Privacy Act Manual

EPA 2190, December 2005

Privacy Act Manual

Abstract

U.S. EPA Directive 2190 - Privacy Act Manual (Revised December 2005) establishes policy and procedures for protecting the privacy of individuals who are identified in the Environmental Protection Agency's information systems and informs Agency employees and officials of their rights and responsibilities under the Privacy Act (5 U.S.C. 552a).

Quick Table of Contents

Full Table of Contents

Chapter 1. Policy and Responsibilities

1. **PURPOSE.** This Manual establishes policy and procedures for protecting the privacy of individuals who are identified in the Environmental Protection Agency's information systems and informs Agency employees and officials of their rights and responsibilities under the Privacy Act (5 U.S.C. 552a). It supplements the EPA regulations in Part 16, Title 40, Code of Federal Regulations (CFR).
2. **POLICY.** The Agency will safeguard personal privacy in its collection, maintenance, use, and dissemination of information about individuals and make such information available to the individual in accordance with the requirements of the Privacy Act.
3. **SCOPE.** This Manual applies to any records under the control of the Agency from which information on a subject individual is retrieved by a personal identifier assigned to the individual. The identifier may be the name of the individual, a number, a symbol, or any other specific retriever assigned to such individual. This Manual applies to such records maintained by the Agency in-house or maintained by a contractor or grantee on behalf of the Agency to accomplish an Agency function.
4. **DEFINITIONS.** Definitions applicable to this Manual are located at Figure 1-1, Definitions Applicable to the Privacy Act.
5. **LEGAL AUTHORITY AND ADMINISTRATIVE GUIDELINES.** The provisions of this Manual are based on these authorities:
    a. The Privacy Act of 1974, 5 U.S.C. 552a, as amended.
    b. OMB Circular No. A-108 (as amended), Responsibilities for the Maintenance of Records About Individuals by Federal Agencies.
    c. OMB's Privacy Act Implementing Guidelines published at 40 Federal Register 28948 and at 49 Federal Register 12338.
    d. EPA's Privacy Act Regulations published at 40 CFR Part 16.
6. **BASIC REQUIREMENTS OF THE PRIVACY ACT.** The basic requirements of the Privacy Act are summarized below:

a. At least sixty days prior to creation of a new System of Records or significant alteration to an existing System, the Agency must submit documentation to OMB and the Congress, and publish a notice of the System in the Federal Register. (See Chapter 2 for details.)

b. Each time the Agency creates a new System of Records or requests that an individual provide his/her social security number, the System Manager must provide the individual with a written "privacy act statement." The statement will inform the individual of the legal authority for collecting the information; whether disclosure of such information by the individual is mandatory or voluntary; the purpose for which the information is being collected and the routine uses which may be made of the information; and the effect on the individual if the individual does not provide the information.

c. To the greatest extent practicable, information about an individual must be collected directly from the individual if the information may be used to make decisions with respect to the individual's rights, benefits, and privileges under Federal programs.

d. The information that the Agency collects and maintains about individuals must be relevant and necessary to the accomplishment of the Agency's purpose as required by statute or Executive order. The office concerned must establish the relevancy of and need for the information, as well as the authority to collect it.

e. The information that is maintained in a System of Records must be kept as accurate, relevant, current, and complete as is possible to assure fairness to the individual.

f. The Agency, upon request from a subject individual, must notify the individual that it is maintaining a record on him/her and must grant the individual access to the record unless the Agency has published a rule exempting the System of Records from this requirement. In addition, the Agency must amend such record upon request, unless the Agency has published a rule exempting the System from this requirement, whenever the subject individual proves that the record is not accurate, relevant, current, or complete. If the Agency does not grant access to or amend an individual's record upon request, it must inform the individual of its refusal to grant access to or amend such record and advise him/her of the appeal rights. (See Chapters 2 and 3 for details.)

g. The Agency must not disclose information from records maintained in a System of Records to any person or agency, except with written consent of the individual to whom the record pertains. There are, however, twelve exceptions which permit disclosures without consent of the individual. They are listed in Figure 1-2. Any other disclosure of the records (other than to the subject individual) is unauthorized.

h. Except for disclosures to EPA officials and employees with an official need to know and disclosures required to be made under the Freedom of Information Act, an accounting of the disclosures that are made from a System of Records must be maintained by the System Manager. Each accounting must include the date, nature, and purpose of the disclosure, and the name and address of the person or agency to whom the disclosure was made. The accounting must be retained for the life of the record or for five years after disclosure, whichever is longer.

i. Each year, at the call of OMB, the Information Management Branch, IMSD, must prepare and submit a report of Agency activities under the Privacy Act.

7. **RESPONSIBILITIES.**

a. **Assistant Administrators, Inspector General, General Counsel, Associate Administrators, Regional Administrators, Laboratory Directors, and Staff Office Directors.** These officials are responsible for implementing the Privacy Act and the requirements specified in this Manual within their respective areas. They are responsible for designating an appropriate EPA employee to serve as System Manager for an existing or proposed System of Records.

b. **Director, Information Management and Services Division, IMSD, Office of Information Resources Management.** This individual provides overall management and policy guidance. The Chief, Information Management Branch, IMSD, is the Privacy Policy Officer and is responsible for policy, procedures and oversight of the Act. He/she administers activities related to establishment, alteration or termination of Systems.

c. **General Counsel.** The General Counsel is the EPA Privacy Appeals Officer and is responsible for interpreting the Act, reviewing Privacy Act notices, regulations, policy statements and related documents for legal form and substance and deciding all written appeals of negative determinations.

d. **Director, Personnel Management Division.** The Director, Personnel Management Division, is responsible for reviewing proposed or altered systems for personnel management implications.

e. **Managers and Supervisors.** Managers and supervisors who maintain records subject to the Privacy Act are responsible for implementing the provisions of this Manual within their respective areas.

f. **System Manager.** The EPA employee responsible for the application of approved Privacy Act policies and procedures relating to an existing or proposed System of Records and, when appropriate, implementing additional practices and procedures to cover special conditions or situations that may arise within the System of Records. In addition, the System Manager is responsible for:

1. Preparing documentation required by the Privacy Act, including notices of new, altered or terminated Systems of Records for publication in the Federal Register. (See Chapter 2.)
2. Making initial decisions whether to grant an individual access to his/her records or amend such records, and whether to extend the date of initial determination concerning requests for access to or amendment of records under the Act.
3. Safeguarding the System under his/her jurisdiction. (See Chapter 4.)
4. Informing employees having official access to the System of the penalties under the Privacy Act. (See par. 8.)

8. **PENALTIES.** The Privacy Act imposes criminal penalties directly on individuals if they violate certain provisions of the Act. Any Federal employee, for instance, is subject to a misdemeanor charge and a fine of not more than $5,000 whenever such employee:

a. Knowing that disclosure is prohibited, willfully discloses in any manner records in a System of Records to any person or agency not entitled to access to such records.

b. Willfully maintains a System of records without publishing the prescribed public notice on the System in the Federal Register.

c. Knowingly and willfully requests or obtains any record from any System of Records under false pretenses. (The penalty for violation of this provision is not limited to Federal Employees.)

(The System Manager is responsible for making employees working with a System of Records fully aware of these provisions and the corresponding penalties.)

9. **EXISTING PRIVACY SYSTEMS.** Figure 1-3 lists existing EPA Systems of Records which have been documented. (Notice published in the Federal Register.)

10. **OTHER PERTINENT EPA DIRECTIVES.** Additional guidance relevant to carrying out the provisions of the Privacy Act is found in other EPA directives as follows:

a. Forms Management Manual, Chapter 1, for forms developed in connection with the Privacy Act.

b. Federal Acquisition Regulation Subpart 24.1 and EPA Acquisition Regulation Subpart 15-24.1 for contracts involving collection and maintenance of information on individuals.

c. Delegations Manual 1-33 for authority to make determinations on appeals from the initial denial and to make determinations on correction or amendment.

d. Reports Management Manual, Chapter 4, for policy on collecting information from the public.

e. Records Management Manual, Chapters 1 and 3, for management and disposal of records.

f. EPA Order 1515.1C dated 8/23/78 for Freedom of Information Act procedures.

g. Federal Register Document Drafting Handbook for preparation of Federal Register documents.

h. Facilities and Support Services Manual, Security Volume, Part III, Chapter 13, for security requirements for Privacy Act data.

Figure 1-1: Definitions Applicable to the Privacy Act

The following definitions are applicable to this Manual:

1. "Access" means availability of a record to a subject individual.
2. "Agency" means the U.S. Environmental Protection Agency.
3. "Disclosure" means the availability or release of a record to anyone other than the subject individual.
4. "Individual" means a citizen of the U.S. or an alien lawfully admitted for permanent residence. It does not include businesses or corporations and, in certain circumstances, may not include sole proprietorships, partnerships, or persons acting in a business capacity identified by the name of one or more persons.
5. "Maintain" means to collect, use, or disseminate when used in connection with the term "record"; and, to have control over or responsibility for a System of Records when used in connection with the term "System of Records".
6. "Personal identifier" is any individual number, symbol, or other identifying designation assigned to an individual but not a name, number, symbol, or other identifying designation that identifies a product, establishment, or action.
7. "Record" means any collection or grouping of information about an individual that is maintained by the Agency, including but not limited to the individual's education, financial transactions, medical history, and criminal or employment history and that contains his/her name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph.
8. "Routine use" means, with respect to the disclosure of a record to a person or agency other than EPA, the use of a record for a purpose which is compatible with the purpose for which the record was collected. It includes disclosures required to be made by statute other than the Freedom of Information Act, 5 U.S.C. 552. It does not include other disclosures which are permitted to be made without the consent of the subject individual pursuant to Section 552a(b) of the Privacy Act, such as disclosures to EPA employees who have official need for the record, to the Bureau of the Census, to the General Accounting Office or to the Congress.
9. "Subject individual" is the individual to whom a record pertains.
10. "System Manager" is the EPA employee designated as the responsible manager of a System of Records.

11. "System of Records" means any group of records under the control of the Agency from which information is retrieved by personal identifier such as the name of the individual, or a number, symbol, or other unique identifier assigned to the individual. Single Agency records or groups of records which are not retrieved by a personal identifier are not part of a System of Records. Uncirculated personal records maintained by individual employees of the Agency which are prepared, maintained, or discarded at the discretion of the employee and which are not subject to the Federal Records Act, 44 U.S.C. 3101, do not constitute a System of Records; provided that such personal papers are not used by the employee or the Agency to make any determination concerning the rights, benefits, or privileges of individuals, and are not incorporated into an existing System of Records. A System of Records comes under the provisions of the Privacy Act.

Figure 1-2: Exceptions to the Privacy Act Prohibition against Disclosure

1. **Internal Disclosures.** The System Manager may make disclosures to officers and employees of the Agency who have a need for the record in the performance of their duties as determined by the System Manager. In some limited circumstances, disclosures to EPA contractors may be considered internal disclosures. Employees should consult with the Office of General Counsel if they have questions in this area.
2. **Disclosures Under the Freedom of Information Act.** Disclosures may be made when required by the Freedom of Information Act if there is a written Freedom of Information Act request. However, when the Freedom of Information Act does not require disclosure, but merely permits disclosure at the Agency's discretion, the Privacy Act disclosure prohibition is applicable.
3. **Routine Use.** Disclosures may be made for a routine use as described and published in the Federal Register notice describing the System or Records.
4. **Bureau of the Census.** Disclosures may be made to the Bureau of the Census for the purpose of planning or carrying out a census or survey or related activity.
5. **Statistical Research/Reporting.** Disclosures may be made to a recipient who has provided the Agency with advanced adequate written assurance that the record will be used solely as a statistical research or reporting record, and that the record is to be transferred in a form that is not individually identifiable.
6. **Preservation of Records.** Disclosures may be made to the National Archives of the United States of a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the National Archives and Records Administration to determine whether the record has such value.
7. **Civil or Criminal Law Enforcement.** Disclosures may be made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the Agency specifying the particular portion of a record desired and the law enforcement activity for which the record is sought.
8. **Health or Safety.** Disclosures may be pursuant to a showing of compelling circumstances affecting the health or safety of individuals if upon such disclosure notification is transmitted to the last known address of such individual.
9. **Congressional Disclosures.** Disclosures may be made to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee or any such joint committee. This exception does not apply to disclosures to individual members of Congress without consent of the individual.

10. **General Accounting Office.** Disclosures may be made to the General Accounting Office for the purpose of carrying out the duties of that office.
11. **Court Order.** Disclosures may be made pursuant to the order of a court of competent jurisdiction.
12. **Debt Collection.** Disclosure may be made to a consumer reporting agency in accordance with Section 3(d) of the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

Figure 1-3: EPA Systems of Records

Following is a list of EPA documented Systems of Records:

System No. and Name	Office
EPA-1 - Payroll System	Payroll Accounts Office
EPA-2 - Personnel Records	Personnel Management Div.; Local Personnel Officers
EPA-3 - Health Unit & Stress Lab Med Records	Personnel Management Div.
EPA-4 - Inspection Reports	Office of Inspector General
EPA-5 - Personnel Security File	Office of Inspector General
EPA-6 - Security Computer Program System	Office of Inspector General
EPA-7 - Travel Voucher, Advance Cards & Payee File System	Financial Management Div.
EPA-8 - Confidential Statement of Employment & Financial Interest	Office of General Counsel
EPA-9 - Freedom of Information Act File	Freedom of Information Offices; Grants, Contracts and General Admin. Div., OGC
EPA-10 - Parking Control File	Facilities & Support Services Div.
EPA-11 - Terminated	
EPA-12 - Terminated	
EPA-13 - Time Accounting Information System	Program Support Division, Office of Pesticide Programs
EPA-14 - Enforcement Case Support Expert Resources Inventory System	Technical Support Branch, Off. of Waste Prog. Enforcement

Chapter 2. Procedures for Creating, Altering or Terminating a System of Records

1. **PURPOSE.** This Chapter outlines procedures for the creation, alteration, or termination of a System of Records that meets the requirements of the Privacy Act.
2. **RESPONSIBILITY.** Assistant Administrators, the Inspector General, the General Counsel, Associate Administrators, Regional Administrators, Laboratory Directors, and Staff Office Directors are responsible for designating System Managers to carry out procedures for creating, altering, or terminating a System of Records.
3. **NEW SYSTEM OF RECORDS.** A new System of Records is one for which no public notice has been published in the Federal Register. Specifically, a new System is created whenever any one of the following criteria is met:
    a. A program, authorized by either a new or an existing statute or Executive order, requires for its successful accomplishment the creation and retrieval of individually identifiable records.
    b. There is a proposed new use of existing records that is incompatible with the purpose for which the records were originally collected. In this case, all individuals covered by the existing System of Records must be notified of the new purpose and routine uses for the records in the System and must be provided with a new Privacy Act statement.
    c. There is a new organization of records, resulting in consolidation of two or more existing systems into one new ("umbrella") system, whenever the consolidation cannot be classified under a current System notice.
    d. It is discovered that records about individuals are being created and used, and that this activity is not covered by a current, published System notice. (This is a "found System.") OMB requires the temporary suspension of data collection and disclosure in this case. (The period of suspension for a found System begins as soon as the System is "found," and continues through the advance notice period required for a new System.)
    e. A new organization (configuration) of existing records about individuals which had not previously been subject to the Privacy Act (i.e., had not been a System of Records) results in the creation of a System of Records.
4. **SIGNIFICANT ALTERATION OF A SYSTEM OF RECORDS.** A significant alteration to an existing System occurs as a result of a change in the manner in which records are organized or the manner in which records are indexed or retrieved, or a change in the nature or scope of the records. A System of Records is considered to be significantly altered when a change to the System will:
    a. Increase or change the number or type of individuals on whom records are maintained. (Changes involving the number, rather than the type, of individuals about whom records are kept need only be reported when the change significantly alters the character and purpose of the System of Records.)
    b. Expand the type or categories of information maintained. For example, if an employee file is expanded to include data on education and training, this would be considered an expansion of the "types or categories of information" maintained.
    c. Alter the manner in which the records are organized or the manner in which the records are indexed or retrieved so as to change the nature or scope of these records, such as splitting an existing System into two or more different Systems such as might occur in a centralization or a decentralization of organizational responsibilities.
    d. Alter the purpose for which information in the System is used.

e. Change the equipment configuration (that is, hardware or software on which the System is operated so as to create the potential for either greater or easier access).

f. Change procedures associated with the System in a manner which affects an individual's exercise of his/her rights.

5. **DOCUMENTATION OF NEW SYSTEM OR SIGNIFICANT ALTERATION OF EXISTING SYSTEM.** Documentation in support of a new System or significant alteration to an existing System must be sent to the Chief, Information Management Branch, IMSD, OIRM, and consist of a draft of the following: (a) narrative report of the System (for OMB); (b) Privacy Act Statement (for the individuals to whom the records pertain); and (c) System notice (Federal Register notice). Documentation must reach the Information Management Branch, IMSD, in sufficient time for Agency review, the sixty-day advance notice required by OMB prior to placing a System in operation, and the thirty-day public comment period after Federal Register publication. Documentation guidelines are contained in Figure 2-1.

6. **REQUESTS FOR WAIVER OF OMB'S SIXTY DAY ADVANCE NOTICE PERIOD.** A waiver from OMB of the sixty day advance notice requirement can be requested by the Assistant Administrator for Administration and Resource Management in compelling cases. Program requests should be made part of the documentation sent to the Chief, Information Management Branch, IMSD.

   a. The waiver must demonstrate that a delay of sixty days in establishing a System of Records--or making significant alteration to an existing System--would not be in the public interest by (1) showing how the public interest would be adversely affected if the waiver were not granted, and explaining why the responsible EPA organization was unable to provide earlier notice; or, (2) demonstrating that suspending operation of a found System would adversely affect the public interest and failure to report it was due to administrative oversight.

   b. Compelling circumstances for which a waiver request would be in the public interest include the following examples: (1) the health and safety of individuals are at serious risk, (2) the statute or Executive order authorizing the program provides a specific date for compliance, (3) there would be serious harm to a class of beneficiaries who are proposed to be included in the System.

7. **MINOR ALTERATIONS TO SYSTEM OF RECORDS.** Alterations that do not meet the criteria of par. 4 above for significantly altered System of Records require only the publication in the Federal Register of a revised notice. The thirty-day public comment period and sixty-day advance notice to OMB are not required. A draft notice is to be sent to the Chief, Information Management Branch, IMSD.

8. **TERMINATION OF SYSTEM OF RECORDS.** A System of Records is considered to be terminated whenever the information is no longer accessed by individuals' names or other identifiers, or whenever it is consolidated with another System of Records. Terminating a System may involve the physical destruction of records; it may involve purging the System of individual identifiers and maintaining the data in another form, such as statistical data; and it may involve altering the manner in which the records are accessed so that records are no longer accessed by the name of the subject individuals or other personal identifiers. Because records retired to a Federal Records Center (FRC) are still under the control of EPA, the act of retiring an inactive System to the FRC does not in itself constitute termination of the System. See Figure 2-2 for documentation guidelines.

Figure 2-1: Documentation Instructions -- New Systems and Major Alterations

Note: Complete documentation, consisting of both paper copy and floppy disk, must be sent to the Chief, Information Management Branch (PM-211-D), Information Management and Services Division, U.S. Environmental Protection Agency, Washington, D.C. 20460.

1. **Federal Register Notice.** The Federal Register notice must be prepared in accordance with the Federal Register Document Drafting Handbook and include the signature element of the Assistant Administrator for Administration and Resources Management. The following must be included in the notice:

   a. **System Name.** Provide the name of the System of Records.

   b. **Security Classification.** Identify the security classification of the System of Records. (Primarily for use by the Defense Department.) If there is no such classification, enter "none."

   c. **System Location.** Specify each address at which the System is maintained. Include Headquarters and field locations and the address of contractors, if any, who may maintain the System for EPA. If there are many locations, the list may be added as an appendix.

   d. **Categories of Individuals in System.** Describe the categories of individuals on whom records are maintained in sufficient detail to enable individuals to determine if there is information on them in the System.

   e. **Categories of Records in System.** Give a brief description of all of the types of information in the System. For example, medical history, employment history.

   f. **Authority for Maintenance of System.** Cite the specific statute(s) and/or Executive order(s) which authorize EPA to maintain the System.

   g. **Purpose(s).** State the reason(s) for creating the System and what the System is designed to accomplish.

   h. **Routine Uses of Records Maintained in the System Including Categories of Users and Purpose of Such Use.** Describe each routine use which will be made of the records, including the categories of users and the purpose of each use.

   i. **Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System.**

      - **Storage.** List all media in which records in the System are maintained (file folders, magnetic tape, microform, etc.). Briefly describe how each medium is stored.
      - **Retrievability.** Describe how the records are indexed and retrieved.
      - **Safeguards.** Describe your security policies and the procedures taken to prevent unauthorized disclosure of the records. Include the categories of EPA employees to whom access will be limited.
      - **Retention and Disposal.** Indicate how long the EPA retains the records in identifiable form. If the records are covered by a Records Control Schedule, so state.

   j. **System Manager and Address.** Give the title and complete business address of the person responsible for the records. A contractor, consultant, or anyone other than an EPA employee may not be designated as a System Manager.

   k. **Notification Procedure.** Provide the procedural information necessary for an individual to find out whether or not there are records about him/her in the System. Provide the complete address of the System Manager to which requests for notification may be presented. Do not include telephone numbers.

   l. **Record Access Procedures.** Provide the procedural information necessary for an individual to gain access to records about him/herself. Give name and address of the

System Manager whom the individuals should contact if they want to gain access to any record about themselves in the System.

m. **Contesting Records Procedures.** Provide procedures for an individual to contest the accuracy, relevancy, completeness and timeliness of records about him/herself. Give name and address of the System Manager to be contacted.

n. **Record Source Categories.** Describe the sources from which the information in the System is obtained. Sources include, but are not limited to, the individual on whom the records are maintained, previous and current employees, other agencies, etc.

o. **Systems Exempted from Certain Provisions of the Act.** Under limited circumstances, the Privacy Act permits agencies to exempt a System of Records from compliance with certain provisions of the Act. (See Chapter 3, par. 3 and Figure 3-1.) Identify the Privacy Act exemption(s), by subsection of the Act, applicable to the System; the provisions of the Act being exempted and a brief statement of the reason for invoking the exemption. Cite the Federal Register issue and page number where the proposed rule creating the exemption was published. If no exemptions are applicable, enter "none."

(NOTE: Attach a completed and signed Federal Register Typesetting Request, EPA Form 2340-15, to the Federal Register notice. This form is available through normal supply channels).

2. **Narrative Report for OMB.** This report, normally not more than two pages, must:

a. Describe the purpose of the System Records.

b. Identify the authority under which the System of Records is to be maintained.

c. Describe briefly the steps the Agency has taken to minimize the risk of unauthorized access to the System, and the higher or lower risk alternatives which the Agency considered.

3. **Privacy Act Statement.** This statement must be in writing and must inform the individual of the authority for collecting the information, the purpose for which the information is being collected on him/her and the routine uses which will be made of the information. The statement must also state whether furnishing information is voluntary or mandatory and explain what the consequences will be if an individual does not agree to furnish the information.

Sample Federal Register Notice -- New System

ENVIRONMENTAL PROTECTION AGENCY

[OA-FRL-2768-2]

Privacy Act of 1974; Proposed New System of Records

AGENCY: Environmental Protection Agency.

ACTION: Privacy Act of 1974, Proposed new system of records.

SUMMARY: As required by law (5 U.S.C.552a) the U.S. Environmental Protection Agency is publishing for comment a new system of records that it is proposing to maintain. The proposed system is "Enforcement Case Support Expert Resources Inventory System." Agency enforcement personnel will use the records to aid in the identification and selection of individuals with appropriate expertise and qualifications to serve either as expert consultants or as expert witnesses in connection with hazardous waste enforcement cases and in maintaining a record of use of experts on enforcement cases.

EFFECTIVE DATE: This system shall become effective as proposed, without further notice thirty days after publication unless comments are received which would result in contrary determination.

FOR FURTHER INFORMATION CONTACT: Mike Kosakowski, Chief, Technical Support Branch, Office of Waste Programs Enforcement (WH-527), U.S. Environmental Protection Agency, 401 M Street, S.W., Washington, D.C. 20460. Telephone: 202-382-5611.

Howard M. Messner,
Assistant Administrator for Administration and Resources Management.

EPA-15

SYSTEM NAME: Enforcement Case Support Expert Resources Inventory System--EPA-14.

SECURITY CLASSIFICATION: None.

SYSTEM LOCATION: Office of Waste Programs Enforcement (WH- 527), U.S. Environmental Protection Agency, 401 M Street, S.W., Washington, D.C. 20460.

CATEGORIES OF INDIVIDUALS IN SYSTEM: Individuals included in the system are experts in scientific and technical fields who have appropriate expertise and qualifications to serve either as consultants or expert witnesses in connection with hazardous waste enforcement cases and who have agreed to be included in the system.

CATEGORIES OF RECORDS IN SYSTEM: Basic input to the system is selected information from a professional resume and supporting documents supplied by the individual which contain such data as name, contact points and telephone numbers, educational background, disciplines, specialty areas, specific subject knowledge, research interests, specific chemical knowledge, membership in technical societies and working groups, awards and honors, consulting experience, background in litigation, professional history (with periods of employment, titles, names of employers, positions held, descriptions of work), and similar information. Certain information is entered in summary form. Other input into the system consists of records pertaining to U.S. EPA's proposed and actual use of the individual as an expert consultant or an expert witness for enforcement cases.

AUTHORITY FOR MAINTENANCE OF SYSTEM: 42 U.S.C. 9604, 9606, 9607 (Enforcement authority under Comprehensive Environmental Response, Compensation and Liability Act); 42 U.S.C. 9628, 9673 (Enforcement authority under Resource Conservation and Recovery Act).

PURPOSE(S): EPA enforcement personnel will use the records to aid in the identification and selection of potential expert consultants and expert witnesses for hazardous waste enforcement cases and in maintaining a record of use experts on cases.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USE:

1. Records of individuals will be disclosed on a case-by-case basis to the U.S. Department of Justice (U.S. DOJ) attorneys who are members of the negotiation/litigation team for the purpose of enabling their participation in the case and permitting their assistance in the selection of expert consultants and expert witnesses.
2. Records of individuals in the system will be disclosed on a case-by-case basis to other scientific and technical experts used by the U.S. EPA to familiarize them with experts for use on the case or to obtain their assistance in identifying possible expert consultants and expert witnesses.
3. Records in the system may be disclosed to OWPE enforcement contractors for the purpose of subcontracting experts identified in the system and for the purpose of updating or otherwise refining records in the system. By the terms of the contract, enforcement contractors are required to maintain the information in confidence and in accordance with the requirements of the Privacy Act.
4. Records in the system may be disclosed to the U.S. DOJ when related to litigation or anticipated litigation involving the records or the subject matter of the records.
5. Also see Prefatory Statement of General Routine Uses 41 FR 39689 (September 15, 1976).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE: Various portions of the system are maintained on computer disks, word-processor disks, and in hard-copy files.

RETRIEVABILITY: Information is retrieved from the computer database and word-processor format by addressing selected data items in the system which cross-reference to an individual's name. The name is used to manually access materials in alphabetized hard-copy files.

SAFEGUARDS: Only authorized individuals have access to the system and it is maintained under a classification of "Enforcement Confidential." Records on the computer disks are protected from access by a unique identification code. Hard-copy files and word-processor disks, when not in use or in the possession of an authorized individual, are maintained in a locked cabinet. Both the computer and cabinets are in rooms protected by door locks in a building with restricted access.

RETENTION AND DISPOSAL: Records are maintained and periodically updated until individuals identified in the system request that their own record be deleted. Other reasons for deletion will be at the discretion of the Expert Resources coordinator and the System Manager.

SYSTEM MANAGER(S) AND ADDRESS: Chief, Technical Support Branch, Office of Waste Programs Enforcement (WH-527), U.S. Environmental Protection Agency, 401 M Street, S.W., Washington, D.C. 20460.

NOTIFICATION PROCEDURES: Inquiries should be addressed to the System Manager. Additional information and requirements will be provided.

RECORD ACCESS PROCEDURES: Inquiries should be addressed to the System Manager. Additional information and requirements will be provided.

CONTESTING RECORDS PROCEDURES: Inquiries should be addressed to the System Manager. The record and the specific information being contested should be identified. The corrective action sought and supporting justification for the correction should be provided by the individual. Additional information and requirements will be provided as necessary.

RECORD SOURCE CATEGORIES:

1. Records furnished by individuals identified in the system. Information may be entered into the system in interpretive and summary form.
2. Records developed by U.S. EPA personnel concerning the proposed and actual use of expert consultants and expert witnesses.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT: None.

Figure 2-2: Documentation Instructions -- Termination of System

Note: Documentation, consisting of both paper copy and floppy disk, must be sent the Chief, Information Management Branch (PM-211-D), Information Management and Services Division, U.S. Environmental Protection Agency, Washington, D.C. 20460.

Whenever one of the conditions in Chapter 2, par. 8, occurs, actual termination of a System of Records is accomplished, and a Federal Register notice is required. A draft Federal Register notice must be sent to the Chief, Information Management Branch, IMSD. The notice must describe the following:

1. System name.
2. Original Federal Register publication citation (volume, page number, and date of publication).
3. Reason for termination.
4. Disposition of records

Sample Federal Register Notice -- Termination

Privacy Act of 1974, Notification of Deletion of System of Records

SUMMARY: The Environmental Protection Agency is deleting a system of records, Statements of Known Financial Interests (EPA-12), that is no longer in use.

DATE: Effective July 29, 1985

FOR FURTHER INFORMATION CONTACT: Mr. Donnell Nantkes, Grants, Contracts, and General Law Division, Office of General Counsel (LE-132G), Washington, D.C. 20460, telephone (202) 382-4550.

SUPPLEMENTARY INFORMATION: On September 8, 1978, and pursuant to the provisions of the Privacy Act of 1974, there was published in the *Federal Register* (43 FR 40057) a notice of the system of records, Statements of Known Financial Interests (EPA-12) Section 207(c) of the Ethics in Government Act (Pub. L. 95-521) superseded the requirement for this report. Accordingly, this notice formally deletes this system of records.

Dated: July 22, 1985
Seymour D. Greenstone,
Acting Assistant Administrator for Administration and Resources Management.

Chapter 3. Access and Amendment

(Revised December 2005)

PURPOSE

The purpose of this Chapter is to describe procedures and responsibilities for responding to a request to access or amend information in a System of Records. This Chapter has been revised to reflect changes in the Agency's process for responding to these types of requests.

PROCESSING REQUESTS FOR ACCESS

3.1 Individual Access to Personal Information

The Privacy Act permits individuals to gain access to records about themselves that EPA maintains in its systems of records, unless the records are covered by an exemption. Individuals also may request that the Agency change or amend incorrect or incomplete information. System managers, or their designees, make initial decisions to release, amend or correct individuals' records, and to extend the date for mailing initial determinations under the Privacy Act.

3.2 Individual Requests for Access

Individuals will address requests for access or amendment to personal information in a Privacy Act system of records to the EPA Privacy Act officer through EPA's Freedom of Information Act (FOIA) Office according to instructions in the relevant Privacy Act notice. A requester who cannot determine which system of records applies should write to the EPA Privacy Act officer. The FOIA Office will assign the request a tracking number and send the individual a letter acknowledging receipt of the request by the Agency

3.2.1 Time Limits

The Agency FOIA Office will acknowledge requests for access within 10 working days after receipt and forward the request to the manager of the system of records to which the request pertains, who will determine whether to grant access to the record. If the system manager cannot make a determination within 30 working days, he or she will inform the requester of the reasons for the delay, and estimate when he or she will make a decision.

3.3 Relationship Between the Privacy Act and the Freedom of Information Act (FOIA)

The Privacy Act provides seven specific exemptions to apply to systems of records. Individuals can use FOIA to seek access to records that are exempt from disclosure under the Privacy Act. The EPA FOIA Office will process Privacy Act requests under both statutes.

The EPA FOIA Office will:

- Process requests by individuals for access to records pertaining to themselves made under FOIA.
- Process requests by individuals for access to records pertaining to themselves made under the Privacy Act of 1974.
- Process requests by individuals for access to records pertaining to themselves that cite both FOIA and the Privacy Act except:
    - When FOIA access provisions provide a greater degree of access; or
    - When access to the information is controlled by another federal statute.
        - If the former applies, the FOIA staff will follow its access provisions.
        - If the latter applies, the FOIA staff will follow the access procedures established under the controlling statute.
    - Process requests by individuals for access to records pertaining to themselves in system of records that do not cite either FOIA or the Privacy Act under the procedures established by FOIA and its implementing regulations.

The system manager must cite the specific provisions of the Privacy Act or FOIA when responding to such requests. He or she may not deny individuals access to personal information concerning themselves that would otherwise be released to them under either Act solely because they fail to cite either Act or cite the wrong Act, regulation or instruction. Furthermore, the system manager must explain to the requester which Act or procedure he or she used when granting or denying access.

3.4 Verification of Identity

All Privacy Act requests must include sufficient information to verify an individual's identity. According to 40 CFR 16.3(c), an individual who cannot provide sufficient identification as listed in 40 CFR 16.4(b) must submit a signed and notarized statement indicating that he or she is the individual to whom the records pertain, and that he or she understands that it is a misdemeanor punishable by a fine up to $5,000 to knowingly and willfully seek or obtain records about another individual under false pretenses.

See Figure 1 below for a sample Privacy Act request letter that the Privacy Act officer or system manager can provide to individuals who need help preparing a request or have not provided sufficient information.

Figure 1: Sample Privacy Act Request Letter

Privacy Act officer [or Freedom of Information officer]
U.S. Environmental Protection Agency
[Street address]
[City, state, zip code]

Re: Privacy Request for Access

Dear:

This is a request under the Privacy Act of 1974.

I request a copy of any records [or specifically named records] about me maintained at EPA. These records are contained in a Privacy Act system of records titled [name of system].

[Optional] To assist with your search for these records, I am providing the following additional information: [for example: full name, Social Security number, date and place of birth]. Also, I have the

following contacts with your Agency: [for example: job applications, periods of employment, loans or Agency programs applied for, etc.].

[Optional] Please consider this request is also made under the Freedom of Information Act. Please provide any additional information that may be available under the FOIA.

If you determine that any portions of these documents are exempt under either of these statutes, I will expect you to release the non-exempt portions to me as the law requires. I reserve the right to appeal any decision to withhold information.

[Optional] Enclosed is [a notarized signature or other identifying document] that will verify my identity. I look forward to receiving your reply.

Thank you for your consideration.

Sincerely,

[Name]
[Address]
[City, state, zip code]

Acceptable identity verification for individuals seeking physical access to their records includes employee and military identification cards, drivers' licenses, other licenses, permits or passes used for routine identification purposes.

When an individual requests access by mail, the individual must provide his or her full name, date and place of birth, or other personal information necessary to locate the record he or she seeks. Additional identifying data and notarization may be required for sensitive information.

If an individual requests that he or she be accompanied by another person during a personal inspection of records or to have the records released directly to another person, he or she must submit a written statement authorizing disclosure in the presence of another person. Furthermore, the individual is not required to explain or justify his or her need for access to any record under this guidance.

(The system manager must not use identification procedures to discourage legitimate requests or to burden needlessly or delay the amendment process. He or she may not refuse access to an individual's records solely because he or she refuses to divulge his or her Social Security number, unless that is the only method by which he or she can retrieve the records.)

Only an EPA system manager may deny access. The denial must be in writing and contain the individuals' rights in accordance with 40 CFR 16.6(a)(2).

3.5 Fees

According to 40 CFR 16.9, EPA charges no fees for providing a copy of the first 100 pages of a record or any portion of a record to an individual to whom the record pertains. The fee schedule for reproducing additional pages is the same as that for FOIA requests. Since Privacy Act requests are also processed as FOIA requests, the fee schedule is governed by FOIA regulations. (See 40 CFR 2.107.)

3.6 Granting Access to Records

The system manager should grant individuals access to the original record or an exact copy of the original record pertaining to themselves without any changes or deletions, unless they have been made according to the Privacy Act's exemption rules. An amended record is considered original for the purpose of granting access. The system manager should clearly explain to the individual any amendments and deletions to records or portions of records.

If the system manager grants access, he or she notifies the Headquarters FOIA office and the individual of the decision. The individual is told:

- Where the records may be inspected;
- The earliest date (i.e., generally no more than 30 working days from the date the Agency receives the request) the records may be inspected; and,

- The times the records will remain open for inspection.

If the individual requests copies by mail, the system manager must notify him or her of the estimated date - no more than 30 working days from the date the Agency receives the request - that the record will be mailed.

3.6.1 Illegible, Incomplete or Partially Exempt Records

The system manager cannot deny an individual access to a record or a copy of a record solely because the physical condition or format of the record does not make it readily available. He or she must recopy or prepare an extract of the record within the stated time limits.

If a portion of a record contains information exempt from access, the system manager must provide an extract or summary containing all of the releasable information in the record, including a clear, written explanation to the individual of all deletions or changes to the records.

3.6.2 Access to Medical Records

Medical records maintained by EPA are not exempt from access provisions, although the Privacy Act authorizes special provisions for them under 552a(f)(3). The system manager may deny an individual direct access to medical or psychological records if he or she, in consultation with a medical doctor, determines that direct disclosure would harm the individual's physical or mental health. In this case, the system manager must offer to send the records to a physician the individual selects.

If the system manager denies direct access, he or she sends the record to the individual's physician, explaining why access without proper professional supervision could be harmful to the individual, unless it is obvious from the record. If the individual refuses or fails to designate a physician, the system manager will not provide the record. Such refusal of access is not considered a denial for Privacy Act reporting purposes.

3.6.3 Access to Information Compiled in Anticipation of Civil Action

The Privacy Act limits access to any information compiled in reasonable anticipation of a civil proceeding under 5 U.S.C. 552a(d)(5). The system manager is not required to disclose to an individual any information compiled in reasonable anticipation of a civil action or proceeding, which includes quasi-judicial and pretrial judicial proceedings. However, he or she is not required to implement this exemption by regulation.

Attorney work products prepared in conjunction with quasi-judicial, pretrial and trial proceedings, including those prepared to advise EPA officials of the possible legal consequences of a given course of action are also protected.

3.6.4 Access to Investigatory Records

The system manager will process requests by individuals for access to investigatory records pertaining to themselves and compiled for law enforcement purposes that have been incorporated into exempt system of records under the Privacy Act or FOIA, depending on which regulation gives the requester the greatest degree of access. The system manager may not deny an individual access to a record solely because it is in the exempt system. The Agency Privacy Act officer and FOIA officer will collaborate, when appropriate, to give the individual optimal access.

The system manager must refer individual requests for access to exempt investigatory records that are temporarily in the possession of a non-investigatory element for settlement or personnel actions to the originating investigating agency. He or she must inform the individual in writing of these referrals.

3.7 Denial of Access

The system manager may deny an individual access to a record pertaining to him or her for the following reasons and for the reasons itemized under Section 3.7.1, "Other Reasons to Deny Access."

If the record:

- Was compiled in reasonable anticipation of civil action;

- Is in a system of records that has been exempted from the access provisions of this guidance under one of the permitted exemptions;
- Contains classified information that has been exempted from the access provision of this regulation under the blanket exemption for such material claimed for all EPA records systems; or
- Is contained in a system of records for which access may be denied under some other federal statute.

The system manager may only deny access to portions of records if the denial serves a legitimate purpose.

3.7.1 Other Reasons to Deny Access

The system manager may also deny access if:

- The individual does not describe the record well enough for employees familiar with the file to locate it with a reasonable amount of effort; or
- The individual fails or refuses to comply with the established procedural requirements, such as refusing to name a physician to receive medical records when required or refusing to pay fees.

The system manager must explain to the individual the specific reason he or she was refused access, and how he or she may obtain it.

3.7.2 Notifying the Individual of Denial of Access

Denials of access must be in writing and include:

- The name, title and signature of the designated denial authority;
- The date of the denial;
- The specific reason for the denial, including the specific citation from the Privacy Act or FOIA;
- Notice to the individual of his or her right to appeal the denial within the 30-calendar-day time limit; and
- The title and address of the Agency Privacy Act officer.

PROCESSING ACCESS APPEALS

3.8 Access Appeal Procedures

The Agency must establish internal appeal procedures that provide for:

- Review by OGC or OIG for systems of records maintained by them, of any appeal by an individual from a denial of access to EPA records.
- Formal written notification to the individual from the system manager that must include:
    - The exact reason for denying the appeal, including specific citation to the provisions of the Privacy Act or other statute;
    - The date of the appeal determination;
    - The name, title and signature of the appeal authority; and
    - A statement informing the applicant of his or her right to seek judicial relief.

If OGC or OIG grants the appeal, it must notify the individual and provide access to the requested records. The written appeal notification granting or denying access is the final Agency action regarding access.

The individual must file any appeals from denial of access within 30 calendar days of receipt of notification. The system manager must process all appeals within 30 days of receipt unless he or she determines that he or she cannot make a fair and equitable review within that period. The system manager must notify the appellant in writing if additional time is required for the appellate review. He

or she must also include the reasons for the delay and the date when the individual may expect an answer to the appeal.

3.8.1 Denial of Appeals by Failure to Act

A requester may consider his or her appeal formally denied if the appeal authority fails:

- To act on the appeal within 30 days;
- To provide the requester with a notice of extension within 30 days; or
- To act within the time limits established in the notice of extension.

PROCESSING REQUESTS FOR AMENDMENTS

3.9 Requests for Amendment

An individual may request the amendment of any record contained in a system of records pertaining to him or her, unless the system of records has been exempted specifically from the amendment procedures of this guidance. Normally, amendments under this guidance are limited to correcting factual matters and not matters of official judgment, such as performance ratings, promotion potential and job performance appraisals.

The individual's request for amendment must in writing and sent to the EPA Privacy Act Officer. The Privacy Act Officer will assign the request a tracking number. The system manager must not use the written requirement to discourage individuals from requesting valid amendments.

A request for amendment must include:

- A description of the item or items to be amended;
- The specific reason for the amendment;
- The type of amendment action sought, i.e., deletion, correction or addition; and
- Copies of available documentary evidence supporting the request.

3.9.1 Burden of Proof

Under 40 CFR 16.5, an individual must support his or her request for amendment adequately for the system manager to approve an amendment request. The individual must submit the request in writing, including his or her name, the name of the system of records, a detailed description of the information they seek to correct or amend, the specific reasons for the correction or amendment and sufficient documentation of identity.

3.9.2 Limits on Previously Submitted Judicial Evidence

Individuals may not use this amendment process to alter evidence presented in the course of judicial or quasi-judicial proceedings. The system manager amends these records through specific procedures established for the amendment of such records.

This process does not allow a system manager to amend information that has already been the subject of a judicial or quasi-judicial determination. However, an individual may challenge the accuracy of the official recording of that determination.

3.9.3 Sufficiency of a Request to Amend

The system manager must consider the following factors when evaluating the sufficiency of a request to amend:

- The accuracy of the information itself; and
- The relevancy, timeliness, completeness and necessity of the recorded information for accomplishing an assigned mission or purpose.

3.9.4 Time Limits

The EPA Privacy Act officer must acknowledge a request to amend in writing within 10 working days of its receipt. There is no need to acknowledge a request if the action is completed within 10 working days and the individual is so informed.

The letter of acknowledgment will clearly identify the request and advise the individual when he or she may expect a determination of amendment of his or her records. Only under the most exceptional circumstances will more than 30 days be required to reach a decision on a request to amend. The system manager must also document fully in the Privacy Act case file any such decision that takes more than 30 days to resolve.

3.10 Agreement to Amendments

If the system manager decides to grant all or part of an amendment request, he or she will amend the record accordingly and notify the requesting individual.

3.10.1 Notification of Previous Recipients

The system manager must notify all previous recipients of the information, as reflected in the Privacy Act case file, of the specific nature and substance of the amendment. (See Section 3.13: Privacy Act Case Files) The system manager must inform the individual of these notifications and honor his or her requests to notify specific federal agencies of the amendment action.

3.11 Denying Amendments

If the system manager denies the request for amendment in whole or in part, he or she must promptly notify the individual of the denial in writing, including:

- The specific reason and authority for denying amendment;
- Notification that the individual may request further review of the decision by OGC or OIG, as appropriate, not later than 30 working days from the date on which he or she requests such review (5 U.S.C. 552a(d)(3));
- The procedures for appealing the decision, citing the position and address of the official to whom he or she must address the appeal; and
- Where he or she can receive assistance in filing the appeal.

3.12 Amendment Appeal Procedures

The Agency must establish procedures to ensure prompt, complete and independent review of each amendment denial appealed by an individual. These procedures must ensure that the reviewing official, i.e., OGC or OIG, receives the appeal, along with all supporting materials, including those sent to the individual and those contained in Agency records. If OGC or OIG denies the appeal completely or in part, it notifies the individual in writing that:

- It has denied the amendment appeal and the specific reason and authority for the denial; and
- If filed properly, it will include the statement of disagreement in the record.

The individual will also be informed that:

- He or she may file a statement of disagreement with the EPA office in control of the record, and the procedures for filing this statement; and
- He or she may seek a judicial review of the decision not to amend.

If the record is amended, the system manager must ensure that:

- He or she promptly notifies the individual of the decision;
- He or she notifies all prior known recipients and retainers of the records of the decision and the specific nature of the amendment; and
- He or she notifies the individual which EPA offices and federal agencies have been told of the amendment.

OGC or OIG, as appropriate, must process all appeals within 30 days unless it determines that it cannot make a fair review within this time limit. If OGC or OIG needs additional time, it must notify the individual in writing of the delay, the reason for the delay and when the individual may expect a final decision on the appeal. OGC or OIG must update the Privacy Act case file to document the reason for the delay.

3.12.1 Statements of Disagreement

If OGC or OIG refuses to amend the record, the individual may submit a concise statement of disagreement, setting forth his or her reasons for disagreeing with the decision not to amend. If the individual files a statement of disagreement, the system manager must annotate the record accordingly and furnish copies of the statement to all future recipients of the disputed information, and to all prior recipients known to hold the disputed record in their systems of records.

OGC or OIG should incorporate the statement of disagreement into the record. If this is not possible, it must ensure that it is apparent from the record that the individual filed a statement of disagreement. The system manager must maintain the statement so that it can be obtained readily when the disputed information is used or disclosed. He or she must annotate automated record systems that are not programmed to accept statements of disagreement so that they clearly indicate that a statement of disagreement is on file and identify the statement with the disputed information in the system. The system manager also must provide a copy of the statement of disagreement whenever he or she discloses the disputed information for any purpose.

3.12.2 EPA Summaries of Reasons for Refusing to Amend

OGC or OIG may, at its discretion, include a summary of reasons for refusing to amend any record for which a requester filed a statement of disagreement. OGC or OIG should only include the reasons it gave the individual for not amending the record, and not include comments on the statement of disagreement itself. OGC or OIG must file the summary and statement of disagreement together.

When disclosing information for which an individual filed a summary, the system manager may include a copy of the summary in the file.

ESTABLISHING PRIVACY ACT CASE FILES

3.13 Privacy Act Case Files

All Agency offices involved in the amendment or access process should establish Privacy Act case files to retain the documentation they receive and generate for each unique record request.

The Privacy Act case file will contain:

- The request for amendment or access;
- Copies of the EPA office's reply granting or denying the request;
- Any appeals from the individual;
- Copies of the action regarding the appeal with supporting documentation not in the basic file; and
- Any other correspondence generated in processing the appeal, including coordination documentation.

The system manager should include only the items listed below in the system of records challenged for amendment or for which access is sought. He or she must not retain copies of unamended records in the basic system of records if OGC or OIG grants a request for amendment.

The system manager must include these items relating to an amendment request in the disputed record system:

- Copies of the amended record;
- The individual's statement of disagreement;

- Program office summaries; and
- Documentation the individual submits.

The system manager may include the following items relating to an access request in the basic records system:

- Copies of the request;
- Program office's action granting or denying total access;
- Appeals filed; and
- Replies to the appeal.

Chapter 4. Physical Safeguards

1. **PURPOSE.** This Chapter prescribes policy and procedures regarding the physical safeguards of information within EPA which has been identified as being subject to the Privacy Act of 1974.
2. **POLICY.** It is EPA policy that all privacy information be safeguarded in accordance with the requirements of the Privacy Act, the applicable Federal Register notice for the System, the Security Volume, FSS Manual, Part III, Chapter 13, and the procedures outlined in this Chapter.
3. **PROTECTION OF PRIVACY ACT RECORDS.**
    a. **Handling.**
        1. Only EPA employees who require access to Privacy Act records in the performance of their official duties shall be permitted to review such documents.
        2. Privacy Act records, while in use, shall be controlled at all times and never left in an unattended office.
        3. Internal distribution within the Agency shall be by hand-carrying or transmitted within a sealed envelope and the intended recipient properly identified on the envelope. In addition, the envelope should be annotated "To be opened by addressee only," or a similar notation.
    b. **Storage.** All Privacy Act records shall be stored as outlined in the current Federal Register notice for that System of Records. Guidelines for storing existing and future Systems are outlined below:
        1. Within a keylocked cabinet within a keylocked room.
        2. When the office configuration does not permit a keylocked room, the storage cabinet should have a bar and a three positioned changeable combination padlock.
        3. Within a security cabinet with a built-in three position changeable combination lock.
        4. Any other manner authorized by the Chief, General Services Branch, Facilities and Support Services Division.
4. **TRANSFER/DESTRUCTION OF PRIVACY ACT RECORDS.**
    a. System Managers contemplating transfer to the Federal Records Center or destruction of information in a System of Records should determine that such data is eligible for transfer/destruction under authorized retention periods in the EPA Records Control Schedules.
    b. Destruction, when authorized by EPA Schedules, must be by shredding or pulping or other method that makes the data unretrievable. (The Security and Records staffs are available for assistance concerning the proper method of destruction.)