U. S. DEPARTMENT OF THE INTERIOR
OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT
DIRECTIVES SYSTEM

Subject Number: ADS - 1
Transmittal Number: 355
Date: 07/09/87

Subject: Policies and Procedures for Implementing the Privacy Act of 1974.

Approval: J. D. Christensen Title: Director

1. Purpose. The purpose of this document is to implement the Privacy Act of 1974, (P.L. 93-579) in accordance with the procedures established in the Department of the Interior regulations contained in 43 CFR 2.46 through 2.79, and in the Departmental Manual Part 383, Policies and Procedures for Implementing the Privacy Act of 1974. It also provides guidelines for routing, recording, processing and reporting requests for access to and amendment of records.

2. Definitions.

a. Act. Section 3 of the Privacy Act, 5 U.S.C. 552a (P.L. 93-579).

b. Bureau. Office of Surface Mining Reclamation and Enforcement (OSMRE).

c. Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

d. Maintain. Pertains to records including their collection, retention, use or dissemination.

e. Record. "Record" means any item, collection, or grouping of information about an individual that is maintained by the Department or Bureau, including but not limited to, education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or other particular means of identifying the individual, such as a finger or voice print, photograph, or social security number.

f. System of Records. A group of any records under the control of the Department or Bureau from which information is retrieved by the name of the individual or some identifying number or symbol assigned to the individual.

g. System Notice. The notice describing a system of records required by 5 U.S.C. 552a(e)(4) to be published in the Federal Register when a new system is established or an existing system is revised.

h. System Manager. The official designated in a system notice as having administrative responsibility for a system of records (also see 3.b.(10)(a)).

i. Medical Records. Records which relate to the identification, prevention, cure or alleviation of any disease, illness or injury including psychological disorders, alcoholism and drug addiction.

j. Personnel Management Records. Records maintained by OSMRE and used for personnel management programs or processes such as staffing, employee development, retirement, and grievances and appeals.

k. Statistical Records. Records in a system of records maintained for statistical research or reporting purposes only and not used in making any determination about an identifiable individual.

l. Routine Use. Use of a record for a purpose which is compatible with the purpose for which it was collected.

m. Computer Matching. A procedure in which a computer is used to compare two or more automated systems of records or a single system with a set of non-Federal records to find data which are common to more than one system or set, conducted for the purpose of improving Government operations, reducing losses from fraud, abuse, error, or loan defaults, and assuring the proper use of Government funds and property.

3. Policy/Procedures.

a. Responsibility.

(1) Privacy Act Officer. The Assistant Director, Budget and Administration, is designated as the OSMRE Privacy Act Officer responsible for administering the Act.

(2) Assistant Privacy Act Officer. The Chief, Division of Personnel, is designated as the Assistant Privacy Act Officer.

(3) Privacy Act Liaison Officers. The Chiefs of the Administrative Service Center, Eastern Field Operations and Western Field Operations are designated as Privacy Act Liaison Officers and should coordinate Privacy Act requests involving their respective areas of responsibility with the Assistant Privacy Act Officer.

Privacy Act Liaison Officers and Field Office Directors shall develop guidelines and operating procedures consistent with this directive. Field Office Directors shall coordinate the Privacy Act activities for requests made to Area Offices.

(4) Supervisors and Managers - are responsible for identifying Privacy Act systems of records under their control.

(5) System Managers. System managers are OSMRE officials designated to administer systems of records under the Privacy Act. As applicable, each Headquarters Assistant Director, Assistant Directors, Eastern and Western Field Operations, Field Office Directors, and Chiefs of the Headquarters staff offices will select employees to serve as system managers. This includes a systems manager for each system of records developed or maintained by a contractor. See the Departmental regulations in 43 CFR 2.53.

b. Procedures.

(1) Establishment of System of Records. OSMRE must submit to the Departmental Privacy Act Officer, no fewer than ninety calendar days in advance, any proposal to establish a new system of records or significantly revise an existing system of records. The ninety calendar days minimum advance notice is required for any proposal identifying a new routine use for an existing system of records. A system may not be created or significantly revised or a new routine use established without the publication of a system notice in the Federal Register and reporting the new or significantly revised system of records to the Office of Management and Budget. See Departmental Manual 383 DM 5, Appendix 3, for details.

(2) System Notice. The Privacy Act requires that a notice be published in the Federal Register describing any system of records that contains personal information accessible by the name of an individual or by codes or symbols identifying individuals. The notice describes the system and tells how an individual can inquire to determine if the system contains personal information on that individual. See 383 DM 5 for more details.

(3) Records Subject to the Privacy Act. The Privacy Act places restrictions on the collection, use and dissemination of records relating to individual persons. Records are subject to the Privacy Act if they contain information about an individual and are retrievable by the subject individual's name, code, symbol, voice print, fingerprints or other identifier. Individuals are permitted to obtain access to records relating to them and seek revisions of these records if they believe them to be incorrect.

(4) Restriction on Dissemination of Records. The Privacy Act prohibits the disclosure of records contained in a system of records to anyone (including other Federal agencies) without the written permission of the person to whom the records relate except as provided in 383 DM 7.2 as supported by 5 U.S.C. 552a(b), which lists twelve exceptions which permit disclosures without the consent of the individual of record. Requests for disclosures for computer matching programs should be carefully reviewed to determine if consent is required or if disclosure would be compatible with the purpose for which the records were originally collected.

(5) Safeguarding Records. Protection of personal information, in systems of records subject to the Privacy Act, may vary between systems. Each system manager shall:

(a) Develop guidelines for protecting personal information in systems of records he or she is responsible for administering, and submit them to the OSMRE Privacy Act Officer.

(b) Post warnings in records system areas to include access limitations, standards of conduct for employees handling Privacy Act records, and possible criminal penalties for violations. See Departmental Manual 383 DM 8.3A, Illustration 1 to the chapter.

(c) Store manual records in locked metal file cabinets or in a locked room, except when the room is occupied by authorized personnel.

(d) Store computerized records subject to safeguards based on recommendations of the National Bureau of Standards contained in "Computer Security Guideline for Implementing the Privacy Act of 1974" (FIPS Pub. 41, May 30, 1975).

(e) Maintain Office of Personnel Management personnel records for administering personnel management programs according to the security requirements prescribed in OPM's regulations (5 CFR 293.106 and 107).

(f) Refuse to disclose a record to a third party or to anyone without clear instructions. See 383 DM 8 for more details for the maintenance of appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and protect against hazards to their integrity.

(6) Conduct of Employee. All OSMRE employees with access to a system of records shall be aware of the requirements of the Act (5 U.S.C. 522a(e)), Departmental regulations 43 CFR 2.52 and 383 DM 9 concerning the handling, disclosure, and alteration of such records and the possibility of criminal penalties for improper disclosures.

(7) Responsiveness to Privacy Act Requests. The Privacy Act guarantees individuals the right of access to their records or to obtain any information pertaining to them which is contained in a system of records, and to review the records and have copies made of all or any part thereof.

(a) Requests shall be in writing. However, an oral request may be honored by the system manager as a matter of administrative discretion.

(b) Notification and Access Requests. Systems managers should promptly advise inquirers as to their requests for notification of the existence of records pertaining to them, and requests to inspect records, if any exist.

(c) Exemption Criteria for Denying Notification of Access. System managers responsible for an exempted system shall document the criteria used in denying requests for notification of access and report their actions to the Privacy Act Officer.

(d) Amendment of Records. An initial decision on a petition for amendment shall be made by the system manager responsible for the system of records containing the challenged record and must, if he or she declines to amend the record as requested, be concurred with by the OSMRE Privacy Act Officer and the Director of OSMRE or his designee. The petition must be acknowledged in writing within ten working days of receipt, if processing is not completed. The decision to accept or reject the petition must be made within no more than 30 working days.

(e) Notification, Access, Petition Denials. A request regarding a record may be denied if the record was compiled in reasonable anticipation of a civil action or proceeding, or if the record is contained in a system of records which has been excepted from the access provisions of the Privacy Act by rulemaking. Denials recommended by a system manager must receive the concurrence of the Privacy Act Officer and the Director of OSMRE or his designee. See 43 CFR 2.60-2.77 and 383 DM 6 for more detail concerning notification access and amendment procedures.

(8) Fees. Unless waived, uniform fees shall be charged for document duplication costs, incurred in responding to Privacy Act requests for access to records. No fee may be charged for searching for or reviewing a record in response to a Privacy Act request. See 43 CFR 2.64(d), Appendix A, for specific charges and criteria for waiving or reducing fees.

(9) Accounting for Disclosure. System managers shall maintain records of disclosures made from Privacy Act systems outside of the Department of the Interior. The record should be maintained for five years or the life of the records, whichever is longer, after the disclosure for which the accounting is made. Record the date, nature and purpose of each disclosure of a record to any person or to another agency and the name and address of the person or agency to whom the disclosure was made. See 43 CFR 2.57 for more details.

(10) Annual Report. OSMRE is required to report to the Department on its calendar year activities relating to the Privacy Act in order to provide data required by OMB, Circular No. 2-108 revised. See 383 DM 6.10 for specific details.

(a) System Managers. Each system manager will maintain a record of the activities of his or her system and send it to the OSMRE Privacy Act Officer along with the narrative statement discussed below. The system managers will also prepare statements justifying the circumstances for invoking exemptions for requests for notification and access. Also to be reported are statements on actions taken to comply with the Act and experience with the Act.

(b) Narrative Format.

1 System managers shall send their reports to the Privacy Act Officer in accordance with OMB requirements as they are published.

2 The Privacy Act Officer, after reviewing and consolidating, will submit the report to the Departmental Privacy Act Officer, Office of the Assistant Secretary for Policy, Budget and Administration, for consolidation into the Department's report to OMB.

c. Routing, Controlling and Disclosing Requested Documents.

(1) Headquarters OSMRE Mail Room.

(a) Envelopes received and marked "Privacy Act Inquiry." Date stamps envelope and delivers unopened to Privacy Act Officer.

(b) Other mail received and not marked "Privacy Act Inquiry."

1 Addressee opens envelopes, scans contents, and determines application to Privacy Act.

2 Stamps date and "Privacy Act Inquiry" on envelope and contents, and delivers to the Privacy Act Officer.

(2) Assistant Privacy Act Officer.

(a) Receives inquiry from Privacy Act Officer.

1 Reviews contents, determines appropriate systems manager.

2 Prepares and attaches form containing routing, due date and other appropriate instructions.

3 Posts in control log and forwards to system managers.

(b) Receives telephone advice on receipt of an uncontrolled "Privacy Act Inquiry" from a system manager.

1 Determines that appropriate system manager has inquiry, or requests that inquiry be delivered to Privacy Act Officer.

2 Prepares instruction form and sends to appropriate system manager for attachment to inquiry.

3 Posts in control log.

(3) System Manager.

(a) Receives inquiry via Privacy Act Officer. Posts in log and acts on inquiry.

(b) Receives inquiry not cleared through Privacy Act Officer.

1 Informs Privacy Act Officer.

2 If Privacy Act Officer advises system manager that he or she is the action office:

a Stamps date and "Privacy Act Inquiry" on document.

b Posts in log.

c Attaches instruction form to inquiry upon receipt from the Privacy Act Officer.

d Acts on inquiry.

3 If advised that he or she is not the action officer, delivers the inquiry to the Privacy Act Officer.

4 If document is to be provided with no fee required, prepares and signs letter addressed to the requester, within 10 days, advising that the document is enclosed or advises that the document will be forwarded within 30 days.

5 If document is to be provided with fee required, he or she may decide to send document and note amount of fee due or may advise that the document is available at a fee covering the cost of reproduction.

6 If access to system of records is to be permitted, advises requester.

d. Denial recommendation process.

(1) System manager recommends denial. A memorandum is prepared which documents the denial criteria and the system manager confers with the Privacy Act Officer. The Privacy Act Officer should seek the advice of the Solicitor's Office with regard to recommendations for denial.

(2) Privacy Act Officer concurs in the denial recommendation. If the Privacy Act Officer concurs in the system manager's recommendation for denial, the requested document will not be made available to the requester.

(3) Privacy Act Officer does not concur in the denial recommendation. If the Privacy Act Officer does not concur in the system manager's recommendation for denial, the requested document will be made available to the requester.

(4) Director or his designee concurs in denial. If the Director or his designee concurs in denying the request, he or she signs a letter to the requester. The official file is sent to the Privacy Act Officer for control and custody with a copy of the letter to the system manager.

(5) Director or his designee does not concur in the denial. If the Director or his designee negates the denial recommendation, he or she so indicates on the letter. The file is returned to the system manager via the Privacy Act Officer, and a letter is prepared releasing the document or advising that it will be available when reproduced.

(6) System manager takes action to release document. Upon release of document, the official record is sent to the Privacy Act Officer.

(7) Privacy Act Officer. The case status is logged and filed in a closed or suspense file, as appropriate.

(8) System manager. Upon receipt of the authorization, files request and sends official file to the Privacy Act Officer.

e. Privacy Act Officer files official case in a closed file.

4. Reporting Requirements. Annual Report. As necessary, Privacy Act Liaison Officers and the Headquarters, Divisions of Personnel will conduct reviews to ensure compliance unit the provisions of this directive.

5. References. Privacy Act of 1974 (P.L. 93-579), Departmental Regulations, Part 2, 43 CFR 2.46-2.79, 5 CFR 294 and 297, Departmental Manual part 383, Policy and Procedures for Implementing the Privacy Act of 1974.

6. Effect on Other Documents. Supersedes ADS-1 dated March 22, 1984. Should be used in conjunction with OSMRE Directive INF-3, Freedom of Information Act.

7. Effective Date. Date of Issuance.

8. Contact. Division of Personnel, Branch of Personnel Policy and Evaluation, (FTS/202) 343-1010.