This technical correction action does not involve technical standards; thus, the requirements of section 12(d) of the National Technology Transfer and Advancement Act of 1995, 15 U.S.C. 272, do not apply. The rule also does not involve special consideration of environmental justice related issues as required by Executive Order 12898, 59 FR 7629 (February 16, 1994). In issuing this rule, EPA has taken the necessary steps to eliminate drafting errors and ambiguity, minimize potential litigation, and provide a clear legal standard for affected conduct, as required by section 3 of Executive Order 12988, 61 FR 4729 (February 7, 1996). EPA has complied with Executive Order 12630, 53 FR 8859 (March 15, 1988), by examining the takings implications of the rule in accordance with the "Attorney General's Supplemental Guidelines for the Evaluation of Risk and Avoidance of Unanticipated Takings" issued under the executive order. This rule does not impose an information collection burden under the provisions of the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.* EPA's compliance with these statutes and Executive Orders for the underlying rule is discussed in the December 1, 2009 **Federal Register** notice. 74 FR 62995.

The Congressional Review Act, 5 U.S.C. 801 *et seq.,* as added by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. Section 808 allows the issuing agency to make a rule effective sooner than otherwise provided by the CRA if the agency makes a good cause finding that notice and public procedure is impracticable, unnecessary or contrary to the public interest. This determination must be supported by a brief statement. 5 U.S.C. 808(2). As stated previously, EPA has made such a good cause finding, including the reasons therefor, and established an effective date of March 8, 2010. The effective date of today's correction is earlier than 30 days after publication. EPA finds that the earlier effective date clarifies the applicability date of the numeric effluent limit and associated monitoring requirements for sites that disturb 20 or more acres of land at one time for all stakeholders. Today's amendment eliminates an inconsistency and thus, reduces the opportunity for confusion. Any additional delay in correcting the error would only increase the potential confusion. Thus, EPA sets an effective date to make the correction immediately effective. EPA will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States prior to publication of the rule in the **Federal Register**. This action is not a "major rule" as defined by 5 U.S.C. 804(2).

List of Subjects in 40 CFR Part 450

Environmental protection, Construction industry, Land development, Erosion, Sediment, Stormwater, Water pollution control.

Dated: March 1, 2010.

Peter S. Silva,

Assistant Administrator for Water.

■ Accordingly, 40 CFR Part 450 is corrected by making the following correcting amendments:

PART 450—CONSTRUCTION AND DEVELOPMENT POINT SOURCE CATEGORY

■ 1. The authority citation for part 450 continues to read as follows:

Authority: 42 U.S.C. 101, 301, 304, 306, 308, 401, 402, 501 and 510.

■ 2. Revise the introductory text of paragraph (a) of § 450.22 to read as follows:

§ 450.22 Effluent limitations reflecting the best available technology economically achievable (BAT).

* * * * *

(a) Beginning no later than August 1, 2011 during construction activity that disturbs 20 or more acres of land at one time, including non-contiguous land disturbances that take place at the same time and are part of a larger common plan of development or sale; and no later than February 2, 2014 during construction activity that disturbs ten or more acres of land area at one time, including non-contiguous land disturbances that take place at the same time and are part of a larger common plan of development or sale, the following requirements apply:

* * * * *

[FR Doc. 2010–4823 Filed 3–5–10; 8:45 am]

BILLING CODE 6560–50–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 2

[ET Docket No. 03–108; FCC 10–12]

Cognitive Radio Technologies and Software Defined Radios

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: This document dismisses a petition for reconsideration filed by the SDR Forum requesting that the Commission modify the policy statements it made in the *Memorandum Opinion and Order (MO&O)* in this proceeding concerning the use of open source software to implement security features in software defined radios (SDRs). While, the Commission dismisses this petition on procedural grounds, it also provides clarification concerning the issues raised therein.

DATES: Effective April 7, 2010.

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

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Memorandum Opinion and Order,* ET Docket No. 03–108, adopted January 14, 2010, and released January 19, 2010. 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 Memorandum Opinion and Order

1. On March 17, 2005, the Commission adopted the *Cognitive Radio Report and Order,* 70 FR 23032, May 4, 2005, in which the rules were modified to reflect ongoing technical developments in cognitive and software defined radio (SDR) technologies.

2. On April 20, 2007, the Commission adopted a *Memorandum Opinion and Order* (MO&O), 72 FR 31190, June 6, 2007, which responded to two petitions filed in response to the *Cognitive Radio Report and Order.* The Commission,

inter alia, granted a petition for clarification filed by Cisco Systems, Inc. ("Cisco") requesting that the Commission clarify: (1) The requirement to approve certain devices as software defined radios; and (2) its policy on the confidentiality of software that controls security measures in software defined radios.

3. In responding to the Cisco petition, the Commission stated that with regard to the use of open source software for implementing software defined radio security measures:

> "* * * manufacturers should not intentionally make the distinctive elements that implement that manufacturer's particular security measures in a software defined radio public, if doing so would increase the risk that these security measures could be defeated or otherwise circumvented to allow operation of the radio in a manner that violates the Commission's rules. A system that is wholly dependent on open source elements will have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio."

4. The SDR Forum filed a petition for reconsideration on July 3, 2007, requesting that the Commission modify the statements.

5. In its petition, the SDR Forum expresses concern that the language in the *MO&O* on the use of open source software for implementing SDR security measures may inadvertently pose a barrier to the development and wide implementation of security techniques that would ensure compliance with the Commission's rules. SDR recommends that these policy statements be modified, stating that manufacturers should have the discretion to discuss their security measures in public so long as the intent of the disclosure is not to enable circumvention of the Commission's rules. The SDR Forum states that the Commission should remain neutral on the security of open source elements because open source approaches are no less secure than proprietary techniques. It specifically requests that the Commission modify the text quoted above by:

> "revising the first sentence to state "a manufacturer may make public its SDR security mechanisms so long as the intent is not to circumvent compliance with Commission rules;" and by deleting the second sentence."

6. The Commission is dismissing the SDR Forum petition for reconsideration on procedural grounds. While the SDR Forum filed comments in response to the *NPRM* in this proceeding, it did not submit comments in response to the Cisco petition for reconsideration that raised the issue of using open source software to implement software defined radio security mechanisms. The Cisco petition was addressed in the Commission's *MO&O* for which the SDR Forum now requests reconsideration. A petition for reconsideration that relies on facts not previously presented to the Commission will be granted only if:

(a) The facts relied on relate to events which have occurred or circumstances which have changed since the last opportunity to present them to the Commission;

(b) The facts relied upon were unknown to the petitioner until after his last opportunity to present them to the Commission, and the petition could not through the exercise of due diligence have learned of the facts in question prior to such opportunity; or

(c) The Commission determines that consideration of the facts relied on is required in the public interest.

The SDR Forum petition does not address why it did not respond to the Cisco petition or claim that any of these three conditions are met in this case. Accordingly, the SDR Forum's petition for reconsideration is procedurally defective and is hereby dismissed. However, the Commission recognizes that the issue of open source software in software defined radios is of interest to the SDR Forum and other parties. Accordingly, the Commission is taking this opportunity to clarify its policies with respect to the use of open source software for implementing security features in software defined radios.

7. The Commission's rules require that a software defined radio manufacturer 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 radio frequency parameters other than those that were approved by the Commission. The Commission's rules require that the manufacturer have reasonable security measures to prevent unauthorized modifications that would affect the RF operating parameters or the circumstances under which the transmitter operates in accordance with Commission rules. Manufacturers may select the methods used to meet these requirements and must describe them in their application for equipment authorization.

8. When a party applies for certification of a software defined radio, the description of the security methods used in the radio is automatically held confidential. The Commission does this because such information often is proprietary and also because revelation of the security methods, or portions thereof, could possibly assist parties in defeating the security features and enable operation of the radio outside the Commission's rules. Out of an abundance of caution—because operation of a radio outside the Commission's rules could result in harmful interference to a wide variety of radio services, including safety-of-life services—the Commission holds the entire description of the security measures confidential. Therefore, the Commission's staff does not have to determine which portions of a software defined radio security methods description filed with an application could be made publicly available without risk that such disclosure could assist parties in defeating the security measures. Further, by automatically holding the description confidential, applicants for certification do not have to specifically request confidentiality for the description of a radio's security mechanisms.

9. Neither the Commission's rules whereby it maintains the confidentiality of a software defined radio's security mechanism nor the policy stated in the *MO&O* prohibit radio manufacturers and software developers from sharing information on the design of security methods with other manufacturers and developers. Rather, the Commission's policy stated only that manufacturers should not make the "distinctive elements" of security features publicly available, if doing so would increase the risk that security measures could be defeated or circumvented to allow operation of a radio in a manner that violates the rules. The Commission's intent was not to prohibit manufacturers from collaborating and sharing information that could allow them to develop more robust security features or reduce the cost of implementing them. In fact, the Commission would encourage such work by industry. The Commission's concern is only with disclosure of those particular elements of a security scheme when such disclosure could facilitate defeating the security scheme. Thus, manufacturers can make whatever information they wish concerning their security methods public, provided they can demonstrate the implementation has a means of controlling access to the distinctive elements that could allow parties to defeat or circumvent the security methods.

10. The Commission emphasizes that it does not prohibit the use of open source software in implementing software defined radio security features. The Commission's concern with open source software is that disclosure of

certain elements of a security scheme could assist parties in defeating the scheme. As Cisco stated in its petition, licensing agreements may require that open source software code be made publicly available. This could potentially lead to public disclosure of this information. For these reasons, the Commission stated in the *MO&O* that a system that is wholly dependent on open source elements would have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio. However, the Commission's statements in the *MO&O* were not intended to prohibit the use of open source software or discourage its use. All applicants seeking to certify a software defined radio are held to the same standard, *i.e.,* they must demonstrate that the radio contains security features sufficient to prevent unauthorized modifications to the radio frequency operating parameter. A party applying for certification of a software defined radio would need to show that public disclosure of the source code would not assist parties in defeating the security scheme, or that disclosure of the distinctive elements of the security scheme would not assist parties in defeating the security scheme. As the SDR Forum notes, security mechanisms can rely on a variety of means to control access, such as keys, passwords or biometric data.

11. Finally, as software defined radio and security technologies continue to develop and mature, the Commission may address the rules for software defined radios, including their security requirements, in future proceedings. The Commission encourages the SDR Forum and other interested parties to participate in such proceedings.

Ordering Clauses

12. The petition for reconsideration filed by the SDR Forum IS *hereby dismissed.* 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).

13. *It is further ordered* that ET Docket No. 03–108 *is terminated.*

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

[FR Doc. 2010–4855 Filed 3–5–10; 8:45 am]

BILLING CODE 6712–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 679

[Docket No. 09100091344–9056–02]

RIN 0648–XU89

Fisheries of the Exclusive Economic Zone Off Alaska; Pacific Cod by Vessels Catching Pacific Cod for Processing by the Offshore Component in the Western Regulatory Area of the Gulf of Alaska

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

ACTION: Temporary rule; closure.

SUMMARY: NMFS is prohibiting directed fishing for Pacific cod by vessels catching Pacific cod for processing by the offshore component in the Western Regulatory Area of the Gulf of Alaska (GOA). This action is necessary to prevent exceeding the A season allocation of the 2010 total allowable catch (TAC) of Pacific cod apportioned to vessels catching Pacific cod for processing by the offshore component of the Western Regulatory Area of the GOA.

DATES: Effective 1200 hrs, Alaska local time (A.l.t.), March 3, 2010, through 1200 hrs, A.l.t., September 1, 2010.

FOR FURTHER INFORMATION CONTACT: Josh Keaton, 907–586–7228.

SUPPLEMENTARY INFORMATION: NMFS manages the groundfish fishery in the GOA exclusive economic zone according to the Fishery Management Plan for Groundfish of the Gulf of Alaska (FMP) prepared by the North Pacific Fishery Management Council under authority of the Magnuson-Stevens Fishery Conservation and Management Act. Regulations governing fishing by U.S. vessels in accordance with the FMP appear at subpart H of 50 CFR part 600 and 50 CFR part 679.

The A season allocation of the 2010 TAC of Pacific cod apportioned to vessels catching Pacific cod for processing by the offshore component of the Western Regulatory Area of the GOA is 1,246 metric tons (mt) as established by the final 2009 and 2010 harvest specifications for groundfish of the GOA (74 FR 7333, February 17, 2010) and inseason adjustment (74 FR 68713, December 29, 2009).

In accordance with § 679.20(d)(1)(i), the Regional Administrator has determined that the A season allocation of the 2010 TAC of Pacific cod apportioned to vessels catching Pacific cod for processing by the offshore component of the Western Regulatory Area of the GOA will soon be reached. Therefore, the Regional Administrator is establishing a directed fishing allowance of 1,096 mt, and is setting aside the remaining 150 mt as bycatch to support other anticipated groundfish fisheries. In accordance with § 679.20(d)(1)(iii), the Regional Administrator finds that this directed fishing allowance has been reached. Consequently, NMFS is prohibiting directed fishing for Pacific cod by vessels catching Pacific cod for processing by the offshore component in the Western Regulatory Area of the GOA.

After the effective date of this closure the maximum retainable amounts at § 679.20(e) and (f) apply at any time during a trip.

Classification

This action responds to the best available information recently obtained from the fishery. The Assistant Administrator for Fisheries, NOAA (AA), finds good cause to waive the requirement to provide prior notice and opportunity for public comment pursuant to the authority set forth at 5 U.S.C. 553(b)(B) as such requirement is impracticable and contrary to the public interest. This requirement is impracticable and contrary to the public interest as it would prevent NMFS from responding to the most recent fisheries data in a timely fashion and would delay the closure of Pacific cod apportioned to vessels catching Pacific cod for processing by the offshore component of the Western Regulatory Area of the GOA. NMFS was unable to publish a notice providing time for public comment because the most recent, relevant data only became available as of March 2, 2010.

The AA also finds good cause to waive the 30-day delay in the effective date of this action under 5 U.S.C. 553(d)(3). This finding is based upon the reasons provided above for waiver of prior notice and opportunity for public comment.

This action is required by § 679.20 and is exempt from review under Executive Order 12866.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: March 3, 2010.

Emily H. Menashes,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2010–4857 Filed 3–3–10; 4:15 pm]

BILLING CODE 3510–22–S