

(1) Operated by or under the authority of any law of any State (or the District of Columbia, American Samoa, Guam, Puerto Rico, and the Virgin Islands).

(2) Operated through an insurance arrangement or on a self-insured basis by an employer.

(3) Operated under the authority of the Federal Employees Compensation Act or the Longshoremen's and Harbor Workers' Compensation Act.

Dated: February 8, 2000.

L.M. Bynum,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 00-3352 Filed 2-15-00; 8:45 am]

BILLING CODE 5001-01-P

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

Department of Defense Privacy Program

AGENCY: Department of Defense.

ACTION: Final rule.

SUMMARY: The Department of Defense is updating policies and responsibilities for the Defense Privacy Program which implements the Privacy Act of 1974, by adding rules of conduct and the composition and responsibilities of the Defense Privacy Board, the Defense Privacy Board Legal Committee, and the DoD Data Integrity Board to DoD Directive 5400.11, DoD Privacy Program for the effective administration of the program.

DATES: This regulation is effective December 13, 1999. Comments must be received by April 17, 2000.

ADDRESSES: Forward comments to the Director, Defense Privacy Office, 1941 Jefferson Davis Highway, Suite 920, Arlington, VA 22202-4502.

FOR FURTHER INFORMATION CONTACT: Mr. Vahan Moushegian, Jr., at (703) 607-2943 or DSN 327-2943.

SUPPLEMENTARY INFORMATION:

Executive Order 12866

It has been determined that this Privacy Act rule for the Department of Defense does not constitute 'significant regulatory action'. Analysis of the rule indicates that it does not have an annual effect on the economy of \$100 million or more; does not create a serious inconsistency or otherwise interfere with an action taken or planned by another agency; does not materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the

rights and obligations of recipients thereof; does not raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in Executive Order 12866 (1993).

Regulatory Flexibility Act

It has been determined that this Privacy Act rule for the Department of Defense does not have significant economic impact on a substantial number of small entities because it is concerned only with the administration of Privacy Act systems of records within the Department of Defense.

Paperwork Reduction Act

It has been determined that this Privacy Act rule for the Department of Defense imposes no information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1974.

List of Subjects in 32 CFR Part 310

Privacy.

Accordingly, 32 CFR part 310, is amended as follows:

1. The authority citation for 32 CFR part 310 continues to read as follows:

Authority: Pub. L. 93-579, 88 Stat 1896 (5 U.S.C. 552a)

2. 32 CFR part 310, subpart A, is revised to read as follows:

Subpart A—DoD Policy

Sec.

- 310.1 Reissuance
- 310.2 Purpose.
- 310.3 Applicability and scope.
- 310.4 Definitions.
- 310.5 Policy.
- 310.6 Responsibilities.
- 310.7 Information requirements.
- 310.8 Rules of conduct.
- 310.9 Privacy boards and office composition and responsibilities.

Authority: Pub. L. 93-579, 88 Stat 1896 (5 U.S.C. 552a)

Subpart A—DoD Policy

§ 310.1 Reissuance.

This part is reissued to consolidate into a single document (32 CFR part 310) Department of Defense (DoD) policies and procedures for implementing the Privacy Act of 1974, as amended (5 U.S.C. 522a) by authorizing the development, publication and maintenance of the DoD Privacy Program set forth by DoD Directive 5400.11¹, December 13, 1999,

¹Copies may be obtained: <http://web7.whs.osd.mil/corres.htm>.

and 5400.11-R², August 31, 1983, both entitled: "DoD Privacy Program."

§ 310.2 Purpose.

This part:

(a) Updates policies and responsibilities of the DoD Privacy Program under 5 U.S.C. 552a, and under OMB Circular A-130.³

(b) Authorizes the Defense Privacy Board, the Defense Privacy Board Legal Committee and the Defense Data Integrity Board.

(c) Continues to authorize the publication of DoD 5400.11-R.

(d) Continues to delegate authorities and responsibilities for the effective administration of the DoD Privacy Program.

§ 310.3 Applicability and scope.

This part:

(a) Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Uniformed Services University of the Health Sciences, the Defense agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). This part is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their Components. Such instructions will not conflict with the provisions of this part.

(b) Shall be made applicable to DoD contractors who are operating a system of records on behalf of a DoD Component, to include any of the activities, such as collecting and disseminating records, associated with maintaining a system of records.

(c) This part does not apply to:

(1) Requests for information from systems of records controlled by the Office of Personnel Management (OPM), although maintained by a DoD Component. These are processed in accordance with OPM's 'Privacy Procedures for Personnel Records' (5 CFR part 297).

(2) Requests for personal information from the General Accounting Office (GAO). These are processed in accordance with DoD Directive 7650.1,⁴ "General Accounting Office Access to Records," September 11, 1997.

(3) Requests for personal information from Congress. These are processed in

²See footnote 1 to § 310.1.

³Copies may be obtained: EOP Publications, NEOB, 725 17th Street, NW Washington, DC 20503.

⁴See footnote 1 to § 310.1.

accordance with DoD Directive 5400.4,⁵ "Provisions of Information to Congress," January 30, 1978, except for those specific provisions in Subpart E— Disclosure of Personal Information to Other Agencies and Third Parties.

(4) Requests for information made under the Freedom of Information Act (5 U.S.C. 552). These are processed in accordance with "DoD Freedom of Information Act Program Regulation" (32 CFR part 286).

§ 310.4 Definitions.

Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

Agency. For the purposes of disclosing records subject to the Privacy Act among DoD Components, the Department of Defense is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and record keeping as regards release to non-DoD agencies; each DoD Component is considered an agency within the meaning of the Privacy Act.

Confidential source. A person or organization who has furnished information to the federal government under an express promise that the person's or the organization's identity will be held in confidence or under an implied promise of such confidentiality if this implied promise was made before September 27, 1975.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or government agency, other than the subject of the record, the subject's designated agent or the subject's legal guardian.

Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

Law enforcement activity. Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

Maintain. Includes maintain, collect, use or disseminate.

Official use. Within the context of this part, this term is used when officials and employees of a DoD Component have a demonstrated need for the use of any record or the information contained therein in the performance of their official duties, subject to DoD 5200.1-R.⁶ "DoD Information Security Program Regulation."

Personal information. Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

Privacy Act request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Member of the public. Any individual or party acting in a private capacity to include federal employees or military personnel.

Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Risk assessment. An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

Routine use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

Statistical record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

System manager. The DoD Component official who is responsible for the operation and management of a system of records.

System of records. A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

Word processing system. A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written or graphic presentations intended to communicate verbally or visually with another individual.

Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, handwiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device.

§ 310.5 Policy.

It is DoD policy that:

(a) The personal privacy of an individual shall be respected and protected.

(b) Personal information shall be collected, maintained, used or disclosed to ensure that:

(1) It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statute or Executive Order.

(2) It shall be collected to the greatest extent practicable directly from the individual.

(3) The individual shall be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing that information.

(4) It shall be relevant, timely, complete and accurate for its intended use; and

(5) Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage or transfer.

(c) No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

(1) Specifically authorized by statute.

(2) Expressly authorized by the individual on whom the record is maintained; or

⁵ See footnote 1 to § 310.1.

⁶ See footnote 1 to § 310.1.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity.

(d) Notices shall be published in the **Federal Register** and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by, 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, used, or disseminated until the required publication/review requirements, as set forth in 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, are satisfied.

(e) Individuals shall be permitted, to the extent authorized by 5 U.S.C. 552a and DoD 5400.11-R, to:

(1) Determine what records pertaining to them are contained in a system of records.

(2) Gain access to such records and to obtain a copy of those records or a part thereof.

(3) Correct or amend such records on a showing that the records are not accurate, relevant, timely or complete.

(4) Appeal a denial of access or a request for amendment.

(f) Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by 5 U.S.C. 552a, DoD 5400.11-R, and DoD 5400.7-R.⁷ When disclosures are made, the individual shall be permitted, to the extent authorized by 5 U.S.C. and DoD 5400.11-R, to seek an accounting of such disclosures from the DoD Component making the release.

(g) Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Imagery and Mapping Agency shall be prohibited to the extent authorized by Pub. L. 86-36 (1959) and 10 U.S.C. 424.

(h) Computer matching programs between the DoD Components and the Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(i) DoD personnel and system managers shall conduct themselves, consistent with § 310.8 so that personal information to be stored in a system of records only shall be collected, maintained, used, and disseminated as is authorized by this part, 5 U.S.C. 552a, and DoD 5400.11-R.

⁷ See footnote 1 to § 310.1.

§ 310.6 Responsibilities.

(a) The Director of Administration and Management, Office of the Secretary of Defense, shall:

(1) Serve as the Senior Privacy Official for the Department of Defense.

(2) Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in 5 U.S.C. 552a and OMB A-130.

(3) Publish DoD 5400.11-R and other guidance, to include Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

(4) Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (§ 310.7).

(b) The Director of Washington Headquarters Services shall supervise and oversee the activities of the Defense Privacy Office (§ 310.7).

(c) The General Counsel of the Department of Defense shall:

(1) Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the DoD Privacy Program.

(2) Review and be the final approval authority on all advisory opinions issued by the Defense Privacy Board or the Defense Privacy Board Legal Committee.

(3) Serve as a member of the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee (§ 310.7).

(d) The Secretaries of the Military Departments and the Heads of the Other DoD Components shall:

(1) Provide adequate funding and personnel to establish and support an effective DoD Privacy Program, to include the appointment of a senior official to serve as the principal point of contact (POC) for DoD Privacy Program matters.

(2) Establish procedures, as well as rules of conduct, necessary to implement this part and DoD 5400.11-R so as to ensure compliance with the requirements of 5 U.S.C. 552a and OMB Circular A-130.

(3) Conduct training, consistent with the requirements of DoD 5400.11-R, on the provisions of this part, 5 U.S.C. 552a, and OMB Circular A-130, and DoD 5400.11-R, for assigned and employed personnel and for those individuals having primary responsibility for implementing the DoD Privacy Program.

(4) Ensure that the DoD Privacy Program periodically shall be reviewed by the Inspectors General or other officials, who shall have specialized knowledge of the DoD Privacy Program.

(5) Submit reports, consistent with the requirements of DoD 5400.11-R, as mandated by 5 U.S.C. 552a and Chapter 8, OMB Circular A-130, and 32 CFR part 275, and as otherwise directed by the Defense Privacy Office.

(e) The Secretaries of the Military Departments shall provide support to the Combatant Commands, as identified in DoD Directive 5100.3,⁸ in the administration of the DoD Privacy Program.

§ 310.7 Information requirements.

The reporting requirements in § 310.6(d)(5) are assigned Report Control Symbol DD-DA&M(A)1379.

§ 310.8 Rules of conduct.

(a) DoD personnel shall:

(1) Take such actions, as considered appropriate, to ensure that personal information contained in a system of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information shall be preserved.

(2) Not disclose any personal information contained in any system of records except as authorized by DoD 5400.11-R or other applicable law or regulation. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

(3) Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this part to the applicable Privacy POC for his or her DoD Component.

(b) DoD system managers for each system of records shall:

(1) Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities for protecting personal information being collected and maintained under the DoD Privacy Program.

(2) Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through their DoD Component Privacy POC to the Defense Privacy Office for publication in the **Federal Register**.

(3) Not maintain any official files on individuals that are retrieved by name or other personal identifier without first ensuring that a notice for the system of records shall have been published in the

⁸ See footnote 1 to § 310.1.

Federal Register. Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, is subject to possible criminal penalties and/or administrative sanctions.

§ 310.9 Privacy boards and office composition and responsibilities.

(a) *The Defense Privacy Board.*—(1) *Membership.* The Board shall consist of the Director of Administration and Management, OSD (DA&M), who shall serve as the Chair; the Director of the Defense Privacy Office, Washington Headquarters Services (WHS), who shall serve as the Executive Secretary and as a member; the representatives designated by the Secretaries of the Military Departments; and the following officials or their designees: the Deputy Under Secretary of Defense for Program Integration (DUSD(PI)); the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)); the Director, Freedom of Information and Security Review, WHS; the General Counsel of the Department of Defense (GC, DoD); and the Director for Information Operations and Reports, WHS (DIO&R). The designees also may be the principal POC for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure that the policies, practices, and procedures of that Program are premised on the requirements of 5 U.S.C. 552a and OMB Circular A-130, as well as other pertinent authority, and that the Privacy Programs of the DoD Component are consistent with, and in furtherance of, the DoD Privacy Program.

(ii) The Board shall serve as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary, to address issues of common concern so as to ensure that uniform and consistent policy shall be adopted and followed by the DoD Components. The Board shall issue advisory opinions as necessary on the DoD Privacy Program so as to promote uniform and consistent application of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(iii) Perform such other duties as determined by the Chair or the Board.

(b) *The Defense Data Integrity Board.*—(1) *Membership.* The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the Defense Privacy Office, WHS, who shall serve as the Executive Secretary;

and the following officials or their designees: the representatives designated by the Secretaries of the Military Departments; the DUSD (PI); the ASD(C3I); the GC, DoD; the DIOR (WHS); and the Director, Defense Manpower Data Center. The designees also may be the principal POC for the DoD Component for privacy matters.

(2) *Responsibilities.* (i) The Board shall oversee and coordinate, consistent with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, all computer matching programs involving personal records contained in system of records maintained by the DoD Components.

(ii) The Board shall review and approve all computer matching agreements between the Department of Defense and the other Federal, State or local governmental agencies, as well as memoranda of understanding when the match is internal to the Department of Defense, to ensure that, under 5 U.S.C. 552a, and OMB Circular A-130 and DoD 5400.11-R, appropriate procedural and due process requirements shall have been established before engaging in computer matching activities.

(c) *The Defense Privacy Board Legal Committee.*—(1) *Membership.* The Committee shall consist of the Director, Defense Privacy Office, WHS, who shall serve as the Chair and the Executive Secretary; the GC, DoD, or designee; and civilian and/or military counsel from each of the DoD Components. The General Counsels (GCs) and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. That does not preclude representation from each office. The GCs of the other DoD Components shall provide legal representation to the Committee. Other DoD civilian or military counsel may be appointed by the Executive Secretary, after coordination with the DoD Component concerned, to serve on the Committee on those occasions when specialized knowledge or expertise shall be required.

(2) *Responsibilities.* (i) The Committee shall serve as the primary legal forum for addressing and resolving all legal issues arising out of or incident to the operation of the DoD Privacy Program.

(ii) The Committee shall consider legal questions regarding the applicability of 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R and questions arising out of or as a result of other statutory and regulatory authority, to include the impact of judicial decisions, on the DoD Privacy Program.

The Committee shall provide advisory opinions to the Defense Privacy Board and, on request, to the DoD Components.

(c) *The Defense Privacy Office.*—(1) *Membership.* It shall consist of a Director and a staff. The Director also shall serve as the Executive Secretary and a member of the Defense Privacy Board; as the Executive Secretary to the Defense Data Integrity Board; and as the Chair and the Executive Secretary to the Defense Privacy Board Legal Committee.

(2) *Responsibilities.* (i) Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

(ii) Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

(iii) Direct the day-to-day activities of the DoD Privacy Program.

(iv) Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

(v) Review proposed new, altered, and amended systems of records, to include submission of required notices for publication in the **Federal Register** and, when required, providing advance notification to the Office of Management and Budget (OMB) and the Congress, consistent with 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(vi) Review proposed DoD Component privacy rulemaking, to include submission of the rule to the Office of the Federal Register for publication and providing to the OMB and the Congress reports, consistent with 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R, and to the Office of the Comptroller General of the United States, consistent with 5 U.S.C. Chapter 8.

(vii) Develop, coordinate, and maintain all DoD computer matching agreements, to include submission of required match notices for publication in the **Federal Register** and advance notification to the OMB and the Congress of the proposed matches, consistent with 5 U.S.C. 552a, OMB Circular A-130, and DoD 5400.11-R.

(viii) Provide advice and support to the DoD Components to ensure that:

(A) All information requirements developed to collect or maintain personal data conform to DoD Privacy Program standards.

(B) Appropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic on non-electronic means; and

(C) Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

(ix) Serve as the principal POC for coordination of privacy and related matters with the OMB and other Federal, State, and local governmental agencies.

(x) Compile and submit the "Biennial 'Privacy Act' Report" and the "Biennial Matching Activity Report" to the OMB as required by OMB Circular A-130 and DoD 5400.11-R

(xi) Update and maintain this part and DoD 5400.11-R.

Dated: February 8, 2000.

L.M. Bynum,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 00-3353 Filed 2-15-00; 8:45 am]

BILLING CODE 5001-10-U

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 59

[AD-FRL-6539-2]

RIN 2060-AE55

National Volatile Organic Compound Emission Standards for Architectural Coatings

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule; amendments.

SUMMARY: On September 11, 1998, EPA published the "National Volatile Organic Compound Emission Standards for Architectural Coatings" under the authority of section 183(e) of the Clean Air Act. In this action, we're changing the address to which exceedance fee payments must be mailed and clarifying the entity to whom payments should be made payable. This action won't change the volatile organic compound (VOC) content limits for architectural coatings or the level of emission reduction that the rule requires.

EFFECTIVE DATE: February 16, 2000.

ADDRESSES: Docket No. A-92-18 contains information considered by EPA in developing the promulgated standards and this action. You can inspect the docket and copy materials from 8 a.m. to 5:30 p.m., Monday through Friday, excluding legal holidays. The docket is located at the EPA's Air and Radiation Docket and Information Center, Waterside Mall, Room M1500, 1st Floor, 401 M Street, SW, Washington, DC 20460; telephone (202) 260-7548 or fax (202) 260-4400. A reasonable fee may be charged for copying.

FOR FURTHER INFORMATION CONTACT: Ms. Linda Herring at (919) 541-5358, Coatings and Consumer Products Group, Emission Standards Division (MD-13), U.S. Environmental Protection Agency, Research Triangle Park, North Carolina

27711 (herring.linda@epa.gov). Any correspondence related to compliance with this rule must be submitted to the appropriate EPA Regional Office listed in § 59.409(a) of 40 CFR part 59.

SUPPLEMENTARY INFORMATION: Section 553 of the Administrative Procedure Act, 5 U.S.C. 553(b)(3)(B), provides that, when an agency for good cause finds that notice and public procedure are impracticable, unnecessary, or contrary to the public interest, the agency may issue a rule without providing notice and an opportunity for public comment. The EPA has determined that there is good cause for making today's rule final without prior proposal and opportunity for comment because these corrections and clarifications are not controversial and do not substantively change the requirements of the architectural coatings rule. Thus, notice and public procedure are unnecessary. The EPA finds that this constitutes good cause under 5 U.S.C. 553(b)(3)(B).

Regulated Entities. You may be affected by these rule amendments if you fall into one of the categories in the following table.

Category	NAICS code	SIC code	Examples of regulated entities
Industry	32551 325510	2851	Manufacturers (which includes packagers and repackagers) and importers of architectural coatings that are manufactured for sale or distribution in the U.S., including all U.S. territories.
State/local/tribal governments			State Departments of Transportation that manufacture their own coatings.

Architectural coatings are coatings that are recommended for field application to stationary structures and their appurtenances, to portable buildings, to pavements, or to curbs.

Use this table only as a guide because this action may also regulate other entities. To determine if it regulates your facility, business, or organization, carefully examine the applicability criteria in § 59.400 of 40 CFR part 59. If you have questions about how it applies, contact Linda Herring (see **FOR FURTHER INFORMATION CONTACT** section of this preamble).

I. Technical Corrections

The EPA published in the **Federal Register** of September 11, 1998 (63 FR 48848), the final rule regulating VOC

emissions from architectural coatings. The address in the rule to which exceedance fee payments must be submitted has changed and, therefore, needs to be updated. In addition, the rule did not specify the entity to whom exceedance fee payments should be made payable. Thus, we're correcting and clarifying the rule as follows:

1. We are changing § 59.403(d) to indicate that the address to which exceedance fee payments must be mailed is located in § 59.409(b) of the rule. This change is necessary to implement the exceedance fee receipt and processing procedures that EPA recently established for this rule.

2. We are removing the word "Regional" from the title of § 59.409 to

reflect that the section includes more than just the addresses of the EPA Regional Offices.

3. We are amending § 59.409 by designating the existing text as paragraph (a) and modifying it so that exceedance fee payments are deleted from the list of items that are sent to the EPA Regional Offices. This change is necessary due to the change in the address for exceedance fee payments.

4. We are amending § 59.409 by adding paragraph (b) that provides the correct address to which exceedance fee payments must be submitted. This change is necessary to specify that exceedance fees should be mailed to: U.S. Environmental Protection Agency, AIM Exceedance Fees, Post Office Box