

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-03-09

To: NRC Management Directives Custodians

Subject: Transmittal of Management Directive 3.2, "Privacy Act"

Purpose: Directive and Handbook 3.2, "Privacy Act," are being revised to clarify the text and make administrative and editorial corrections. Under responsibilities and authority portion, adds Director, ADD/OCIO, to ensure privacy impact assessments are conducted; adds to office directors/regional administrators to ensure Privacy Act statements are prepared and included on forms as applicable; and adds to FOIA/PA Officer to issue annual yellow announcement re Privacy Act and to canvass office directors/regional administrators biennially regarding their responsibilities and to identify any unnoticed systems of records. Removes list of systems of records and refers individuals to the Web for current listing. Clarifies two system manager responsibilities: to provide a copy of the list of locations of duplicate records, if applicable, and issue annual guidance to custodians of duplicate records.

Office and

Division of Origin: Office of the Chief Information Officer
Web, Publishing, and Distribution Services Division

Contact: Sandra Northern, 415-6879

Date Approved: September 15, 1998 (**Revised: June 16, 2003**)

Volume: 3 Information Management

OFFICE OF ADMINISTRATION

Part: 1 Publications, Mail, and Information Disclosure

Directive: 3.2 Privacy Act

Availability: Rules and Directives Branch
Office of Administration
Michael T. Lesar, (301) 415-7163
Christy Moore, (301) 415-7086

Privacy Act

Directive

3.2

Contents

Policy	1
Objectives	1
Organizational Responsibilities and	
Delegations of Authority	2
Chairman	2
The Commission	2
Executive Director for Operations (EDO)	2
Chief Information Officer (CIO)	3
General Counsel (GC)	3
Inspector General (IG)	4
Office Directors and Regional Administrators	5
Director, Division of Accounting and Finance (DAF), Office of the Chief Financial Officer (OCFO)	6
Assistant Inspector General for Investigations (AIGI)	6
Director, Applications Development Division (ADD), Office of the Chief Information Officer (OCIO)	6
Director, Web, Publishing, and Distribution Services Division (WPDSD), OCIO	7
Director, Division of Facilities and Security (DFS), Office of Administration (ADM)	8
Director, Division of Contracts (DC), ADM	8
Freedom of Information Act and Privacy Act (FOIA/PA) Officer, WPDSD, OCIO	8
Applicability	10
Handbook	10
References	11



U. S. Nuclear Regulatory Commission

Volume: 3 Information Management
Part: 1 Publications, Mail, and Information
Disclosure

OCIO

Privacy Act Directive 3.2

Policy (3.2-01)

It is the policy of the U.S. Nuclear Regulatory Commission to ensure that systems of records are established and maintained to protect the rights of individuals from unnecessary invasion of personal privacy in accordance with the Federal Privacy Act of 1974, as amended (5 U.S.C. 552a). The processing of initial requests or appeals, consistent with the requirements and the time limits of the Privacy Act and 10 CFR Part 9, Subpart B, are not restated herein.

Objectives (3.2-02)

- To develop procedures by which individuals may determine the existence of, seek access to, and request correction or amendment of records concerning themselves that are maintained in the NRC's systems of records. (021)
- To ensure that NRC collects, maintains, uses, and disseminates any record of identifiable personal information in a manner that ensures that the action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of the information. (022)

Organizational Responsibilities and
Delegations of Authority
(3.2-03)

Chairman
(031)

If and when necessary, designates a Data Integrity Board of senior agency officials to evaluate, coordinate, and oversee implementation of any NRC computer matching program covered by the Privacy Act.

The Commission
(032)

Approves substantive changes to NRC regulations (10 CFR Part 9, Subpart B) that implement the Privacy Act and to systems of records established in compliance with the provisions of the Privacy Act and applicable guidelines.

Executive Director for Operations (EDO)
(033)

- Exercises final determination on appeals of adverse initial decisions denying access to a record, denying a request to amend or correct a record, or denying a request for an accounting of disclosures when the records are not located in the Office of the Inspector General (OIG). (a)
- Ensures that any statement of disagreement or statement of explanation concerning final adverse determinations to amend or correct records other than those located in OIG are processed as prescribed in 10 CFR 9.67 and 9.68. (b)

Organizational Responsibilities and Delegations of Authority (3.2-03) (continued)

Chief Information Officer (CIO) (034)

- As designated by the Chairman, serves as the NRC senior official with primary responsibility for privacy policy. (a)
- Designates the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, the official responsible for implementing and administering the Privacy Act program in accordance with NRC regulations. (b)
- Ensures that a program to administer the Privacy Act is established and effectively implemented within the NRC. (c)
- Issues *Federal Register* notices establishing new and amending existing systems of records and amendments to NRC regulations (10 CFR Part 9) implementing the Privacy Act in accordance with delegated authority. (d)
- Provides advice and assistance in the development of technical safeguards for the preservation of data integrity and security for systems of records using automated records or processes. (e)

General Counsel (GC) (035)

- Advises and assists in the development and implementation of NRC regulations and procedures established to comply with the Privacy Act. (a)
- Coordinates NRC activities relating to lawsuits filed under the Privacy Act. (b)

Organizational Responsibilities and
Delegations of Authority
(3.2-03) (continued)

General Counsel (GC)
(035) (continued)

- Advises and assists in determinations with respect to systems of records, requests to gain access to records or to correct or amend records, and other matters under the Privacy Act. (c)
- Advises and assists in the development of new and revised systems of records and, to ensure legal sufficiency, reviews all system notices before publication in the *Federal Register* and all Privacy Act Statements on NRC forms. (d)

Inspector General (IG)
(036)

- Implements Privacy Act and NRC procedures for responding to all requests for records located in the Office of the Inspector General (OIG). (a)
- Determines appeals on initial decisions of the Assistant Inspector General for Investigations denying access to records and amendment or correction of records, located in OIG, or a request for an accounting of disclosures. (b)
- Exercises final determination on appeals of adverse initial decisions denying access to a record, denying a request to amend or correct a record, or denying an accounting of disclosures when the records are located in OIG. (c)
- Ensures that any statement of disagreement or statement of explanation concerning final adverse determinations to amend or correct records located in OIG are processed as prescribed in 10 CFR 9.67 and 9.68. (d)

Organizational Responsibilities and Delegations of Authority

(3.2-03) (continued)

Office Directors and Regional Administrators (037)

- Ensure that all employees under their jurisdiction are informed of the provisions of this directive and that they comply with these provisions. (a)
- Provide adequate safeguards for Privacy Act records and develop a system security plan in accordance with Management Directive 12.5, "NRC Automated Information Security Program," for each automated system of records under their control or purview. (b)
- Conduct periodic reviews of systems of records under their control to ensure compliance with guidelines and procedures implementing the Privacy Act. (c)
- Ensure that the FOIA/PA Officer, OCIO, is informed about any new or contemplated systems of records or revisions to existing systems of records to carry out the functions of their office or region. Advice and assistance should be obtained from the FOIA/PA Officer, OCIO. (d)
- Ensure that Privacy Act statements are prepared and included on forms (paper or electronic) used to solicit personal information from individuals that will be maintained in a system of records. Guidance on this topic is available from the FOIA/PA Officer, OCIO. (e)

Organizational Responsibilities and
Delegations of Authority
(3.2-03) (continued)

Director, Division of Accounting and Finance (DAF),
Office of the Chief Financial Officer (OCFO)
(038)

- Receives fees charged for reproduction of records under the Privacy Act. (a)
- Implements appropriate agency debt collection procedures to collect delinquent fees charged for reproduction of records released under the Privacy Act. (b)

Assistant Inspector General for
Investigations (AIGI)
(039)

- Determines whether to release or withhold access to records, amend or correct records, and to provide an accounting of disclosures for records regarding the respective programs located in OIG. (a)
- Ensures that corrections or amendments are made to records regarding OIG's respective programs when a determination has been made that the requested correction or amendment should be granted. (b)

Director, Applications Development
Division (ADD), Office of the Chief
Information Officer (OCIO)
(0310)

Ensures that privacy impact assessments are conducted and reviewed before the NRC collects information in an identifiable form (information that permits the identity of the

Organizational Responsibilities and
Delegations of Authority
(3.2-03) (continued)

Director, Applications Development
Division (ADD), Office of the Chief
Information Officer (OCIO)
(0310) (continued)

individual to whom the information applies to be reasonably inferred directly or indirectly) or before developing or procuring information technology that collects, maintains, or disseminates such information, obtaining guidance from the Office of Management and Budget (OMB) (E-Government Act of 2002, Title II, Section 208).

Director, Web, Publishing, and Distribution
Services Division (WPDSD), OCIO
(0311)

- Develops policy and manages the NRC Privacy Act program for the collection, maintenance, and disclosure of personal information. (a)
- Recommends appropriate amendments to NRC regulations implementing the Privacy Act and *Federal Register* notices describing any new or revised systems of records. (b)
- Ensures review of the maintenance, use, or disposition of NRC official records covered by the Privacy Act to ascertain that records management policies and procedures are adequate and are being satisfactorily implemented, that the retention and disposal segments of system notices are consistent with approved records disposition schedules, and that Privacy Act statements are available for all forms (paper or electronic) that require them. (c)

Organizational Responsibilities and
Delegations of Authority
(3.2-03) (continued)

Director, Division of Facilities and Security (DFS),
Office of Administration (ADM)
(0312)

- Advises and assists, upon request, in the development of proper methods for safeguarding records covered by the Privacy Act. (a)
- Reviews classified information in systems of records and advises the FOIA/PA Officer and system managers regarding disclosure of this information. (b)

Director, Division of Contracts (DC), ADM
(0313)

Ensures that if an NRC contract provides for the design, development, or operation of a system of records (operation meaning the performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records), appropriate clauses, for example, Federal Acquisition Regulation (FAR) 52.224-1, Privacy Act Notification; 52.224-2, Privacy Act; and 52.239-1, Privacy or Security Safeguards, are included in the solicitation and contract in order to make the provisions of the Privacy Act binding on the contractor and his or her employees (5 U.S.C. 552a(m)).

Freedom of Information Act and Privacy
Act (FOIA/PA) Officer, WPDSD, OCIO
(0314)

- Administers the Privacy Act program for NRC and assumes responsibility for functions delegated by regulations to the CIO. (a)

Organizational Responsibilities and Delegations of Authority (3.2-03) (continued)

Freedom of Information Act and Privacy Act (FOIA/PA) Officer, WPDSD, OCIO (0314) (continued)

- Periodically reviews activities involving systems of records to ascertain the level of compliance with Privacy Act guidelines and procedures and provides advice, guidance, assistance, and training to system managers and NRC staff, as needed. (b)
- Prepares reports for submission to OMB, the President, and the Congress, and prepares rules and notices for publication in the *Federal Register*. (c)
- Prepares new and reviews existing Privacy Act statements for NRC forms (paper or electronic) that request individuals to furnish information about themselves. (d)
- Receives and processes requests for emergency disclosures of records, for subpoenaed or other court-ordered records, and to identify the existence of records, to gain access to records or to an accounting of disclosures, and to correct or amend records. (e)
- Ensures that appropriate fees are charged for reproduction of records as prescribed in 10 CFR 9.85. (f)
- Administers the agency responsibilities for implementing the reporting and publication requirements of the Privacy Act according to Appendix I to OMB Circular A-130. (g)
- Periodically reminds employees of their responsibilities by— (h)

Organizational Responsibilities and Delegations of Authority (3.2-03) (continued)

Freedom of Information Act and Privacy Act (FOIA/PA) Officer, WPDSD, OCIO (0314) (continued)

- Issuing annual Yellow Announcements as part of a continuing effort to ensure that agency personnel are familiar with the requirements of the Privacy Act. (i)
- Biennially canvassing office directors and regional administrators to remind them of their responsibilities to ensure that all employees under their jurisdiction are informed of and comply with the provisions of this directive and handbook and to identify any systems under their jurisdiction that contain personal information about individuals that are not already identified as systems of records. (ii)

Applicability (3.2-04)

The policy and guidance in this directive and handbook apply to all NRC employees. Contractors working under NRC contracts are bound by the same restrictions as NRC employees. In some instances, NRC contractors must sign nondisclosure agreements before they obtain information from a Privacy Act system of records.

Handbook (3.2-05)

Handbook 3.2 contains the procedures and guidelines used to implement the provisions of the Privacy Act of 1974, as amended.

References

(3.2-07)

Best Practices: Privacy, Internal Revenue Service, Privacy Impact Assessment, February 25, 2000.

Code of Federal Regulations

10 CFR Part 9, "Public Records."

48 CFR 52.224-1, "Privacy Act Notification."

48 CFR 52.224-2, "Privacy Act."

48 CFR 52.239-1, "Privacy or Security Safeguards."

M-01-05, Memorandum for Heads of Executive Departments and Agencies, "Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy," December 20, 2000.

NRC Documents

Management Directives—

3.1, "Freedom of Information Act."

12.5, "NRC Automated Information Security Program."

12.6, "NRC Sensitive Unclassified Information Security Program."

NRC NUREG-0910, "NRC Comprehensive Records Disposition Schedule," Revision 3, February 1998.

Office of Management and Budget, Circular A-130, "Management of Federal Information Resources," revision dated November 28, 2000, and published December 12, 2000 (65 FR 77677) (Transmittal Memorandum No. 4).

References

(3.2-07) (continued)

Presidential Memorandum for the Heads of Executive Departments and Agencies, "Privacy and Personal Information in Federal Records," May 14, 1998.

United States Code

Debt Collection Act of 1982 (31 U.S.C. 3701-3719), as amended by Pub. L. 104-134.

E-Government Act of 2002, Public Law 107-347, Title II, Section 208(b), Privacy Impact Assessments.

Federal Claims Collection Act, as amended (31 U.S.C. 3711(e)).

"Fraud and False Statements; Statements or Entries Generally" (18 U.S.C. 1001).

Freedom of Information Act of 1966, as amended (5 U.S.C. 552).

Privacy Act of 1974, as amended (5 U.S.C. 552a).

U.S. Department of Justice "Freedom of Information Act & Privacy Act Overview."

Privacy Act

Handbook

3.2

Contents

Part I

General	1
Privacy Act Records (A)	1
Personal Records (B)	2

Part II

NRC Systems of Records	3
<i>Federal Register</i> Notices (A)	3
Disclosures From Systems of Records (B)	5
Accounting for Disclosures (C)	7

Part III

Individual Access to and Correction of Records	9
Access to Records Maintained in a System of Records (A)	9
Privacy Act Exemptions (B)	9
Criminal Penalties (C)	10
Civil Penalties (D)	10

Part IV

Collection of Information From or About an Individual	11
Restrictions on Collecting or Maintaining Information About Individuals (A)	11
Collection of Information Directly From an Individual (B)	11
Privacy Act Statement (C)	12

Part V

Responsibilities of NRC Employees Who Work With Records	
Containing Information About Individuals	14
Responsibilities of System Managers (A)	14
Responsibilities of Custodians (B)	16
Responsibilities of NRC Employees (C)	17
Glossary	19

Part I General

The Federal Privacy Act of 1974, as amended (5 U.S.C. 552a), establishes safeguards for the protection of records the Federal Government collects, maintains, uses, and disseminates on individuals (U.S. citizens or aliens lawfully admitted for permanent residence). It balances the Government's need to maintain information on individuals with the rights of individuals to be protected against unwarranted invasion of personal privacy. Any questions about the Privacy Act should be directed to the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, Web, Publishing, and Distribution Services Division, Office of the Chief Information Officer.

Privacy Act Records (A)

The Privacy Act applies when information is retrieved by a personal identifier from agency records (e.g., paper records, electronic records, and microfiche) that contain information about individuals. In addition to containing information about individuals, the records also must contain a personal identifier, such as a person's name, Social Security number, or case number assigned to the individual.

(1)

At the present time, the Privacy Act does not apply if information is not retrieved by a personal identifier. However, any employee who maintains or is planning to maintain information about individuals retrievable by a personal identifier in either an automated or other format shall contact the FOIA/PA Officer for an up-to-date determination as to whether the Privacy Act applies to the records.

(2)

The Privacy Act applies to records maintained by the executive branch of the Federal Government, to independent regulatory

Privacy Act Records (A) (continued)

agencies, such as the NRC, to Government-controlled corporations, such as the Postal Service, and to certain contractors operating a system of records for or on behalf of a Federal agency to accomplish an agency function. (3)

The Privacy Act does not apply to records held by Congress, the courts, State and local governments, or private companies or organizations, except in certain instances in which they hold a special type of contract or agreement with a Federal agency. (4)

Personal Records (B)

Uncirculated personal notes, papers, and records, including electronic records, that are retained or discarded at the author's sole discretion and are not commingled with agency records are personal records over which the NRC exercises no control. However, if a personal record is shown or transmitted to any other individual, including orally or by e-mail, or is commingled with agency records, it may become an agency record subject to Privacy Act requirements.

Part II

NRC Systems of Records

A system of records is a group of Privacy Act records under the control of NRC from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifier assigned to an individual. The system may consist of electronic records, paper records, photographs, microfiche, and the like, alone or in any combination of formats. The system manager is the NRC employee responsible for the policies and practices governing the system of records. The duties and responsibilities of system managers, custodians of duplicate systems of records, and NRC employees who work with Privacy Act records are contained in Part V of this handbook. A current list of NRC systems of records is provided on the internal and external Web sites. Any questions about NRC's systems of records should be directed to the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, Web, Publishing, and Distribution Services Division, Office of the Chief Information Officer.

Federal Register Notices (A)

Federal agencies covered by the Privacy Act are required to publish descriptions of their systems of records in the *Federal Register*. Notices describing new or significantly revised systems of records must be published for public comment at least 40 days before they become effective and copies must be sent concurrently to Congress and the Office of Management and Budget (OMB) for their review. (1)

Each *Federal Register* notice for a system of records must include the following information: (2)

- Name and location of the system and the location(s) of any duplicate systems of records (a)

Federal Register Notices (A) (continued)

- Categories of individuals on whom records are maintained (b)
- Categories of records in the system (c)
- Routine uses that permit disclosures of records in the system to someone outside the agency (d)
- Agency policies and practices regarding storage, retrieval, safeguards, retention, and disposal of the records in the system (e)
- Sources of records in the system (f)
- Title and business address of the agency official(s) who is (are) responsible for the system (g)
- Agency procedures for individuals to follow to determine if information on themselves is contained in the system, to access that information, and to contest its content (h)
- Any exemptions for nondisclosure that have been adopted by rulemaking to apply to the system (i)

Employees shall notify the FOIA/PA Officer in writing at least 120 days before the proposed effective date of any new system of records or any significant changes to an existing system of records. The FOIA/PA Officer, after consultation with the Office of the General Counsel, shall determine whether the current system of records notice must be amended and whether a report on the amendment must be submitted to the Congress and OMB. Changes to an existing system of records include the following: (3)

- Increases or decreases in the number or types of individuals on whom records are maintained (other than normal growth)(a)

Federal Register Notices (A) (continued)

- Increases in the types or categories of information maintained (b)
- Changes to the purpose for which information is used or to whom the information is disclosed (c)
- Changes to the nature or scope of records by altering the manner in which the records are organized or the manner in which they are indexed or retrieved (d)
- Substantially greater access to the records resulting from changes in the equipment configuration (either hardware or software) (e)
- Deletion of an existing exemption contained in 10 CFR 9.95 or the addition of a new exemption (f)
- Introduction of any new, altered, or renewed computer matching program in which NRC will participate as a source or recipient agency using records maintained in the system of records (g)

Disclosures From Systems of
Records (B)

Information from a system of records cannot be disclosed to another person (a third party) without the written consent of the record subject (individual) unless the disclosure is permitted by one of the following 12 Privacy Act conditions of disclosure:

- To agency employees who “need to know” the record to perform their official duties (1)

Disclosures From Systems of Records (B) (continued)

- In response to a request under the Freedom of Information Act (FOIA) when it was determined that the public interest in disclosure outweighs the privacy interest of the individual (2)
- For a routine use, as stated in the published *Federal Register* notice for that system of records (3)
- To the Bureau of the Census for purposes of planning or carrying out a census or a survey or a related activity (4)
- To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record and the record shall be transferred in a form that is not individually identifiable (5)
- To the National Archives and Records Administration as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for the Archivist of the United States (or his or her designee) to determine whether the record has such value (6)
- 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— (7)
 - the activity is authorized by law (a)
 - the head of the agency or instrumentality has made a written request to the agency that maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought (b)

Disclosures From Systems of Records (B) (continued)

- To a third person if— (8)
 - compelling circumstances have been shown to affect the health or safety of an individual (a)
 - disclosure notification is transmitted to the last known address of subject individual (b)
- To either House of Congress or, to the extent the matter is within its jurisdiction, any committee or subcommittee, any joint committee, or subcommittee of any such joint committee (9)
- To the Comptroller General, or any of his or her authorized representatives, in the course of the performance of the duties of the General Accounting Office (10)
- Pursuant to the order of a court of competent jurisdiction (11)
- To a consumer reporting agency pursuant to the Debt Collection Act (12)

Accounting for Disclosures (C)

Disclosures from a system of records include disclosures by written, oral, electronic, or visual means. (1)

NRC employees working with records in a system of records must maintain a written accounting of any disclosures made from the system to persons outside the agency, except those released in response to a FOIA request. It is not necessary to account for disclosures made to agency employees with a “need to know” the information to perform their official duties. (2)

Accounting for Disclosures (C) (continued)

The accounting must be kept for at least 5 years or the lifetime of the record, whichever is longer. The accounting record shall contain the date, the nature, and the purpose of the disclosure, and the name and address of the person or agency to whom the disclosure was made. (3)

Individuals can request access to an accounting of their disclosures from any system of records by filing a written request with the FOIA/PA Officer. (4)

Part III

Individual Access to and Correction of Records

Access to Records Maintained in a System of Records (A)

The Privacy Act gives any individual, including any NRC employee, the right to seek the following with regard to his or her records maintained in systems of records: (1)

- Verification of the existence of a record on the individual (a)
- Access to his or her own records (b)
- Access to his or her accountings of disclosures (c)
- Amendment, correction, or deletion of his or her records when they are not accurate, relevant, timely, or complete (d)

Requests for records may be made in person or in writing. Subpart B, "Privacy Act Regulations," of 10 CFR Part 9 contains the procedures for individuals to follow to access their records as well as the requirements applicable to NRC employees with regard to the use and dissemination of such records. Employees may direct questions to the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, Web, Publishing, and Distribution Services Division, Office of the Chief Information Officer. (2)

Privacy Act Exemptions (B)

With the exception of records compiled in reasonable anticipation of a civil action or proceeding before a court or administrative tribunal under 10 CFR 9.61(a), records concerning an individual that are contained in a system of records may be exempt from

Privacy Act Exemptions (B) (continued)

disclosure to the individual only if the records meet the requirements in 10 CFR 9.61(b) or (c) and have been exempt under 10 CFR 9.95. Records or portions of records exempt under 10 CFR 9.61(c) are exempt from the provisions of the Privacy Act relating to access and amendment. Criminal law enforcement records or portions of records exempt under 10 CFR 9.61(b) are exempt from access and amendment as well as from additional provisions of the Privacy Act.

Criminal Penalties (C)

The Privacy Act provides criminal penalties and fines up to \$5000 for any officer or employee of an agency, including certain contractor employees, who willfully— (1)

- Discloses information from Privacy Act records when he or she knows that the disclosure is prohibited (a)
- Maintains a system of records without first publishing a system notice in the *Federal Register* (b)

Criminal penalties also may be imposed on any person who knowingly and willfully requests or obtains any record from the agency concerning an individual under false pretenses. (2)

Civil Penalties (D)

Privacy Act violations subject to civil remedies and the available civil remedies are contained in 10 CFR 9.90(a).

Part IV

Collection of Information From or About an Individual

Restrictions on Collecting or Maintaining Information About Individuals (A)

Only information about an individual that is relevant and necessary to accomplish a purpose of the NRC required by statute or Executive order may be maintained in an NRC system of records. (1)

The Privacy Act prohibits the collection or maintenance of records on how individuals exercise their First Amendment rights unless specifically authorized by law or related to an authorized law enforcement activity. (2)

Collection of Information Directly From an Individual (B)

To the greatest extent practicable, information for a system of records should be collected directly from the individual concerned whenever the information may result in adverse determinations about the individual's rights, benefits, and privileges under Federal programs. (1)

NRC employees or system managers shall ensure that individuals from whom information is collected about themselves for a system of records are informed of— (2)

- Reasons for requesting the information (a)
- Authority that authorizes the solicitation of the information (b)

Collection of Information Directly From an Individual (B) (continued)

- Type of disclosure (i.e., mandatory or voluntary) (c)
- Use of the information (d)
- Consequences, if any, of not providing the information (e)

NRC employees shall advise their supervisors about the existence or contemplated development of any electronic, paper, or other record system in which information about individuals is or will be retrieved by means of individual names or other personal identifiers.
(3)

Individuals from whom information about themselves is collected for a system of records, whether collected orally, electronically, or in writing, shall be provided with a Privacy Act statement on the form or document used to collect the information or on a separate form or document that can be retained by the individual, about the authority and purpose for collecting the information, the uses that will be made of the information, whether disclosure is mandatory or voluntary, and the effects, if any, of not furnishing the information.
(4)

Privacy Act Statement (C)

Any forms or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records must contain a Privacy Act statement as part of that form or separately so that the individual can retain it. A Privacy Act statement must contain the information needed to inform an individual of reasons and authority for, and use of, the information collected and must be approved by the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, Web, Publishing, and Distribution Services Division, Office of the Chief Information Officer. (1)

Privacy Act Statement (C) (continued)

Before using a new form or revising or reprinting an existing form or other document requesting information about an individual that is subject to the Privacy Act, NRC employees and system managers shall contact the FOIA/PA Officer for guidance on preparing or updating Privacy Act statements. The FOIA/PA Officer will coordinate with the Office of the General Counsel the approval of Privacy Act statements for NRC forms that request individuals to furnish information about themselves. (2)

Individuals who are requested to provide their Social Security number (SSN) shall be informed of the statutory or other authority under which the number is solicited, what uses will be made of it, and whether disclosure is mandatory or voluntary. Individuals who are asked to provide their SSN voluntarily must be advised that furnishing the SSN is not required and that no penalty or denial of benefits will result from refusal to provide it. (3)

Part V

Responsibilities of NRC Employees Who Work With Records Containing Information About Individuals

The responsibilities of system managers designated in the system of records notice published in the *Federal Register*, of custodians of duplicate systems, and of NRC employees using records contained within a system are given below.

Responsibilities of System Managers (A)

- Maintain any system of records in their control by developing and applying Privacy Act guidelines and procedures that provide for assignment of responsibility for records supervision, maintenance, and servicing, and the training of personnel assigned Privacy Act duties. (1)
- Maintain the system of records under the physical safeguards standards governing confidentiality and protection of records contained in the most recent system of records notice published in the *Federal Register*. Maintain automated systems in accordance with the system security plan developed for each automated system. (2)
- Institute and monitor a program to ensure that information in the system of records is accurate, relevant, timely, complete, and necessary for an agency purpose. (3)
- Ensure that collection of information from individuals is conducted as required in Part IV of this handbook. (4)

Responsibilities of System Managers (A) (continued)

- Establish guidelines and procedures consistent with this directive and 10 CFR Part 9, Subpart B, for gaining access to information in the system of records and for processing requests to identify the existence of a record, to access a record, to correct or amend a record, or to obtain an accounting of disclosures. (5)
- Maintain an accounting of disclosures, required by Part II of this handbook, when information about an individual maintained in a system of records is disseminated orally, electronically, or in writing to another person or to another agency unless the disclosure is to an NRC employee with a “need to know” or in response to a request pursuant to the Freedom of Information Act. (6)
- Maintain records showing the location of all duplicate systems of records or portions of duplicate systems and an inventory of any records stored off site. (7)
 - System managers will be prepared to provide a copy of their list, if applicable, during the biennial systems of records review.
- Inform the custodians of the system of records and any duplicate system of records as well as any employees who work with the records protected by the Privacy Act about the procedures, guidelines, and safeguards applicable to that system and ensure that they are followed. (8)
 - System managers will issue annual guidance as a reminder of the responsibilities involved, as stated in this handbook, which includes protecting records from unauthorized access, securing records in locked file cabinets, use of opaque envelopes when sending records through the mail, and maintaining copies of required records only. The FOIA/PA Officer will be sent a copy of this guidance as notification that this action has been completed.

Responsibilities of System Managers (A) (continued)

- Obtain, when necessary, from the Freedom of Information Act and Privacy Act (FOIA/PA) Officer, Web, Publishing, and Distribution Services Division, Office of the Chief Information Officer, advice and assistance on requests made in person to gain access to, or to correct or amend, records. (9)
- Notify the FOIA/PA Officer in writing at least 120 days before the proposed effective date of any changes to the system of records so that it may be determined if the current system notice must be amended and if a report on the amendment must be submitted to the Congress and the Office of Management and Budget. (10)
- Provide the FOIA/PA Officer with an initial determination as to whether to grant an individual access to his or her records or to amend such records and whether to extend the date of initial determination concerning requests for access to or amendment of records under the Privacy Act. (11)

Responsibilities of Custodians (B)

- Notify the system manager identified in the current system notice of the existence of any duplicate system of records or duplicate portion of a system. Failure to notify the system manager of duplicate systems or portions of systems may result in the maintenance of an unnoticed and, therefore, unauthorized system of records that could result in an individual being subject to the criminal penalties listed in Part III of this handbook. It is assumed that each office or branch maintains general personnel, travel, and payroll accounting records for persons within the organization, and it is not necessary to notify the system manager of duplicate systems in these cases. (1)
- Must comply with all requirements applicable to system managers stated above in Section (A) of this part. (2)

Responsibilities of NRC Employees (C)

- Collect no information about individuals unless authorized to collect it in the scope of their official duties. (1)
- Collect only that information about individuals that is relevant and necessary to NRC functions or responsibilities. (2)
- Collect information, wherever possible, directly from the individual to whom it relates. (3)
- Provide individuals from whom information about themselves is collected, whether orally, electronically, or in writing, with a Privacy Act statement as specified in Part IV of this handbook. This statement may be on the form or document used to collect the information or on a separate form or document that can be retained by the individual. The statement should include— (4)
 - The authority for collection (a)
 - The purpose for collecting the information (b)
 - The uses that will be made of the information (c)
 - Whether the disclosure is mandatory or voluntary (d)
 - The effects, if any, of not furnishing the information (e)
- Ensure that all information collected that is retrieved by an individual's name or other personal identifier is maintained in an authorized system of records for which a system notice has been published in the *Federal Register*. (5)
- Disseminate no information concerning individuals to persons other than those authorized by the Privacy Act or by the routine use disclosures published in the current system of records notice as specified in Part II(A) and (B) of this handbook. (6)

Responsibilities of NRC Employees (C) (continued)

- Disseminate no information concerning individuals to other NRC employees unless they have a “need to know” the information in order to perform their official duties. (7)
- Maintain an accounting of disclosures, as specified in Part II of this handbook, when information about an individual is disseminated from a system of records. (8)
- Maintain and process information concerning individuals in a manner that will ensure no inadvertent or unauthorized disclosures are made of the information. (9)
- Bring to the attention of the responsible system manager— (10)
 - Any information in a system of records used by the NRC to make a determination about an individual that appears inaccurate, irrelevant, untimely, or incomplete (a)
 - Any changes contemplated or being developed on an existing system of records that might require a revision to the published system notice (b)
 - Any duplicate systems of records. (c)
- Advise the FOIA/PA Officer about the existence or contemplated development of any new record system for which information about individuals is or will be retrieved by means of their names or other personal identifiers. (11)
- Maintain no record that describes how any individual exercises rights guaranteed by the First Amendment, unless expressly authorized by statute, or by the individual about whom the record is maintained, or unless the record is pertinent to and in the scope of an authorized law enforcement activity. (12)

Glossary

Computer matching program.

Any computerized comparison of—

(1) Two or more automated systems of records or a system of records with non-Federal records maintained by a State or local government for the purpose of—

(a) Establishing or verifying eligibility or continued compliance of applicants, recipients, beneficiaries, participants, or providers of services with respect to assistance or payments under Federal benefit programs or

(b) Recouping payments or delinquent debts under such programs

or

(2) Two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal (State or local government) records.

A computer matching program under the Privacy Act does not include—

(1) Matches done to produce statistical data without any personal identifiers;

(2) Matches done to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(3) Matches done by the Office of the Inspector General for certain criminal or civil law enforcement purposes;

Glossary (continued)

(4) Matches of Federal personnel records for routine administrative purposes and matches by an agency using records from its own systems of records if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

and

(5) Certain matches of tax information.

Custodian of a duplicate system of records. An NRC employee who maintains a duplicate system of records. The responsibilities of custodians of duplicate systems are contained in Part V of this handbook.

Duplicate system of records. A group of records that are similar to records contained in an NRC system of records. It need not contain all of the records contained in the primary system.

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

Privacy impact assessment (PIA). A process used to evaluate privacy in any new information systems, systems under development, or systems undergoing major modifications. It is designed to guide system owners and developers in assessing privacy through the early stages of development and is completed as part of the Capital Planning and Investment Control (CPIC) process. Privacy must be considered when requirements are being analyzed and decisions are being made about what data are to be used, how the data are to be used, who will use the data, and whether the implementation of the requirements presents any threats to privacy. The PIA consists of gathering data from a project on privacy issues, identifying and resolving the privacy risks, and a review by the FOIA/PA Officer. The PIA is a series of questions that when completed will describe the data in the

Glossary (continued)

system, access to the data, attributes of the data, and maintenance of administrative controls.

Record. Any item, collection, or grouping of information about an individual that is maintained by the NRC, including, but not limited to, the individual's education, financial transactions, medical history, employment history or criminal history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. A record may be in electronic, paper, or other format.

Routine use. With regard to the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected, as described in a notice published in the *Federal Register*.

Statistical record. A record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by the Census Act, 13 U.S.C. 8.

System manager. NRC official responsible for maintaining a system of records. The responsibilities of system managers are contained in Part V of this handbook.

Systems of records. A group of records under the control of the NRC from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifying particular assigned to an individual.