufacturer must be certified as software defined radios and comply with security requirements to prevent unauthorized modifications to the radio frequency operating parameters. We also clarify the security requirements that such equipment must meet.

10. In addition to these changes, we make several other changes to the authorization requirements for software defined radios. We find that the specific rule that requires manufacturers to supply a copy of their radio software (source code) to the Commission upon request is unnecessary because such software is generally not useful for certification review and may have become an unnecessary barrier to entry. In addition, the Commission already has authority to request to request and examine any component (whether software or hardware) of a radio system when needed for certification under Commission rules. We therefore delete this requirement as discussed below. Further, we clearly define the information about the radio software that must be submitted with applications for software defined radios. Additionally, we allow certification of certain part 15 unlicensed transmitters that have the technical capability of operating outside part 15 frequency bands, provided the equipment incorporates features to limit operation to authorized frequencies when used in the United States.

Cognitive and Software Defined Radio Security

a. Software Defined Radio Definition and Applicability of Rules

11. To reflect new kinds of conditions sometimes being included in our certification rules, we are broadening the definition of software defined radio to include devices where a software change could change not only the operating parameters of frequency range, modulation type or maximum output power, but also the circumstances under which a transmitter operates in accordance with Commission rules. For example, to make available otherwise unusable spectrum, we have required that certain radio transmitters include a DFS algorithm that further conditions use of spectrum beyond frequency range, modulation type, and maximum output. We are also changing the rules to require certain equipment to comply with the rules for software defined radios, including the requirement to incorporate security features to prevent unauthorized modifications to the software that controls the RF operating parameters. Specifically, we are requiring equipment in which the software that controls the radio frequency operating parameters is designed or expected to be modified by a party other than the manufacturer to comply with the rules for software defined radios. Because this change is limited to radios that contain RF affecting software that is third party modifiable, we believe that this change will affect only a small subset of equipment available in the marketplace today. We are making no change to the authorization requirements for the vast majority of devices such as cellular/PCS telephones, Wi-Fi equipment and two-way radios where the software that

controls the RF operating parameters is not designed or expected to be modified by a party other than the manufacturer.

12. We have modified our definition of software defined radio because, under recent rules, certain software changes that do not directly affect the technical operating parameters affect whether the device can be certified under our rules. The direct effects are addressed in the current definition of a software defined radio: frequency range, modulation type or maximum output power (either radiated or conducted). Our rules, however, now sometimes require additional radio functions such as DFS to prevent interference to other users. Even though these functions are being implemented and controlled by software in a radio, they do not currently fall within the definition of a software defined radio.

13. We are changing the definition of software defined radio to address software changes that directly or indirectly affect the compliance of a device with the Commission's rules. The modified definition will read as follows.

Software defined radio. A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

14. We are also changing the applicability of our rules to address software defined radios with relevant software that is designed or expected to be modified by a party other than the manufacturer. If a radio is not certified as a software defined radio, a manufacturer is not required to demonstrate in the equipment certification process that it incorporates features designed to prevent unauthorized changes to the software that would permit violation of Commission rules the equipment's certification, thus increasing the risk of interference to authorized radio services. We find that such a showing is in the public interest when a radio's RF-affecting software is designed or expected to be modified by a third party other than the manufacturer. In addition to minimizing the potential for unauthorized modifications to software defined radios, these changes will benefit manufacturers by allowing them to take advantage of the streamlined Class III permissive change procedure when they develop revised software that affects the RF operating parameters of the radio.

15. We find that the rules we are adopting that require the certification of certain radios as software defined radios will not be unduly burdensome on manufacturers or restrain the development of technology. Only a relatively small number of radios will be affected by this requirement because most RF affecting radio software is not designed or expected to be modified by a party other than the manufacturer, and we are not changing the rules for radios that are not designed or expected to be modified by a party other than the manufacturer. Thus, there will be no change to the authorization requirement for the vast majority of devices including cellular/PCS telephones, land mobile transceivers and Wi-Fi equipment, provided the software that directly or indirectly controls the RF emissions of these devices is not designed or expected to be modified by a party other than the manufacturer. Also, manufacturers of radios that are software modifiable typically already take steps to prevent unauthorized modifications to the software in a radio, so we expect that only rarely will manufacturers have to make significant design changes to comply with the security requirements. In addition, as discussed below, we are adopting changes to simplify the information that must be submitted with an application for a software defined radio. Finally, we find that the requirements we are adopting are consistent with the Commission's authority under section 302 of the Communications Act to make reasonable regulations, consistent with the public interest, which govern the interference potential of radio frequency devices.

16. We find that the standard we are adopting adequately protects against interference to other users. We disagree with the commenters who argue that only radios that can be remotely modified in large numbers should be required to be certified as software defined radios. We first find this definitional standard to be too difficult to apply. We also note that a radio that lacks security features to prevent unauthorized changes to the RF operating parameters could be easily modifiable to operate in unauthorized bands, and therefore has a high potential to interfere with authorized users in many different bands, including public safety bands. We therefore find that the requirement to certify certain radios as software defined radios should apply to all radios which are software modifiable by the user, not just those which could be remotely modified in large numbers.

17. *Permissive changes to software defined radios.* We are modifying the Class III permissive change rule, § 2.1043(b)(3), to make the wording consistent with the modified definition of software defined radio adopted. Additionally, we are setting forth a policy for permissive changes to radios that were approved before the effective date of the rules adopted in this *Report and Order*. Specifically, when a grantee wishes to make a permissive change to a previously approved device, the device will continue to be classified in the same manner that it was at the time it was originally certified, *i.e.*, software defined or non-software defined radio. Thus, a device that was approved as a non-software defined radio before the rules adopted herein become effective will not have to be re-certified as a software defined radio even if it meets the new standard for mandatory certification as a software defined radio. A device that was certified as a software defined radio will continue to be treated as such when a request for a permissive change is filed. Parties should note that we are not changing the requirement that Class III changes are permitted only for software defined radios in which no Class II changes have been made from the originally approved device.

b. Security Requirements for Software Defined Radios

18. We are clarifying the requirements in the rules that are intended to prevent unauthorized changes to the operating parameters of software defined radios. The Commission's equipment approval rules currently require that manufacturers take steps to ensure that only software that has been approved with a software defined radio can be loaded into such a radio. The current rule states that the software must not allow the user to operate the transmitter with frequencies, output power, modulation types or other parameters outside of those that were approved. Manufacturers may use authentication codes or any other means to meet these requirements, and must describe the methods in their application for equipment authorization.

19. We find that the current approach that manufacturers take steps to prevent unauthorized changes to the software in a radio, but does not require the use of specific security measures, is the most appropriate method to ensure the security of software defined radios. This approach allows manufacturers to respond to improvements in security technology more quickly and with the best solutions for a particular product

because no Commission action is necessary to permit manufacturers to use new security technologies. Therefore, we are maintaining the current security requirement. The record shows that manufacturers are aware of the need to incorporate security measures in software defined radios and are in fact doing so. We note that NTIA has recommended that, as a long term goal, we consider requiring ''Protection Profiles''—an approach currently under consideration in the SDR Forum—as part of the equipment certification process for software defined radios. After industry progresses further in its deliberations, we may consider the possible applicability of Protection Profiles, or certain concepts of Protection Profiles, to equipment certification in a future proceeding that addresses the security of software defined and cognitive radios.

20. Our security requirements for software defined radios give manufacturers flexibility to determine the appropriate security measures for a device. However, manufacturers also have the responsibility to choose security measures that can not be easily defeated by unintended parties. In the event that a software defined radio is found to be easily modifiable by end users, we would expect the responsible party as defined by our rules to immediately cease marketing the equipment and to take steps to ensure that future production of the equipment complies with the rules. Any potential forfeiture for non-compliance with the software defined radio security requirements would be considered on a case-by-case basis, taking into account all relevant factors, in the same manner as forfeitures are considered for non-compliant hardware-based equipment. In determining whether to issue any forfeiture penalties for a non-compliant device, the Commission takes into account the nature, circumstances, extent and gravity of the violations and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as may be relevant and appropriate. The Commission has specific guidelines for assessing forfeitures, but may issue higher or lower forfeitures than provided in the guidelines, issue no forfeiture at all, or apply alternative or additional sanctions as permitted by statute.

21. We decline to establish specific limitations on the responsible party's liability for a device that incorporates specific type(s) of security measures in the event that it is later determined that unauthorized modifications can be easily made to the radio frequency operating parameters of the device. The responsible party's liability for a non-compliant device is most appropriately determined on a case-by-case basis. Further, we agree with Intel that such an approach could be counterproductive because manufacturers would tend to design equipment to incorporate specific security features and may have little incentive to design equipment with robust security features, especially where more secure features add cost to a device. However, the Commission may consider compliance with industry security standards as a factor in determining the responsible party's liability.

22. We are simplifying the structure of the rules for software defined radios by moving the security requirements for software defined radios from § 2.932(e) into § 2.944. Section 2.944 currently contains a requirement for parties to submit a copy of radio software to the Commission upon request. We are changing that requirement as well as the applicability of the security requirements for software defined radios. We are placing the requirements for software defined radios into a single rule section, § 2.944, for easier reference. We are also modifying § 2.1033, which lists the information to be included in an application for certification, to make clear that an application for certification of a software defined radio must include the information specified in the revised § 2.944.

23. As part of the revisions to § 2.944, we are providing specific examples of the types of security measures that the Commission may consider to be acceptable for preventing unauthorized modifications to equipment. These examples are intended only to provide guidance to industry, and the use of one or more of these methods in a particular device should not be construed to limit a manufacturer's liability or responsibility to take appropriate corrective action in the event that parties other than the manufacturer are able to make unauthorized modifications to a device. This section will state that manufacturers may use any reasonable means to prevent impermissible modifications to the radio software including, but not limited to, the following and must describe the method(s) used for a particular device in the application for certification:

- The use of a private network that allows only authenticated users to download software.
- Coding in hardware that is decoded by software to verify that new software can be legally loaded into a device.
- Electronic signatures in software.

c. Amateur Equipment and D/A Converters

24. In the *NPRM*, we proposed to exempt manufactured software defined radios that are designed to operate solely in amateur bands from any mandatory declaration and certification requirements, provided the equipment incorporates features in hardware to prevent operation outside of amateur bands. We also sought comment on the need to restrict the mass marketing of high-speed digital-to-analog (D/A) converters that could be diverted for use as radio transmitters. No parties have provided any information that shows that software programmable amateur transceivers or high-speed D/A converters present any significantly greater risk of interference to authorized radio services than hardware radios. Therefore, we decline to adopt any new regulations for amateur transceivers or D/A converters at this time. However, we note that certain unauthorized modifications of amateur transmitters are unlawful, and may revisit both of these issues in the future if misuse of such devices results in significant interference to authorized spectrum users.

Submission of Radio Software

25. We are removing the requirement that an applicant for authorization of a software defined radio or the grantee or other party responsible for the compliance of a software defined radio submit a copy of the software that controls the radio frequency operating parameters upon request. We find that a copy of software source code is generally not be a useful aid in determining whether unauthorized changes have been made to the operating parameters of a device because software changes that have no effect on these parameters are frequently made by manufacturers. We also are concerned that this specific rule may be overly burdensome because we have observed that some equipment that could be authorized under the rules for software defined radios is not being authorized under these rules. The fact that the software in a device being marketed may differ somewhat from software previously supplied to the Commission would not necessarily indicate that any unauthorized changes have been made to a device's RF affecting operating parameters. In the event that questions arise about the compliance of a particular device, the

Commission has the authority to request and examine any component (whether software or hardware) of a radio system when needed for certification under Commission rules without the need for a specific requirement to submit radio software. Grantees of equipment certification are required to maintain records of equipment specifications and any changes that may affect compliance and must make these records available for inspection by the Commission. Further, the party responsible for the compliance of the device or any party who markets the device must supply a sample of the device to the Commission upon request.

26. We are adopting a requirement to submit a high level software operational description or flow diagram. The requirement we are adopting is analogous to the requirements in the rules that were developed for hardware based equipment that require applicants for equipment certification to supply a block diagram, schematic diagram and a brief description of the circuit functions of a device, along with a statement describing how the device operates. In this regard, the software operational description or flow diagram must describe or show how the RF functions in the radio, including the modulation type, operating frequency and power level are controlled or modified by software, and must describe the security or authentication methods that are incorporated to prevent unauthorized software changes. The description can include text, logic or flow diagrams, state descriptions or other material that provides the Commission's staff with a reasonable understanding of the operation of a device being certified and whether the device complies with the rules. The Commission's staff will work with applicants for certification to ensure that these requirements are clear and will issue appropriate additional guidance as necessary.

27. We agree with comments that information on how software within a software defined radio operates would be company proprietary information and that making this information publicly available would result in competitive harm to a manufacturer. Further, we find that information on the security methods that manufacturers employ to prevent unauthorized modifications to the RF operating parameters of a device would be considered company proprietary information. Additionally, making information on security measures publicly available could assist unauthorized parties in determining ways to defeat them. We also conclude that, if we were to make information on software defined radio operation and security measures generally available to the public, entities seeking equipment certification may not provide sufficient information for the Commission to determine whether the device at issue would operate in compliance with our rules. Accordingly, we will modify § 0.457(d) of the rules to state that the descriptions of the security features and software operation for a software defined radio are presumptively protected from public disclosure and will not routinely be made available for public inspection. This presumptive protection will apply only to the descriptions of the security features and software operation for a software defined radio and not to any other exhibits in the application for certification which will normally be made available for public inspection after grant of the application. An applicant for certification of a software defined radio must file a specific request and pay the appropriate filing fee to have other exhibits in the application held confidential, assuming the exhibits are eligible for confidential treatment. To avoid possible delays in processing applications, applicants should ensure that exhibits for which confidential treatment is automatically afforded or for which it is requested are clearly identified and that these exhibits do not contain information that is not eligible for such treatment.

28. We decline to allow TCBs to certify software defined radios at this time. The changes that we are adopting to automatically afford confidential treatment to the description of software and security features in software defined radio applications address the confidentiality concerns of parties who requested that TCBs be allowed to certify software defined radios to protect this information from public disclosure. Additionally, as the Commission has previously stated, because software defined radio is a new technology, TCBs will not be permitted to certify software defined radios until the Commission has more experience with them and can properly advise TCBs on how to apply the applicable rules. The Commission's Laboratory maintains a list of types of devices, including software defined radios, that TCBs are excluded from certifying. The Laboratory will remove software defined radios from this exclusion list when it determines that TCBs are capable of certifying them.

Automatic Frequency Selection by Unlicensed Devices

29. We are changing part 15 of the rules to allow certification of unlicensed transmitters that are capable of operation outside of permissible part 15 frequency bands, provided the transmitters incorporate an automatic frequency selection mechanism to ensure that they operate only on frequencies where unlicensed operation is permitted when operated in the United States.

30. We will allow certification of part 15 devices that operate outside permissible frequency bands using a master/client model. The terms ''master'' and ''client'' were defined in the U–NII proceeding for U–NII devices. We will define these terms for other types of part 15 devices consistent with the U–NII definitions. That is, a master device will be defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices. A network always has at least one device operating in master mode. A client device will be defined as a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network. We, of course, require master devices marketed within the United States to operate only in permissible part 15 frequency bands, which will ensure that they enable operation of client devices only within permissible part 15 frequency bands. Manufacturers that wish to market master devices that are hardware-capable of operating outside of permissible part 15 frequency bands for use in other countries, but use software to limit their operation to permissible part 15 frequency bands, must incorporate security features into them to limit the operating frequency range for devices marketed in the United States and must certify the devices as software defined radios. Different software can then be installed in master devices that are used outside of the United States to change the operating frequency range for use in other countries. Client devices that can also act as master devices must meet the certification requirements of a master device, and thus must be certified as software defined radios if the manufacturer wishes to incorporate additional frequency bands for use in other countries.

31. We will allow the certification of client devices such as wireless LAN cards used in desktop or notebook computers if they have the capability of operating outside permissible part 15 frequency bands. Client devices may transmit only under the control of a master device. Because master devices are limited to operation on permissible

part 15 frequencies, they will direct client devices to operate on only permissible part 15 frequencies.

32. The changes we have adopted will benefit manufacturers by allowing production of devices that can be used in multiple countries, thus reducing equipment costs. At the same time, the requirement to limit the frequency range of master devices sold in the United States will minimize the likelihood that devices will operate outside permissible frequency bands and cause interference to authorized services.

Interruptible Spectrum Leasing

33. In this section, we are describing the technical methods that a cognitive radio could use to enable interruptible secondary use of licensed spectrum by other parties. The concepts in this section would apply to lessors who want a high level assurance of reclaiming leased spectrum when they need it. We find that there are technologies available now or under development that could safely allow for interruptible spectrum leasing. We find that cognitive radio technologies, or even trunked radio technologies, would allow implementation of the following general principles that interested parties state would be essential to enable interruptible leased use of spectrum:

1. The licensee must have positive control as to when the lessee can access the spectrum.
2. The licensee must have positive control to terminate the use of the spectrum by the lessee so it can revert back to the licensee's use.
3. Reversion must occur immediately upon action by the licensee unless that licensee has made specific provisions for a slower reversion time.
4. The equipment used by the licensee and the lessee must perform access and reversion functions with an extremely high degree of reliability.
5. The equipment used by the licensee and the lessee must incorporate security features to prevent inadvertent misuse of, and to thwart malicious misuse of, the licensee's spectrum.

34. There are at least three different technical approaches that currently exist or are under development that a licensee could employ that would comply with the intent of these principles and enable interruptible spectrum leasing. One approach would be for a licensee to allow leasing using an existing trunked system. A trunked system uses a central controller to select the operating frequencies of radios in the system. When a radio is ready to begin transmitting, it sends a request for an operating frequency to a central controller over a control channel. The controller dynamically assigns an operating frequency to that radio and the other radios with which it communicates. Such a centralized system could be used to assign channels to radios operating under the terms of a lease, or de-assign channels when a licensee needs to use the spectrum. This could be done through a wireless control channel as is currently done to assign channels to radios in the system. Alternatively, information about leased channel availability could be provided by the trunked system controller to the lessee's equipment through a wired link.

35. The beacon approach proposed in the *NPRM* and described above is similar to a trunked system in that it uses a centralized controller to enable operation of lessee's equipment. The beacon could operate either on a frequency licensed to the public safety entity or on a separate control frequency in another band. The approach would require additional infrastructure such as the beacon transmitters and radios that are capable of receiving the beacon and adjusting their operation in response to the beacon signal.

36. A third method that could enable leased use of spectrum is by an exchange of ''tokens'' sent to the lessee's devices. Token approaches rely on the encrypted exchange of unique information to verify a user's identity when opening and maintaining a secure communications exchange. Tokens would provide a means of ensuring that lessees transmit only on available frequencies when they receive an electronic token authorizing them to do so. These tokens could also enforce terms of a lease such as the specific period of time that transmission on a frequency is allowed, thus providing a licensee with a high level of confidence that lessees will vacate the spectrum when required under the terms of the lease. Such token technology is already in use in other resource allocation problems, such as the enforcement of software license terms and avoiding data transmission conflicts between computers on local area networks.

37. At this point, we see no need to adopt any particular technical model for interruptible spectrum leasing. Ultimately, a licensee must itself be satisfied that the technical mechanism being implemented under a lease does in fact provide it with the ability in real time to reclaim use of its spectrum when necessary.

Final Regulatory Flexibility Analysis

38. As required by the Regulatory Flexibility Act (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Notice of Proposed Rule Making and Order, Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies (NPRM).*[2] The Commission sought written public comments on the proposals in the Notice, including comment on the IRFA.[3] This Final Regulatory Flexibility Analysis conforms to the RFA.[4]

A. Need for, and Objectives of, the Report and Order

39. Advances in technology are creating the potential for radio systems to use radio spectrum more intensively and more efficiently than in the past. Software-defined and cognitive, or ''smart,'' radios are allowing and will increasingly allow more intensive access to, and use of, spectrum than possible with traditional, hardware-based radio systems. In this *Report and Order*, the Commission continues the process of modifying the rules to reflect these ongoing technical developments in radio technologies. The Commission first adopted rules for software defined radios in 2001, recognizing that manufacturers were beginning to use software to help determine the RF characteristics of radios, and that the equipment rules, which assumed hardware changes were needed to modify a radio's behavior, held the potential of discouraging development of software defined radios by requiring repeated approvals for repeated software changes. In light of the Commission's experience with these rules, and the record in this proceeding, it is modifying and clarifying the equipment rules to further facilitate the development and deployment of software defined and cognitive radios.

40. In the *Report and Order,* the Commission makes several changes to parts 2 and 15 of the rules. Specifically, it:

(1) Eliminates the requirement for applicants and grantees of certification of software defined radios to supply a copy of the software that controls the RF

[1] *See* 5 U.S.C. 603. The RFA, *see* 5 U.S.C. 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Public Law 104–121, Title II, 110 Stat. 857 (1996).

[2] *See Notice of Proposed Rule Making and Order* in ET Docket No. 03–108, 18 FCC Rcd 26859 (2003), 69 FR 7397, February 17, 2004.

[3] *Id.*

[4] *See* 5 U.S.C. 604.

operating parameters of the radio upon request;

(2) Requires applicants for certification of software defined radios to supply a high level operational description of the software that controls the radio frequency operating parameters;

(3) Requires that radios in which the software that controls the RF operating parameters is designed or expected to be modified by a party other than the manufacturer to incorporate a means to prevent unauthorized software changes, and requires such radios to be certified as software defined radios;

(4) Allows certification of unlicensed transmitters that have the capability of operating outside permissible part 15 frequency bands, provided the transmitters incorporate a software control to limit operation to permissible part 15 frequency bands when used in the United States.

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

41. None.

C. Description and Estimate of the Number of Small Entities To Which the Rules Apply

42. 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.[5] The RFA defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''small business concern'' under section 3 of the Small Business Act.[6] Under the Small Business Act, a ''small business concern'' is one that: (1) Is independently owned and operated; (2) is not dominant in its field of operations; and (3) meets may additional criteria established by the Small Business Administration (SBA).[7]

Wireless Communications Equipment Manufacturers

43. The SBA has established a small business size standard for radio and television broadcasting and wireless communications equipment manufacturing. Under this standard, firms are considered small if they have 750 or fewer employees.[8] Census Bureau data for 1997 indicate that, for that year, there were a total of 1,215 establishments[9] in this category.[10] Of those, there were 1,150 that had employment under 500, and an additional 37 that had employment of 500 to 999. The percentage of wireless equipment manufacturers in this category is approximately 61.35 percent,[11] so the Commission estimates that the number of wireless equipment manufacturers with employment under 500 was actually closer to 706, with and additional 23 establishments having employment of between 500 and 999. Given the above, the Commission estimates that the majority of wireless communications equipment manufacturers are small businesses.

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

44. Unlicensed transmitters are required to be certified before they can be imported into or marketed within the United States. The certification process requires the manufacturer or other party responsible for compliance to have the equipment tested and electronically file an application form, measurement report and other information on the equipment with the Commission or a designated Telecommunication Certification Body (TCB). Software defined radios at present may be approved only by the Commission and not by TCBs, although the Commission has stated that it will eventually allow TCBs to approve them. The Report and Order does not change this requirement.

45. Applicants for certification of a software defined radio will be required to supply a high level operational description of the software that controls the radio frequency operating parameters.

46. Manufacturers of radios in which the software that controls the radio frequency operating parameters is designed or expected to be modified by a party other than the manufacturer must incorporate a means to prevent unauthorized software changes that must be described in the application for certification. Such software changeable radios must be declared as software defined radios in the application for certification. Most radios at the present are not software modifiable, and manufacturers of those that are generally already take steps to prevent unauthorized modifications, so we expect that only rarely would manufacturers have to redesign equipment to comply with this requirement.

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

47. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[12]

48. The Commission sought comment in the *NPRM* about whether it should make compliance with the software defined radio rules, including the requirement to demonstrate that a radio incorporates security features, mandatory rather than optional for certain types of radio transmitters. Based on the comments received, the Commission made these requirements mandatory only for the small subset of radio transmitters in which the software that controls the radio frequency operating parameters is designed or expected to be modified by a party other than the manufacturer. This change will ensure that radio transmitters can not be easily modified and cause interference to authorized services, while minimizing the filing burden on applicants for certification by requiring only a small number of devices to be certified as software defined radios.

49. The Commission simplified the filing requirements for software defined radios to benefit all entities, including

[5] *See* U.S.C. 603(b)(3).

[6] *Id.* 601(3).

[7] *Id.* 632.

[8] 1997 Economic Census, Manufacturing, Industry Series, Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing, Document No. E97M–3342B (August 1999), at 9; 1997 Economic Census, Manufacturing, Industry Series, Other Communications Equipment Manufacturing, Document No. EC97M–3342C (September 1999), at 9 (both available at *http://www.census.gov/prod/www/abs/97ecmani.html).*

[9] The number of ''establishments'' is a less helpful indicator of small business prevalence in this context than would be the number of ''firms'' or ''companies,'' because the latter take into account the concept of common ownership or control. Any single physical locations for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census breaks out data for firms or companies only to give the total number of such entities for 1997, which was 1,089.

[10] U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, ''Industry Statistics by Employment Size,'' Table 4, NAICS code 334220 (issued August 1999).

[11] *Id.* Table 5, ''Industry Statistics by Industry and Primary Product Class Specialization: 1997.''

[12] *See* 5 U.S.C. 603(c).

small entities. It eliminated the requirement to supply software source code upon request because such software is not generally useful for certification review and may have become an unnecessary barrier to entry. The Commission will instead require the submission of a software description at the time of certification as supported by a number of parties in comments. Because such a description would generally be considered company proprietary information, the Commission will automatically hold such information confidential without the need for applicants for certification to file a specific request for confidentiality and pay a fee. Eliminating the need to file a specific confidentiality request and pay a fee is expected to benefit small entities that have fewer resources to comply with regulatory requirements.

F. Congressional Review Act

The Commission will send a copy of the Report and Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act, *see* 5 U.S.C. 801(a)(1)(A). In addition, the Commission will send a copy of the *Report and Order,* including FRFA, to the Chief Counsel for Advocacy of the Small Business Administration.

Ordering Clauses

50. Parts 0, 2, and 15 of the Commission's Rules are amended as specified in rule changes, effective August 2, 2005. This action is taken pursuant to the authority contained in sections 4(i), 301, 302, 303(e), 303(f) and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. sections 154(i), 301, 302, 303(e), 303(f) and 303(r).

51. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, shall send a copy of the *Report and Order,* including the Final Regulatory Flexibility Analysis to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Parts 0, 2, and 15

Communications equipment, Radio. Report and recordkeeping requirements.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

Rule Changes

■ For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 0, 2, and 15 as follows:

PART 0—COMMISSION ORGANIZATION

■ 1. The authority citation for part 0 continues to read as follows:

Authority: Secs. 5, 48 Stat. 1068, as amended; 47 U.S.C. 155.

■ 2. Section 0.457 is amended by revising paragraph (d)(1)(ii) to read as follows:

§ 0.457 Records not routinely available for public inspection.

* * * * *

(d) * * *

(1) * * *

(ii) Applications for equipment authorizations (type acceptance, type approval, certification, or advance approval of subscription television systems), and materials relating to such applications, are not routinely available for public inspection prior to the effective date of the authorization. The effective date of the authorization will, upon request, be deferred to a date no earlier than that specified by the applicant. Following the effective date of the authorization, the application and related materials (including technical specifications and test measurements) will be made available for inspection upon request (See § 0.460). Portions of applications for equipment certification of scanning receivers and related materials will not be made available for inspection. This information includes that necessary to prevent modification of scanning receivers to receive Cellular Service frequencies, such as schematic diagrams, technical narratives describing equipment operation, and relevant design details. Portions of applications for equipment certification of software defined radios that describe the operation of the device's software and security features will not be made available for inspection.

* * * * *

PART 2—FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

■ 3. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303 and 336, unless otherwise noted.

■ 4. Section 2.1(c) is amended by revising the following definition of ''software defined radio'' to read as follows:

§ 2.1 Terms and definitions.

* * * * *

(c) * * *

Software defined radio. A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

* * * * *

§ 2.932 [Amended]

■ 5. Section 2.932 is amended by removing paragraph (e).

■ 6. Section 2.944 is revised to read as follows:

§ 2.944 Software defined radios.

(a) Manufacturers must take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio. The software must not allow the user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

(b) Any radio in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, must comply with the requirements in paragraph (a) of this section and must be certified as a software defined radio.

(c) Applications for certification of software defined radios must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters.

■ 7. Section 2.1033 is amended by adding new paragraphs (b)(12) and (c)(18) to read as follows:

§ 2.1033 Application for certification.

* * * * *

(b) * * *

(12) An application for certification of a software defined radio must include the information required by § 2.944.

* * * * *

(c) * * *

(18) An application for certification of a software defined radio must include the information required by § 2.944.

* * * * *

■ 8. Section 2.1043 is amended by revising paragraph (b)(3) to read as follows:

§ 2.1043 Changes in certificated equipment.

* * * * *

(b) * * *

(3) A Class III permissive change includes modifications to the software of a software defined radio transmitter that change the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules. When a Class III permissive change is made, the grantee shall supply the Commission with a description of the changes and test results showing that the equipment complies with the applicable rules with the new software loaded, including compliance with the applicable RF exposure requirements. The modified software shall not be loaded into the equipment, and the equipment shall not be marketed with the modified software under the existing grant of certification, prior to acknowledgement by the Commission that the change is acceptable. Class III changes are permitted only for equipment in which no Class II changes have been made from the originally approved device.

Note to paragraph (b)(3): Any software change that degrades spurious and out-of-band emissions previously reported to the Commission at the time of initial certification would be considered a change in frequency or modulation and would require a Class III permissive change or new equipment authorization application.

* * * * *

PART 15—RADIO FREQUENCY DEVICES

■ 9. The authority citation of part 15 continues to read as follows:

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

■ 10. Section 15.202 is added to read as follows:

§ 15.202 Certified operating frequency range

Client devices that operate in a master/client network may be certified if they have the capability of operating outside permissible part 15 frequency bands, provided they operate on only permissible part 15 frequencies under the control of the master device with which they communicate. Master devices marketed within the United States must be limited to operation on permissible part 15 frequencies. Client devices that can also act as master devices must meet the requirements of a master device. For the purposes of this section, a master device is defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices. A network always has at least one device operating in master mode. A client device is defined as a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network.

[FR Doc. 05–8808 Filed 5–3–05; 8:45 am]

BILLING CODE 6712–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 660

[Docket No. 040830250–5062–03; I.D. 042205C]

Fisheries Off West Coast States and in the Western Pacific; Pacific Coast Groundfish Fishery; Specifications and Management Measures; Inseason Adjustments; Pacific Halibut Fisheries; Corrections

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Inseason adjustments to management measures; announcement of incidental halibut retention allowance; corrections; request for comments.

SUMMARY: NMFS announces changes to management measures in the commercial and recreational Pacific Coast groundfish fisheries. NMFS also announces regulations for the retention of Pacific halibut landed incidentally in the limited entry longline primary sablefish fishery north of Pt. Chehalis, WA (46°53.30′ N. lat.). This document also contains notification of a voluntary closed area (also called an ''area to be avoided'') off Washington for salmon trollers. These actions, which are authorized by the Pacific Coast Groundfish Fishery Management Plan (FMP), will allow fisheries to access more abundant groundfish stocks while protecting overfished and depleted stocks. This action also corrects the trawl gear regulatory language for chafing gear and selective flatfish trawl gear.

DATES: Effective 0001 hours (local time) May 1, 2005, except that the amendments to 50 CFR 660.381 (b)(5)(i) are effective June 3, 2005. Comments on this rule will be accepted through June 3, 2005.

ADDRESSES: You may submit comments, identified by 042205C, by any of the following methods:

- E-mail: GroundfishInseason2.nwr@noaa.gov. Include I.D. number in the subject line of the message.
- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 206–526–6736, Attn: Carrie Nordeen.
- Mail: D. Robert Lohn, Administrator, Northwest Region, NMFS, Attn: Carrie Nordeen, 7600 Sand Point Way NE, Seattle, WA 98115–0070.

FOR FURTHER INFORMATION CONTACT: Jamie Goen or Carrie Nordeen (Northwest Region, NMFS), phone: 206–526–6140; fax: 206–526–6736; and e-mail: *carrie.nordeen@noaa.gov*.

SUPPLEMENTARY INFORMATION:

Electronic Access

This **Federal Register** document is available on the Government Printing Office's website at: *www.gpoaccess.gov/fr/index.html*.

Background information and documents are available at the NMFS Northwest Region website at: *www.nwr.noaa.gov/1sustfsh/gdfsh01.htm* and at the Pacific Fishery Management Council's website at: *www.pcouncil.org*.

Background

The Pacific Coast Groundfish FMP and its implementing regulations at title 50 in the Code of Federal Regulations (CFR), part 660, subpart G, regulate fishing for over 80 species of groundfish off the coasts of Washington, Oregon, and California. Groundfish specifications and management measures are developed by the Pacific Fishery Management Council (Pacific Council), and are implemented by