implement statutory amendments to the Immigration and Nationality Act (INA), made by the Immigration Act of 1990 (IMMACT '90), Pub. L. 101–649. Sections 101, 111, 112, 121 and 162(b)(1)(E) of IMMACT '90 restructured INA 203. Most of the changes to the regulations in the Interim Rule are editorial and relate primarily to numerical designations and citations. IMMACT '90 sections 101 and 121 amended the INA by separating family-related immigration from employment-related immigration and created new preference classes. These changes required the transfer of several regulations from subpart C of this part to subpart D, which more appropriately relates to immigrants subject to numerical limitations. In addition, the regulation at 22 CFR 42.21 was amended to add language benefiting spouses of deceased U.S. citizens entitled to immediate relative status. The regulations published with Interim Rule 1491 will continue to retain the effective date of October 1, 1991.

EFFECTIVE DATE: This final rule is effective September 16, 1993.

FOR FURTHER INFORMATION CONTACT: Stephen K. Fischel, Chief, Legislation and Regulations Division, Visa Services, Department of State, Washington, DC 20522–0113, (202) 663–1204.

SUPPLEMENTARY INFORMATION: Sections 101, 111, 112, 121 and 162(b)(1)(E) of IMMACT '90 restructured section 203 of the INA. Those changes in turn affected part 42, title 22 of the Code of Federal Regulations. Consequently, former §§ 42.24–42.27 in subpart C were redesignated as §§ 42.32(d) (1) through (4) and transferred to subpart D, which pertains to aliens subject to numerical ceilings; subpart D was substantially restructured because of the additional classes relating to immigrants subject to numerical limitations formerly listed in subpart C. Sections 42.34, 42.35 and 42.36 were deleted from subpart C as no longer falling within the criteria of immigrants not subject to numerical limitations. In addition, the imposition of a petition requirement under INA 204, as amended by IMMACT '90 section 162(b)(1)(E), on certain special immigrant classes vests the Immigration and Naturalization Service with the responsibility for determining that the alien qualifies as a special immigrant. Prior to the IMMACT '90 such responsibility was vested in the consular officer. Interim Rule 1491, published in the **Federal Register** at 56 FR 49675, October 1, 1991, invited interested persons to submit comments concerning the amendments therein. No comments were received.

PART 42—[AMENDED]

1. Authority citation for part 42 continues to read as follows:

Authority: 8 U.S.C. 1104; 8 U.S.C. 1101 note.

2. Accordingly, the Interim Rule's regulations and effective date of October 1, 1991 at part 42, FR 49675 are adopted without changes.

Dated: September 3, 1993.

Mary A. Ryan,

Assistant Secretary for Consular Affairs.

[FR Doc. 93–22629 Filed 9–15–93; 8:45 am]

BILLING CODE 4710–06–M

---

22 CFR Part 42

[Public Notice 1864]

Visas: Documentation of Immigrants Under the Immigration and Nationality Act, as Amended; Miscellaneous Amendments

AGENCY: Bureau of Consular Affairs, DOS.

ACTION: Final rule.

SUMMARY: This final rule is a followup to Interim Rule 1490, published at page 49678, FR 56, October 1, 1991. The Interim Rule amended part 42 of title 22, Code of Federal Regulations, to implement statutory revisions to the Immigration and Nationality Act (INA) made by the Immigration Act of 1990 (IMMACT '90), Pub. L. 101–649. Most of the amendments are editorial. In addition to the editorial changes, the Interim Rule revised a substantive procedure in § 42.83 for initiating action to terminate the registration of an alien entitled to an immigrant status. The regulations contained in the Interim Rule, § § 42.11 through 42.83, will continue to retain the effective date of October 1, 1991.

EFFECTIVE DATE: This final rule is effective September 16, 1993.

FOR FURTHER INFORMATION CONTACT: Stephen K. Fischel, Chief, Legislation and Regulations Division, Visa Services, Department of State, Washington, DC 20522–0113, (202) 663–1204.

SUPPLEMENTARY INFORMATION: Except for the regulations in subpart C, relating to individual classes of aliens, subpart D, relating to special immigrants under INA 101(a)(27)(D), and subpart F, relating to numerical controls and priority dates, the Interim Rule contains all other regulations in part 42 which was affected by the Immigration Act of 1990. The majority of those changes are editorial and reflect statutory provisions mandated by Public Law 101–649.

Interim Rule 1490, published in the **Federal Register** at 56 FR 49678, October 1, 1991, invited interested persons to submit comments concerning the amendments therein. No comments were received.

PART 42—[AMENDED]

1. Authority citation for part 42 continues to read as follows:

Authority: 8 U.S.C. 1104; 8 U.S.C. 1101 note.

2. Accordingly, the Interim Rule's regulations and effective date of October 1, 1991 at 56 FR 49678 are adopted without changes.

September 2, 1993.

Mary A. Ryan,

Assistant Secretary for Consular Affairs.

[FR Doc. 93–22630 Filed 9–15–93; 8:45 am]

BILLING CODE 4710–06–M

UNITED STATES INFORMATION AGENCY

22 CFR Part 514

[Rulemaking No. 102]

Exchange-Visitor Program

AGENCY: United States Information Agency.

ACTION: Notice of final rule; correction.

SUMMARY: The Agency issued a final rule on March 19, 1993 at 58 FR 15180–15220. This notice corrects several inadvertent administrative errors which appeared in the final rule.

DATES: March 19, 1993.

ADDRESSES: Stanley S. Colvin, Assistant General Counsel, Office of the General Counsel, room 700, United States Information Agency, 301 Fourth Street, SW., Washington, DC 20547, (202) 619–6829.

FOR FURTHER INFORMATION CONTACT: Stanley S. Colvin, Assistant General Counsel, Office of the General Counsel, room 700, United States Information Agency, 301 Fourth Street, SW., Washington, DC 20547, (202) 619–6829.

SUPPLEMENTARY INFORMATION: On March 19, 1993 the Agency published final regulations governing the administration of the Exchange Visitor Program. 58 FR 15180–15220. Upon its review of the published regulations, the Agency discovered several inadvertent typographical and other administrative

errors. The purpose of this notice is to correct those errors.

R. Wallace Stuart,
Acting General Counsel.

List of Subjects in 22 CFR Part 514

Cultural Exchange Programs.

PART 514—[AMENDED]

Accordingly, the United States Information Agency is correcting the final rule published March 19, 1993, as follows:

1. The *Supplementary Information* section dealing with Subpart B: Specific Program Provisions, which appears at 58 FR 15185, is corrected in the third column, in the first complete paragraph, by deleting the reference to 8 CFR 274.1(j) and inserting in lieu thereof "8 CFR 274a.1(j)."

2. The *Supplementary Information* section dealing with Subpart C: Status of Exchange Visitors, which appears at 58 FR 15193, is corrected by deleting the words "in INS adjudication" in the third full paragraph in the third column.

§ 514.20 [Amended]

3. Section 514.20(j)(1), appearing at 58 FR 15202, is corrected by deleting "§ 514.43(c)" in the last full line of the paragraph, and inserting in lieu thereof, "§ 514.43(b)".

4. The heading of § 514.20 Short-term scholars, appearing at 58 FR 15203, is corrected to read "§ 514.21 Short-term scholars."

§ 514.22 [Amended]

5. Section 514.22(d)(1)(iv), which appears at 52 FR 15204 is corrected by deleting the word "of" before the word "evaluation", and adding the word "of" before the word "each".

§ 514.27 [Amended]

6. Section 514.27(b)(2), which appears at 58 FR 15209, is corrected by deleting the word "Will" before the words "be able".

7. Section 514.27(e)(1), which appears at 58 FR 15209, is corrected by adding the words "as described in paragraph (b) of this section" after the word "training" and before the word "is".

§ 514.44 [Amended]

8. Section 514.44(a)(2), appearing at 58 FR 15212, is corrected by deleting the word "national" in the last line of the paragraph, and inserting in lieu thereof, the word "public."

9. Section 514.44(f)(4)(iv), appearing at 58 FR 15213, is corrected by deleting the word "Board" in the last line of the paragraph, and inserting in lieu thereof, the word "Branch."

[FR Doc. 93–22585 Filed 9–15–93; 8:45 am]
BILLING CODE 8230–01–M

DEPARTMENT OF JUSTICE

Office of Justice Programs

28 CFR Part 23

Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies

AGENCY: Office of Justice Programs, Justice.

ACTION: Final rule.

SUMMARY: The regulation governing criminal intelligence systems operating through support under title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines.

EFFECTIVE DATE: September 16, 1993.

FOR FURTHER INFORMATION CONTACT: Olga R. Trujillo, Acting General Counsel, Office of Justice Programs, 633 Indiana Ave., NW., room 1268, Washington, DC 20531, Telephone (202) 307–0790.

SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the **Federal Register** on February 27, 1992, (57 FR 6691).

The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows:

Confidentiality of Information

Sec. 812 * * *

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

This statutory provision and its implementing regulation apply to intelligence systems funded under title I of the Act, whether the system is operated by a single law enforcement agency, is an interjurisdictional intelligence system, is funded with discretionary grant funds, or is funded by a State with formula grant funds awarded under the Act's Drug Control and System Improvement Grant Program pursuant to part E, subpart 1 of the Act, 42 U.S.C. 3751–3759.

The need for change to 28 CFR part 23 grew out of the program experience of the Office of Justice Programs (OJP) and its component agency, the Bureau of Justice Assistance (BJA), with the regulation and the changing and expanding law enforcement agency need to respond to criminal mobility, the National drug program, the increased complexity of criminal networks and conspiracies, and the limited funding available to State and local law enforcement agencies. In addition, law enforcement's capability to perform intelligence database and analytical functions has been enhanced by technological advancements and sophisticated analytical techniques.

28 CFR part 23 governs the basic requirements of the intelligence system process. The process includes—

1. Information submission or collection
2. Secure storage
3. Inquiry and search capability
4. Controlled dissemination, and
5. Purge and review process

Information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation. The definition includes both systems that store detailed intelligence or investigative information on the suspected criminal activities of subjects and those which store only information designed to identify individuals or organizations that are the subject of an inquiry or analysis (a so-called "pointer system"). It does not include criminal history record information or identification (fingerprint) systems.

There are nine significant areas of change to the regulation:

(1) Nomenclature changes (authority citations, organizational names) are included to bring the regulation up to date.

(2) Definitions of terms (28 CFR 23.3(b)) are modified or added as appropriate. The term "intelligence system" is redefined to clarify the fact that historical telephone toll files, analytical information, and work

products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation; the terms "interjurisdictional intelligence system", "criminal intelligence information", "participating agency", "intelligence project", and "validation of information" are key terms that are defined in the regulation for the first time.

(3) The operating principles for intelligence systems (28 CFR 23.20) are modified to define the term "reasonable suspicion" or "criminal predicate". The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence data base (28 CFR 23.20(c)). This determination, as well as determinations that information was legally obtained (28 CFR 23.20(d)) and that a recipient of the information has a need to know and a right to know the information in the performance of a law enforcement function (28 CFR 23.20(e)), are established as the responsibility of the project for an interjurisdictional intelligence system. However, the regulation permits these responsibilities to be delegated to a properly trained participating agency which is subject to project inspection and audit (28 CFR 23.20 (c), (d), (g)).

(4) Security requirements are established to protect the integrity of the intelligence data base and the information stored in the data base (28 CFR 23.20(g)(1) (i)–(vi)).

(5) The regulation provides that information retained in the system must be reviewed and validated for continuing compliance with system submission criteria within a 5-year retention period. Any information not validated within that period must be purged from the system (28 CFR 23.20(h)).

(6) Another change continues the general prohibition of direct remote terminal access to intelligence information in a funded intelligence system but provides an exception for systems which obtain express OJP approval based on a determination that the system has adequate policies and procedures in place to insure that access to system intelligence information is limited to authorized system users (28 CFR 23.20(i)(1)). OJP will carefully review all requests for exception to assure that a need exists and that system integrity will be provided and maintained (28 CFR 23.20(i)(1)).

(7) The regulation requires participating agencies to maintain back-up files for information submitted to an interjurisdictional intelligence system and provide for inspection and audit by project staff (28 CFR 23.20(h)).

(8) The final rule also includes a provision allowing the Attorney General or the Attorney General's designee to authorize a departure from the specific requirements of this part, in those cases where it is clearly shown that such waiver would promote the purposes and effectiveness of a criminal intelligence system while at the same time ensuring compliance with all applicable laws and protection for the privacy and constitutional rights of individuals. The Department recognizes that other provisions of federal law may be applicable to (or may be adopted in the future with respect to) certain submitters or users of information in criminal intelligence systems. Moreover, as technological developments unfold over time in this area, experience may show that particular aspects of the requirements in this part may no longer be needed to serve their intended purpose or may even prevent desirable technological advances. Accordingly, this provision grants the flexibility to make such beneficial adaptations in particular cases or classes without the necessity to undertake a new rulemaking process. This waiver authority could only be exercised by the Attorney General or designee, in writing, upon a clear and convincing showing (28 CFR 23.20 (o)).

(9) The funding guidelines (28 CFR 23.30) are revised to permit funded intelligence systems to collect information either on organized criminal activity that represents a significant and recognized threat to the population or on criminal activity that is multi-jurisdictional in nature.

Rulemaking History

On February 27, 1992, the Department of Justice, Office of Justice Programs, published a notice of proposed rulemaking in the **Federal Register** (57 FR 6691).

The Office of Justice Programs received a total of eleven comments on the proposed regulation, seven from State agencies, two from Regional Information Sharing Systems (RISS) program fund recipients, one from a Federal agency, and one from the RISS Project Directors Association. Comments will be discussed in the order in which they address the substance of the proposed regulation.

Discussion of Comments

Title—Part 23

Comment: One commentor suggested reinserting the word "Operating" in the title of the regulation to read "Criminal Intelligence Systems Operating Policies" to reflect that the regulation applies only to policies governing system operations.

Response: Agreed. The title has been changed.

Applicability—Section 23.3(a)

Comment: A question was raised by one respondent as to whether the applicability of the regulation under § 23.3(a) to systems "operating through support" under the Crime Control Act included agencies receiving any assistance funds and who operated an intelligence system or only those who received assistance funds for the specific purpose of funding the operation of an intelligence system.

Response: The regulation applies to grantees and subgrantees who receive and use Crime Control Act funds to fund the operation of an intelligence system.

Comment: Another commentor asked whether the purchase of software, office equipment, or the payment of staff salaries for a criminal intelligence system would constitute "operating through support" under the Crime Control Act.

Response: Any direct Crime Control Act fund support that contributes to the operation of a criminal intelligence system would subject the system to the operation of the policy standards during the period of fund support.

Comment: A third commentor inquired whether an agency's purchase of a telephone pen register or computer equipment to store and analyze pen register information would subject the agency or its information systems to the regulation.

Response: No, neither a pen register nor equipment to analyze telephone toll information fall under the definition of a criminal intelligence system even though they may assist an agency to produce investigative or other information for an intelligence system.

Applicability—Section 23.3(b)

Comment: Several commentors questioned whether information systems that are designed to collect information on criminal suspects for purposes of inquiry and analysis, and which provide for dissemination of such information, qualify as "criminal intelligence systems." One pointed out that the information qualifying for system submission could not be

"unconfirmed" or "soft" intelligence. Rather, it would generally have to be investigative file-based information to meet the "reasonable suspicion" test.

Response: The character of an information system as a criminal intelligence system does not depend upon the source or categorization of the underlying information as "raw" or "soft" intelligence, preliminary investigation information, or investigative information, findings or determinations. It depends upon the purpose for which the information system exists and the type of information it contains. If the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity, and the information is identifying or descriptive information about the individual and the suspected criminal activity, then the system is a criminal intelligence system for purposes of the regulation. Only those criminal intelligence systems that receive, store and provide for the interagency exchange and analysis of criminal intelligence information in a manner consistent with this regulation are eligible for funding support with Crime Control Act funds.

Comment: One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems.

Response: No. A CHRI system contains information collected on arrests, detention, indictments, informations or other charges, dispositions, sentencing, correctional supervision, and release. It encompasses systems designed to collect, process, preserve, or disseminate such information.

CHRI is factual, historical and objective information which provides a criminal justice system "profile" of an individual's past and present involvement in the criminal justice system. A fugitive file is designed to provide factual information to assist in the arrest of individuals for whom there is an outstanding want or warrant. Criminal intelligence information, by contrast, is both factual and conjectural (reasonable suspicion), current and subjective. It is intended for law enforcement use only, to provide law enforcement officers and agencies with useful information on criminal suspects and to foster interagency coordination and cooperation. A criminal intelligence system can have criminal history record information in it as an identifier but a CHRI system would not contain the suspected criminal activity information contained in a criminal intelligence system.

This distinction provides the basis for the limitations on criminal intelligence systems set forth in the operating policies. Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.

Comment: Another commentor asked whether a law enforcement agency's criminal intelligence information unit, located at headquarters, which authorizes no outside access to information in its intelligence system, would be subject to the regulation.

Response: No. The sharing of investigative or general file information on criminal subjects within an agency is a practice that takes place on a daily basis and is necessary for the efficient and effective operation of a law enforcement agency. Consequently, whether such a system is described as a case management or intelligence system, the regulation is not intended to apply to the exchange or sharing of such information when it takes place within a single law enforcement agency or organizational entity. For these purposes, an operational multi-jurisdictional task force would be considered a single organizational entity provided that it is established by and operates under a written memorandum of understanding or interagency agreement. The definition of "Criminal Intelligence System" has been modified to clarify this point. However, if a single agency or entity system provides access to system information to outside agencies on an inquiry or request basis, as a matter of either policy or practice, the system would qualify as a criminal intelligence system and be subject to the regulation.

Comment: A commentor questioned whether the proposed exclusion of "analytical information and work products" from the definition of "Intelligence System" was intended to exclude all dissemination of analytical results from coverage under the regulation.

Response: No. The exceptions in the proposed definition of "Intelligence System" of modus operandi files, historical telephone toll files and analytical information and work products are potentially confusing. The exceptions reflect types of data that may or may not qualify as "Criminal Intelligence Information" depending on particular facts and circumstances. Consequently, these exceptions have been deleted from the definition of "Intelligence System" in the final rule. For example, analytical information and work products that are derived from unevaluated or bulk data (i.e. information that has not been tested to determine that it meets intelligence system submission criteria) are not intelligence information if they are returned to the submitting agency. This information and its products cannot be retained, stored, or made available for dissemination in an intelligence system unless and until the information has been evaluated and determined to meet system submission criteria. The proposed definition of "Analytical Information and Work Products" in § 23.3(b) has also been deleted.

To address the above issues, the definition of "Intelligence System" has been modified to define a "Criminal Intelligence System or Intelligence System" to mean "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information."

Comment: Several commentors raised questions regarding the concept of "evaluated data" in the definition of "Criminal Intelligence Information", requesting guidance on what criteria to use in evaluating data. Another questioned whether there needed to be an active investigation as the basis for information to fall within the definition and whether information on an individual who or organization which is not the primary subject or target of an investigation or other data source, e.g. a criminal associate or co-conspirator, can qualify as "Criminal Intelligence Information."

Response: The definition of "Criminal Intelligence Information" has been revised to reflect that data is evaluated for two purposes related to criminal intelligence system submissions: (1) To determine that it is relevant in identifying a criminal suspect and the criminal activity involved; and (2) to determine that the data meets criminal intelligence system submission criteria, including reasonable suspicion of involvement in criminal activity. As rewritten, there is no requirement that an "active investigation" is necessary. Further, the revised language makes it clear that individuals or organizations who are not primary subjects or targets can be identified in the criminal intelligence information, provided that

they independently meet system submission criteria.

Comment: One commentor requested clarification of the role of the "Project" in the operation of an intelligence system, i.e. is the project required to have physical control (possession) of the information in an intelligence system or will authority over the system (operational control) suffice?

Response: Operational control over an intelligence system's intelligence information is sufficient. The regulation seeks to establish a single locus of authority and responsibility for system information. Once that principle is established, the regulation permits, for example, the establishment of remote (off premises) data bases that meet applicable security requirements.

Operating Principles—Section 23.20(c)

Comment: One respondent took the position that "Reasonable Suspicion", as defined in § 23.20(c), is not necessary to the protection of individual privacy and Constitutional rights, suggesting instead that information in a funded intelligence system need only be "necessary and relevant to an agency's lawful purposes."

Response: While it is agreed that the standard suggested is appropriate for investigative or other information files maintained for use by or within an agency, the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of "hits" in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Comment: The prior commentor also criticized the proposed definition of reasonable suspicion for its specific reference to an "investigative file" as the source of intelligence system information, the potential inconsistency between the concepts of "infer" and "conclude" as standards for determining whether reasonable suspicion is justified by the information available, and the use of "reasonable possibility" rather than "articulable" or "sufficient" facts as the operative standard to conclude that reasonable suspicion exists.

Response: The reference to an "investigative file" as the information source has been broadened to encompass any information source. The information available must provide a basis for the submitter to "believe" there is a reasonable possibility of the subject's involvement in the criminal activity or enterprise. The concept of a "basis to believe" requires reasoning and logic coupled with sound judgment based on experience in law enforcement rather than a mere hunch, whim, or guess. The belief that is formed, that there is a "reasonable possibility" of criminal involvement, has been retained because the proposed standard is appropriately less restrictive than that which is required to establish probable cause.

Operating Principles—Section 23.20(d)

Comment: Section 23.20(d) prohibits the inclusion in an intelligence system of information obtained in violation of Federal, State, or local law or ordinance. Would a project be potentially liable for accepting, maintaining and disseminating such information even if it did not know that the information was illegally obtained?

Response: In addition to protecting the rights of individuals and organizations that may be subjects in a criminal intelligence system, this prohibition serves to protect a project from liability for disseminating illegally obtained information. A clear project policy that prohibits the submission of illegally obtained information, coupled with an examination of supporting information to determine that the information was obtained legally or the delegation of such authority to a properly trained participating agency, and the establishment and performance of routine inspection and audit of participating agency records, should be sufficient to shield a project from potential liability based on negligence in the performance of its intelligence information screening function.

Operating Principles—Section 23.20(h)

Comment: One commentor requested clarification of the "periodic review" requirement in § 23.20(h) and what constitutes an "explanation of decision to retain" information.

Response: The periodic review requirement is designed to insure that system information is accurate and as up-to-date as reasonably possible. When a review has occurred, the record is appropriately updated and notated. The explanation of decision to retain can be a variety of reasons including "active investigation", "preliminary review in progress", "subject believed still active in jurisdiction", and the like. When information that has been reviewed or updated and a determination made that it continues to meet system submission criteria, the information has been "validated" and begins a new retention period. The regulation limits the retention period to a maximum of five years without a review and validation of the information.

Operating Principles—Section 23.20(i)

Comment: One commentor requested a definition of "remote terminal" and asked how OJP would determine whether "adequate policies and procedures" are in place to insure the continued integrity of a criminal intelligence system.

Response: A "remote terminal" is hardware that enables a participating agency to input into or access information from a project's criminal intelligence database without the intervention of project staff. While the security requirements set forth in § 23.20(g)(1)–(5) should minimize the threat to system integrity from unauthorized access to and the use of system information, special measures are called for when direct remote terminal access is authorized.

The Office of Justice Programs will expect any request for approval of remote terminal access to include information on the following system protection measures:

1. Procedures for identification of authorized remote terminals and security of terminals;
2. Authorized access officer (remote terminal operator) identification and verification procedures;
3. Provisions for the levels of dissemination of information as directed by the submitting agency;
4. Provisions for the rejection of submissions unless critical data fields are completed;
5. Technological safeguards on system access, use, dissemination, and review and purge;
6. Physical security of the system;
7. Training and certification of system-participating agency personnel;
8. Provisions for the audit of system-participating agencies, to include: file data supporting submissions to the system; security of access terminals; and policy and procedure compliance; and
9. Documentation for audit trails of the entire system operation.

Moreover, a waiver provision has been added to ensure flexibility in adapting quickly to technological and legal changes which may impact any of the requirements contained in this regulation. See § 23.20(o).

Comment: Related to the above discussion, another commentor asked whether restrictions on direct remote terminal access would prohibit remote

access to an "index" of information in the system.

Response: Yes. The ability to obtain all information directly from a criminal intelligence system through the use of hardware based outside the system constitutes direct remote terminal access contrary to the provisions of § 23.20(i)(1), except as specifically approved by OJP. Thus, a hit/no hit response, if gleaned from an index, would bring a remote terminal within the scope of the requirement for OJP approval of direct remote terminal access.

Comment: One commentor pointed out that the requirement for prior OJP approval of "modifications to system design" was overly broad and could be read to require that even minor changes be submitted for approval. The commentor proposed a substitute which would limit the requirement to those modifications "that alter the system's identified goals in a way contrary to the requirements of (this regulation)."

Response: While it is agreed that the language is broad, the proposed limitation is too restrictive. The intent was that "modifications to system design" refer to "major" changes to the system, such as the nature of the information collected, the place or method of information storage, the authorized uses of information in the system, and provisions for access to system information by authorized participating agencies. This clarification has been incorporated in the regulation. In order to decentralize responsibility for approval of system design modifications, the proposed regulation has been revised to provide for approval of such modifications by the grantor agency rather than OJP. A similar change has been made to § 23.20(j).

Operating Principles—Section 23.20(n)

Comment: Several commentors expressed concern with the verification procedures set forth in § 23.20(n). One suggested that file information cannot "verify" the correctness of submissions but instead serves to "document" or "substantiate" its correctness. Another proposed deleting the requirements that (1) files maintained by participating agencies to support system submissions be subject to the operating principles, and (2) participating agencies are authorized to maintain such files separately from other agency files. The first requirement conflicts with the normal investigative procedures of a law enforcement agency in that all information in agency source files cannot meet the operating principles, particularly the reasonable suspicion and relevancy requirements. The important principle is that the information which is gleaned from an agency's source files and submitted to the system meet the operating principles. The second requirement has no practical value. At most, it results in the creation of duplicative files or in submission information being segregated from source files.

Response: OJP agrees with both comments. The word "documents" has been substituted for "verifies" and the provisions subjecting participating agency source files to the operating principles and authorizing maintenance of separate files have been deleted. Projects should use their audit and inspection access to agency source files to document the correctness of participating agency submissions on a sample basis.

Funding Guidelines—Section 23.30(b)

Comment: One commentor asked: Who defines the areas of criminal activity that "represent a significant and recognized threat to the population?"

Response: The determination of areas of criminal activity focus and priority are matters for projects, project policy boards and member agencies to determine, provided that the additional regulatory requirements set forth in § 23.30(b) are met.

Monitoring and Auditing of Grants—Section 23.40(a)

Comment: One commentor asked: "Who is responsible for developing the specialized monitoring and audit of awards for intelligence systems to insure compliance with the operating principles"?

Response: The grantor agency (the agency awarding a sub-grant to support an intelligence system) shall establish and approve a plan for specialized monitoring and audit of sub-awards prior to award. For the BJA Formula Grant Program, the State agency receiving the award from BJA is the grantor agency. Technical assistance and support in establishing a monitoring and audit plan is available through BJA.

Information on Juveniles

Comment: Can intelligence information pertaining to a juvenile who otherwise meets criminal intelligence system submission criteria be entered into an intelligence database?

Response: There is no limitation or restriction on entering intelligence information on juvenile subjects set forth in Federal law or regulation. However, State law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies. Therefore, State laws should be carefully reviewed to determine their impact on this practice and appropriate project policies adopted.

Executive Order 12291

These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act

These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601–612. These regulations, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act

There are no collection of information requirements contained in the regulation.

List of Subjects in 28 CFR Part 23

Administrative practice and procedure, Grant programs, Intelligence, Law enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23—CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

Sec.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub. L. 90–351, as amended by Pub. L. 91–644, Pub. L. 93–83, Pub. L. 93–415, Pub. L. 94–430, Pub. L. 94–503, Pub. L. 95–115, Pub. L. 96–157, Pub. L. 98–473, Pub. L. 99–570, Pub. L. 100–690, and Pub. L. 101–647), are utilized in conformance with the privacy and constitutional rights of individuals.

§23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq.*, as amended (Pub. L. 90–351, as amended by Pub. L. 91–644, Pub. L. 93–83, Pub. L. 93–415, Pub. L. 94–430, Pub. L. 94–503, Pub. L. 95–115, Pub. L. 96–157, Pub. L. 98–473, Pub. L. 99–570, Pub. L. 100–690, and Pub. L. 101–647).

(b) As used in these policies: (1) *Criminal Intelligence System* or *Intelligence System* means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) *Interjurisdictional Intelligence System* means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) *Criminal Intelligence Information* means data which has been evaluated to determine that it: (i) Is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) *Participating Agency* means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) *Intelligence Project* or *Project* means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) *Validation of Information* means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) *Reasonable Suspicion* or *Criminal Predicate* is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f)(1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99–508, 18 U.S.C. 2510–2520, 2701–2709 and 3121–3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d)(1) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(i) Assume official responsibility and accountability for actions taken in the name of the joint entity, and

(ii) Certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

(2) The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in

accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR part 23 Criminal Intelligence Systems Policies.

Laurie Robinson,

Acting Assistant Attorney General, Office of Justice Programs.

[FR Doc. 93–22614 Filed 9–15–93; 8:45 am]

BILLING CODE 4410–18–P

DEPARTMENT OF VETERANS AFFAIRS

38 CFR Part 47

RIN 2900–AE27

Reporting Health Care Practitioners to State Licensing Boards

AGENCY: Department of Veterans Affairs.

ACTION: Final rule.

SUMMARY: This document sets forth the policy of the Department of Veterans Affairs (VA) for reporting physicians, dentists, and other health care professionals to State licensing boards under authority of the act captioned "Veterans' Administration Health-Care Amendments of 1985" (the Act) and other authority. The intended effect of this policy is to cooperate with State licensing boards for the purpose of promoting better health care.

EFFECTIVE DATE: September 16, 1993.

FOR FURTHER INFORMATION CONTACT: Susan J. Brennan (10A2), Department of Veterans Affairs, 810 Vermont Ave. NW., Washington, DC 20420.

SUPPLEMENTARY INFORMATION: VA has had a longstanding practice of reporting to State licensing boards any separated licensed health care professional whose clinical practice so significantly failed to meet generally accepted standards of clinical practice as to raise reasonable concern for the safety of patients. More recently, the Act, among other things, established a mandate for VA to conduct a program to report to State licensing boards any separated licensed health-care professional (a) who was fired or who resigned following the completion of a disciplinary action relating to such individual's clinical competence, (b) who resigned after having had such individual's clinical privileges restricted or revoked, or (c) who resigned after serious concerns about such individual's clinical competence have been raised but not resolved. VA's longstanding practice and its Congressional mandate are compatible and the purpose of this part is to establish a final rule reflecting that it is the policy of the VA to report separated health care professionals to State licensing boards consistent with its longstanding practice and its Congressional mandate.

The following are examples of actions that meet the criteria for reporting: (a) Significant deficiencies in clinical practice such as lack of diagnostic or treatment capability, errors in transcribing, administering or documenting medications, inability to perform clinical procedures considered basic to the performance of one's occupation, performing procedures not included in one's clinical privileges in other than emergency situations; (b) patient neglect or abandonment; (c) mental health impairment sufficient to cause the individual to behave inappropriately in the patient care environment or to provide unsafe patient care; (d) physical health impairment sufficient to cause the individual to provide unsafe patient care; (e) substance abuse when it affects the individual's ability to perform appropriately as a health care provider or in the patient care environment; (f) falsification of credentials; (g) falsification of medical records or prescriptions; (h) theft of drugs; (i) inappropriate dispensing of drugs; (j) unethical behavior (such as sexual misconduct toward a patient); (k) mental, physical, sexual, or verbal abuse of a patient (examples of patient abuse include intentional omission of care, willful violation of a patient's privacy, willful physical injury, intimidation, harassment, or ridicule); and (l) violation of research ethics.

Executive Order 12291 and Regulatory Flexibility Act

Executive Order 12291 requires the Department to prepare and publish an initial regulatory impact analysis for any proposed major rule. A major rule is defined as any regulation that is likely to: (1) Have an annual effect on the economy of $100 million or more; (2) cause a major increase in costs or prices for consumers, individual industries, government agencies, or geographic regions; or (3) result in significant adverse effects on competition, employment, investment, productivity, innovation or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic or export markets.

The Department has determined that this final rule does not meet the criteria for a major rule as defined by section 1(b) of Executive Order 12291. Based on experience, for purposes of this Order, it is anticipated that a relatively insignificant number of health care professionals would be reported under this final rule (significantly less than one percent). Under these circumstances, the final rule would have little direct effect on the economy or on Federal or State expenditures. Consequently, the Department has concluded that a regulatory impact analysis is not required.

Also, the Secretary certifies that this final rule does not have a significant economic impact on a substantial number of small entities, and does not require a regulatory flexibility analysis under the Regulatory Flexibility Act of 1980. Under the circumstances explained above, the VA does not anticipate that a substantial number of small entities would be significantly affected by the final rule.

There are no applicable Catalog of Federal Domestic Assistance program numbers.

List of Subjects in 38 CFR Part 47

Health professions.

Approved: May 20, 1993.

Jesse Brown,

Secretary of Veterans Affairs.

For the reasons set forth in the preamble, 38 CFR is amended by adding a new part 47 to read as follows:

PART 47—POLICY REGARDING REPORTING HEALTH CARE PROFESSIONALS UNDER AUTHORITY OF PUBLIC LAW 99–166 AND 38 U.S.C. 501

Subpart A—General Provisions

Sec.

47.1 Definitions.

47.2 Purpose.

Subpart B—Reporting Under Authority of Pub. L. 99–166 and 38 U.S.C. 501.

47.3 Reporting to State licensing boards.

Authority: Pub. L. 99–166, 99 Stat. 941; 38 U.S.C. 501.

Subpart A—General Provisions

47.1 Definitions.

(a) *Act* means section 204 of the act captioned "Veterans Administration Health-Care Amendments of 1985" (Pub. L. 99–166, 99 Stat. 941).

(b) *Dentist* means a doctor of dental surgery or dental medicine legally authorized to practice dental surgery or medical dentistry by a State (or any individual who, without authority, holds himself or herself out to be so authorized).

(c) *Other health care professional* means an individual other than a physician or dentist who is licensed or otherwise authorized by a State to provide health care services (or any individual who, without authority, holds himself or herself out to be so licensed or authorized).

(d) *Physician* means a doctor of medicine or osteopathy legally authorized to practice medicine or surgery by a State (or any individual who, without authority, holds himself or herself out to be so authorized).

(e) *State* means the fifty States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands and any other territories or possessions of the United States.

(f) *State Licensing Board* means, with respect to a physician, dentist or other health care practitioner in a State, the agency of the State which is primarily responsible for the licensing of the physician, dentist or practitioner to provide health care services.

(g) *Generally accepted standards of clinical practice* means reasonable competence in the clinical aspects of one's responsibilities, as well as the moral and ethical behavior necessary to carry out those responsibilities.

(h) *Separated licensed health care professional* means a licensed health care professional who is no longer on VA rolls, regardless of whether the individual left voluntarily or involuntarily and regardless of the reason why the individual left.

(Authority: Pub. L. 99–166, 99 Stat. 941; 38 U.S.C. 501.)

§ 47.2 Purpose.

VA has had a longstanding practice of reporting to state licensing boards any separated licensed health care professional whose clinical practice so significantly failed to meet generally accepted standards of clinical practice as to raise reasonable concern for the safety of patients. More recently, the Act, among other things, established a mandate for VA to conduct a program to report to state licensing boards any separated licensed health-care professional who was fired or who resigned following the completion of a disciplinary action relating to such individual's clinical competence, who resigned after having had such individual's clinical privileges restricted or revoked, or who resigned after serious concerns about such individual's clinical competence have been raised but not resolved. VA's longstanding practice and its Congressional mandate are compatible and the purpose of this Part is to reflect that it is the policy of VA to report separated health care professionals to state licensing boards consistent with its longstanding practice and its Congressional mandate.

(Authority: Pub. L. 99–166, 99 Stat. 941; 38 U.S.C. 501.)

Subpart B—Reporting Under Authority of Public Law 99–166 and 38 U.S.C. 501

§ 47.3 Reporting to State licensing boards.

VA will report to state licensing boards any separated licensed health-care professional in accordance with its longstanding policy and its Congressional mandate which are both specified in § 47.2 of this Part. The following are examples of actions that meet the criteria for reporting:

(a) Significant deficiencies in clinical practice such as lack of diagnostic or treatment capability, errors in transcribing, administering or documenting medications, inability to perform clinical procedures considered basic to the performance of one's occupation, performing procedures not included in one's clinical privileges in other than emergency situations;

(b) Patient neglect or abandonment;

(c) Mental health impairment sufficient to cause the individual to behave inappropriately in the patient care environment or to provide unsafe patient care;

(d) Physical health impairment sufficient to cause the individual to provide unsafe patient care;

(e) Substance abuse when it affects the individual's ability to perform appropriately as a health care provider or in the patient care environment;

(f) Falsification of credentials;

(g) Falsification of medical records or prescriptions;

(h) Theft of drugs;

(i) Inappropriate dispensing of drugs;

(j) Unethical behavior (such as sexual misconduct toward a patient);

(k) Mental, physical, sexual, or verbal abuse of a patient (examples of patient abuse include intentional omission of care, willful violation of a patient's privacy, willful physical injury, intimidation, harassment, or ridicule); and

(l) Violation of research ethics.

(Authority: Pub. L. 99–166, 99 Stat. 941; 38 U.S.C. 501.)

[FR Doc. 93–22504 Filed 9–15–93; 8:45 am]
BILLING CODE 8320–01–M

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 185

[OPP–260053A; FRL–4645–4]

RIN No. 2070–AB78

Reinstatement of Food Additive Regulations for Benomyl, Mancozeb, Phosmet, and Trifluralin

AGENCY: Environmental Protection Agency (EPA).

ACTION: Reinstatement of Regulations.

SUMMARY: On July 14, 1993, EPA published in the **Federal Register** a final rule revoking certain food additive regulations (58 FR 37862). Consistent with its statement in the final rule, EPA decided to stay the revocations only for such time as would be necessary to rule on petitions requesting a further stay of the effectiveness of the final rule. EPA signed a stay document on August 27, 1993. However, due to an administrative error, the stay document was not published in the **Federal Register** as intended. By this document, EPA is implementing the August 27, 1993 stay action by reinstating the food additive regulations inadvertently removed from the Code of Federal Regulations. EPA is allowing 15 days for public comment on the petitions requesting a further stay of the final rule.

DATES: The effective date of this regulation is August 30, 1993. Any affected person may submit comments on the stay requests summarized in this document on or before October 1, 1993.

ADDRESSES: Comments, identified by the document control number, OPP-260053A, may be submitted to: the Public Response and Program Resources Branch, Field Operations Division (H7506C), Environmental Protection Agency, 401 M st., SW., Washington, DC 20460. In person, comments may be submitted to, and materials related to this document may be reviewed in, the Public Docket and Freedom of Information Section, Field Opeartions Division, Office of Pesticide Programs, Enviromental Protection Agency, Rm. 1132, CM #2, 1921 Jefferson Davis Hwy., Arlington, VA, Telephone: 703-305-5805. The docket is open from 8 a.m. to 4:30 p.m., Monday through Friday, except for legal holidays. Certain information may be subject to section 10 to the Federal Insecticide, Fungicide and Rodenticide Act (FIFRA). Inquiries regarding these materials may be directed to the docket staff at the telephone number given above.

FOR FURTHER INFORMATION CONTACT: Lisa Engstrom, Special Review Branch