

U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

**MD 3.2**

**PRIVACY ACT**

**DT-17-104**

*Volume 3* Information Management

*Approved By:* Mark A. Satorius  
Executive Director for Operations

*Date Approved:* July 10, 2014

*Cert. Date:* N/A, for the latest version of any NRC directive or handbook, see the [online MD catalog](#).

*Issuing Office:* Office of Information Services  
Customer Service Division

*Contact Name:* Sally Hardy  
301-415-5607

**EXECUTIVE SUMMARY**

Directive and Handbook 3.2, "Privacy Act," are being revised to update guidance and make administrative changes. This revision—

- Reflects the April 2013 reorganization of the Office of Information Services.
- Incorporates the June 12, 1998, memorandum designating the Chief Information Officer (CIO) as Senior Official for Privacy Policy.
- Incorporates the June 15, 2009, memorandum delegating, to the Deputy Executive Director for Corporate Management, the EDO's authority to make final agency determinations on Privacy Act Appeals from non-Office of Inspector General (OIG) initial denials.
- Incorporates the November 28, 2012, memorandum delegating, to James Flanagan (currently, Director of the Office of Information Services), the CIO's authorities and responsibilities as the Senior Agency Official for Privacy.
- Incorporates current policy, standards, and procedures, including the Office of Management and Budget (OMB) M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," and OMB M-10-23, "Guidance for Agency Use of Third-Party Web Sites and Applications."
- Incorporates recommendations from the OIG Audit Report OIG-13-A-08, "Independent Evaluation of NRC's Use and Security of Social Media," January 23, 2013.

---

**TABLE OF CONTENTS**

<b>I. POLICY</b>	<b>3</b>
<b>II. OBJECTIVES</b>	<b>3</b>
<b>III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY</b>	<b>3</b>
A. Chairman	3
B. Commission	3
C. Executive Director for Operations (EDO)	3
D. Deputy Executive Director for Corporate Management (DEDCM) and Chief Information Officer (CIO)	4
E. General Counsel (GC)	4
F. Inspector General (IG)	4
G. Director, Office of Public Affairs (OPA)	5
H. Director, Office of Information Services (OIS)	5
I. Office Directors and Regional Administrators	6
J. Director, Division of the Controller (DOC), Office of the Chief Financial Officer (OCFO)	6
K. Director, Computer Security Office (CSO)	7
L. Assistant Inspector General for Investigations (AIG), OIG	7
M. Director, Customer Service Division (CSD), OIS	7
N. Director, Division of Security Operations (DSO), Office of Nuclear Security and Incident Response (NSIR)	8
O. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)	8
P. Director, Acquisition Management Division (AMD), ADM	8
Q. Privacy Act (PA) Officer, CSD, OIS	8
<b>IV. APPLICABILITY</b>	<b>9</b>
<b>V. DIRECTIVE HANDBOOK</b>	<b>10</b>
<b>VI. REFERENCES</b>	<b>10</b>

---

## I. POLICY

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 Title 10 of the *Code of Federal Regulations* (CFR) Part 9, Subpart B, "Privacy Act Regulations," are not restated herein.

## II. OBJECTIVES

- 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 Privacy Act systems of records.
- Ensure that NRC collects, maintains, uses, and disseminates any record of personally identifiable information (PII) 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. The latest guidance addressing PII, including definition and protections, is available on NRC's internal Web site, "Personally Identifiable Information (PII) Project," at <http://www.internal.nrc.gov/PII/index.html>.

## III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

### A. Chairman

1. 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.
2. Designates the Senior Official for Privacy Policy.

### B. Commission

Approves substantive changes to NRC regulations (10 CFR Part 9, Subpart B) that implement the Privacy Act.

### C. Executive Director for Operations (EDO)

1. 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, except for those records from a system of records maintained in the Office of the Inspector General (OIG) where this function will be the responsibility of the Inspector General (IG).

2. Ensures that any statement of disagreement or statement of explanation concerning final adverse determinations to amend or correct records are processed as prescribed in 10 CFR 9.67, "Statements of Disagreement," and 10 CFR 9.68, "NRC Statement of Explanation," except for those records from a system of records maintained in OIG where this function will be the responsibility of the IG.

**D. Deputy Executive Director for Corporate Management (DEDCM) and Chief Information Officer (CIO)**

1. Serves as the Senior Official for Privacy Policy.
2. Ensures that a program to administer the Privacy Act is established and effectively implemented within NRC.
3. Serves as the Senior Agency Official for Privacy (SAOP) (the official with overall responsibility and accountability, for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with Federal laws, regulations, and policies relating to information privacy) and delegates the authorities and responsibilities of the SAOP, as necessary.
4. Makes the final determinations on behalf of the Executive Director for Operations (EDO) on appeals of initial denials of Privacy Act requests and correction or amendment of Privacy Act records, in whole or in part, involving records denied by an office director who reports to the EDO and on appeals of a denial for a waiver or a reduction of fees or a denial of a request for expedited processing.

**E. General Counsel (GC)**

1. Advises and assists in the development and implementation of NRC regulations and procedures established to comply with the Privacy Act.
2. Coordinates NRC activities relating to lawsuits filed under the Privacy Act.
3. Advises and assists in determination 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.
4. 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.

**F. Inspector General (IG)**

1. Implements Privacy Act and NRC procedures for responding to all requests for records from a system of records maintained in OIG.

2. Determines appeals on initial decisions of the Assistant Inspector General for Investigations (AIGI) denying access to records and amendment or correction of records from a system of records maintained in OIG or a request for an accounting of disclosures.
3. Exercises final determination on appeals of adverse initial decisions denying access to records, denying a request to amend or correct records, or denying an accounting of disclosures when the records are from a system of records maintained in OIG.
4. Ensures that any statement of disagreement or statement of explanation concerning final adverse determinations to amend or correct records from a system of records maintained in OIG are processed as prescribed in 10 CFR 9.67 and 9.68.

**G. Director, Office of Public Affairs (OPA)**

1. Establishes NRC official media accounts/platforms and manages the agency's use of social media as an additional tool for communication with the general public on agency mission, activities, and actions. In conjunction with OIS, ensures adherence to relevant parts of the Privacy Act.
2. Provides presentations about social media to program offices throughout the agency, including the regional offices. OPA created and manages a Social Media Champions Certificate program to encourage agencywide support of social media.

**H. Director, Office of Information Services (OIS)**

1. As delegated by the Chief Information Officer, assumes the authorities and responsibilities of the SAOP.
2. Designates the Privacy Act (PA) Officer, the official responsible for implementing and administering the Privacy Act program, in accordance with NRC regulations.
3. Approves and issues *Federal Register* notices (FRN) establishing new and amending existing systems of records in accordance with delegated authority.
4. Issues amendments to NRC regulations (10 CFR Part 9) implementing the Privacy Act.
5. 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.
6. Implements a program for administering the privacy provisions of Section 208 of the E-Government Act of 2002.

**I. Office Directors and Regional Administrators**

1. Ensure that all employees in their jurisdiction are informed of the provisions of this management directive (MD) and that they comply with these provisions.
2. Provide adequate safeguards for Privacy Act records and develop a system security plan in accordance with MD 12.5, "NRC Cyber Security Program," for each automated system of records in their control or purview.
3. Conduct periodic reviews of systems of records in their control to ensure compliance with guidelines and procedures implementing the Privacy Act.
4. Ensure that the PA Officer, OIS, is informed of any new or contemplated systems of records or revisions to existing systems of records necessary to carry out the functions of their office or region. Advice and assistance should be obtained from the PA Officer, OIS.
5. 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 PA Officer, OIS.
6. Ensure that privacy impact assessments are prepared and submitted to OIS before developing or procuring information technology (IT) that collects, maintains, or disseminates personal information about individuals or when initiating, consistent with the Paperwork Reduction Act, a new electronic collection of personal information in identifiable form from 10 or more persons. Guidance is available from the PA Officer, OIS.
7. Issue exceptions in cases in which it is necessary to remove unredacted versions of paper documents containing PII outside of NRC-controlled space. The exceptions must be in writing, describe why unredacted documents are necessary, and describe how the documents will be protected while outside NRC-controlled space. These exceptions should be granted infrequently and a copy of the written exception must be provided to the Director of OIS.

**J. Director, Division of the Controller (DOC), Office of the Chief Financial Officer (OCFO)**

1. Receives fees charged for reproduction of records in the Privacy Act.
2. Implements appropriate agency debt collection procedures to collect delinquent fees charged for reproduction of records released in the Privacy Act.

**K. Director, Computer Security Office (CSO)**

1. Administers NRC's IT security program.
2. Develops and maintains IT security policies, procedures, and control techniques for electronic privacy information to address all applicable requirements.
3. Trains and oversees personnel with significant responsibilities for IT security.
4. Assists senior agency officials concerning their IT security responsibilities.
5. Approves encryption for use in protecting privacy information in systems and during transmission.
6. Notifies the senior agency official for privacy within 1 hour of discovery for incidents involving PII.

**L. Assistant Inspector General for Investigations (AIG), OIG**

1. Determines whether to release or withhold access to records, to amend or correct records, and to provide an accounting of disclosures for records from a system of records maintained in OIG.
2. Ensures that corrections or amendments are made to records from a system of records maintained in OIG when a determination has been made that the requested correction or amendment should be granted.

**M. Director, Customer Service Division (CSD), OIS**

1. Develops policy and manages the NRC Privacy Act program for the collection, maintenance, and disclosure of personal information.
2. Recommends appropriate amendments to NRC regulations implementing the Privacy Act and issues FRNs describing any new or revised systems of records.
3. 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.
4. Ensures privacy impact assessments are reviewed to address the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and records management requirements.

5. Examines a third party's privacy policy to evaluate the risks and determine whether the Web site or application is appropriate for the NRC's use upon the submission of a Privacy Impact Assessment/Privacy Threshold Analysis by the site owner.
6. Ensures that privacy impact assessments are conducted, reviewed, and approved before NRC collects information in an identifiable form (information that permits the identity of the individual to whom the information applies to be reasonably inferred directly or indirectly) or before developing or procuring IT that collects, maintains, or disseminates this information.

**N. Director, Division of Security Operations (DSO), Office of Nuclear Security and Incident Response (NSIR)**

Reviews classified information in systems of records and advises the PA Officer and system managers regarding disclosure of information.

**O. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)**

Advises and assists, upon request, in the development of proper methods for safeguarding records covered by the Privacy Act.

**P. Director, Acquisition Management Division (AMD), ADM**

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 citations, for example, Federal Acquisition Regulation (FAR) 48 CFR 52.224-1, "Privacy Act Notification"; 48 CFR 52.224-2, "Privacy Act"; and 48 CFR 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)).

**Q. Privacy Act (PA) Officer, CSD, OIS**

1. Implements and administers the Privacy Act program for NRC in accordance with the Privacy Act and NRC and the oversight agency's regulations, policies, procedures, and guidance, and exercises the functions delegated by 10 CFR Part 9, Subpart B.
2. 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.
3. Prepares reports for submission to the Office of Management and Budget (OMB), the President, and the Congress, and prepares rules and notices for publication in the *Federal Register*.

4. Prepares new and reviews existing Privacy Act Statements for NRC forms (paper or electronic) that request individuals to furnish information about themselves.
5. Acknowledges receipt of written requests to verify the existence of, obtain access to, or correct or amend records maintained by NRC in a system of records.
6. Determines whether to release or withhold access to records, correct or amend records, or to provide an accounting of disclosures for records, except for those records from a system of records maintained in OIG where this function will be the responsibility of the AIGI.
7. Ensures that corrections or amendments are made to records when a determination has been made that the requested correction or amendment should be granted, except for those records from a system of records maintained in OIG where this function will be the responsibility of the AIGI.
8. Receives and processes requests for emergency disclosures of records, for subpoenaed or other court-ordered records, to identify the existence of records, to gain access to records or to an accounting of disclosures, and to correct or amend records.
9. Ensures that appropriate fees are charged for reproduction of records as prescribed in 10 CFR 9.85, "Fees."
10. Administers the agency responsibilities for implementing the reporting and publication requirements of the Privacy Act according to Appendix I to OMB Circular A-130.
11. Periodically reminds employees of their responsibilities by—
  - (a) Issuing annual Yellow Announcements as part of a continuing effort to ensure that agency personnel are familiar with the requirements of the Privacy Act.
  - (b) Biennially advising office directors and regional administrators of their responsibilities to ensure that all employees in their jurisdiction are informed of and comply with the provisions of this directive and handbook and to identify any systems in their jurisdiction that contain personal information about individuals that are not already identified as systems of records.

#### **IV. APPLICABILITY**

The policy and guidance in this directive and handbook apply to all NRC employees. Contractors who are working on 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.

## V. DIRECTIVE HANDBOOK

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

## VI. REFERENCES

### ***Code of Federal Regulations***

- 10 CFR Part 9, "Public Records."
- 10 CFR 9.67, "Statements of Disagreements."
- 10 CFR 9.68, "NRC Statement of Explanation."
- 10 CFR 9.85, "Fees."
- 10 CFR Part 9, Subpart B, "Privacy Act Regulations."
- 48 CFR 52.224-1, "Privacy Act Notification."
- 48 CFR 52.224-2, "Privacy Act."
- 48 CFR 52.239-1, "Privacy or Security Safeguards."
- 48 CFR Part 24, Subpart 24.1, "Protection of Individual Privacy."

### ***Department of Justice***

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

### ***Internal Revenue Service***

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

### ***Nuclear Regulatory Commission***

"Interim Guidance on the Use of Social Media," dated December 28, 2010 ([ML103060402](#)).

Management Directive—

- 3.1, "Freedom of Information Act."
- 5.5, "Public Affairs Program."
- 9.2, "Organization and Functions, Office of the Inspector General."
- 12.5, "NRC Cyber Security Program."
- 12.6, "NRC Sensitive Unclassified Information Security Program."

Memorandum Regarding Delegation of Authority for Responses to Freedom of Information Act and Privacy Act Appeals, June 15, 2009.

Memorandum Regarding Delegation of Authority – Senior Agency Official for Privacy, November 28, 2012 ([ML12318A320](#)).

Memorandum Regarding Designation of Chief Information Officer as Senior Official for Privacy Policy, June 12, 1998.

Memorandum, Reminder of Privacy Act Responsibilities, November 10, 2011 ([ML11298A264](#)).

NRC Agencywide Rules of Behavior for Authorized Computer Use (ML13042A318).

NRC NUREG-0910, “NRC Comprehensive Records Disposition Schedule,” Revision 4, March 2005.

NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information, available at <http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf>.

OIG Audit Report OIG-13-A-08, “Independent Evaluation of NRC’s Use and Security of Social Media,” January 23, 2013 ([ML13023A007](#)).

“Personally Identifiable Information (PII) Project,” at <http://www.internal.nrc.gov/PII/index.html>.

Response to the OIG Audit Report OIG-13-A-08, “Independent Evaluation of NRC’s Use and Security of Social Media,” March 1, 2013 ([ML13051A776](#)).

### ***Office of Management and Budget (OMB) Documents***

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.

M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” September 26, 2003.

M-05-08, “Designation of Senior Agency Officials for Privacy,” February 11, 2005.

M-06-15, “Safeguarding Personally Identifiable Information,” May 22, 2006.

M-06-16, “Protection of Sensitive Agency Information,” June 23, 2006.

M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” July 12, 2006.

M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007.

M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," June 25, 2010, at [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-22.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf).

M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," June 25, 2010, at [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-23.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf).

OMB, 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).

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 (Pub. L. 107-347), Title II, Section 208(b), Privacy Impact Assessments (44 U.S.C. 3501 note).

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).

Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

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

U.S. NUCLEAR REGULATORY COMMISSION DIRECTIVE HANDBOOK (DH)

**DH 3.2**

**PRIVACY ACT**

**DT-17-104**

*Volume 3* Information Management

*Approved By:* Mark A. Satorius  
Executive Director for Operations

*Date Approved:* July 10, 2014

*Expiration Date:* July 10, 2019

*Issuing Office:* Office of Information Services  
Customer Service Division

*Contact Name:* Sally Hardy  
301-415-5607

**EXECUTIVE SUMMARY**

Directive and Handbook 3.2, "Privacy Act," are being revised to update guidance and make administrative changes. This revision—

- Reflects the April 2013 reorganization of the Office of Information Services.
- Incorporates the June 12, 1998, memorandum designating the Chief Information Officer (CIO) as Senior Official for Privacy Policy.
- Incorporates the June 15, 2009, memorandum delegating, to the Deputy Executive Director for Corporate Management, the EDO's authority to make final agency determinations on Privacy Act Appeals from non-Office of Inspector General (OIG) initial denials.
- Incorporates the November 28, 2012, memorandum delegating, to James Flanagan (currently, Director of the Office of Information Services), the CIO's authorities and responsibilities as the Senior Agency Official for Privacy.
- Incorporates current policy, standards, and procedures, including the Office of Management and Budget (OMB) M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," and OMB M-10-23, "Guidance for Agency Use of Third-Party Web Sites and Applications."
- Incorporates recommendations from the OIG Audit Report OIG-13-A-08, "Independent Evaluation of NRC's Use and Security of Social Media," January 23, 2013.

**TABLE OF CONTENTS**

**I. GENERAL.....3**

    A. Privacy Act Records .....3

    B. Personal Records .....4

**II. NRC SYSTEMS OF RECORDS.....4**

    A. Federal Register Notices .....4

    B. Disclosure From Systems of Records.....5

    C. Unauthorized Disclosures From Systems of Records .....7

    D. Accounting for Disclosures .....7

    E. Government Contractors .....7

**III. INDIVIDUAL ACCESS TO AND CORRECTION OF RECORDS .....8**

    A. Access to Records Maintained in a System of Records .....8

    B. Privacy Act Exemptions .....8

    C. Criminal Penalties.....9

    D. Civil Penalties .....9

**IV. COLLECTION OF INFORMATION FROM OR ABOUT AN INDIVIDUAL.....9**

    A. Restrictions on Collecting or Maintaining Information About Individuals.....9

    B. Collection of Information Directly From an Individual .....9

    C. Privacy Act Statement .....10

**V. RESPONSIBILITIES OF NRC EMPLOYEES WHO WORK WITH RECORDS CONTAINING INFORMATION ABOUT INDIVIDUALS.....11**

    A. Responsibilities of System Managers .....11

    B. Responsibilities of Custodians .....12

    C. Responsibilities of NRC Employees.....12

**VI. PRIVACY IMPACT ASSESSMENT .....15**

**VII. SOCIAL MEDIA .....15**

    A. Third Party Privacy Policies .....16

    B. Privacy Impact Assessment.....16

    C. Profiles .....17

    D. Federal Guidance .....17

    E. External Links .....17

    F. Information Collection .....17

    G. NRC Privacy Policy .....17

H. Privacy Notice .....	18
<b>VIII. GLOSSARY .....</b>	<b>18</b>

---

## 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 Privacy Act (PA) Officer, Customer Service Division (CSD), Office of Information Services (OIS).

### A. Privacy Act Records

1. 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 (e.g., a person's name, Social Security number, passport/visa number, or case number assigned to the individual).
2. 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 PA Officer for an up-to-date determination as to whether the Privacy Act applies to the records.
3. The Privacy Act applies to records maintained by the executive branch of the Federal Government, to independent regulatory agencies (e.g., the U.S. Nuclear Regulatory Commission), to Government-controlled corporations (e.g., 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.
4. 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.
5. Electronic records implementations must comply with Management Directive (MD) 12.5, "NRC Cyber Security Program."

## B. Personal Records

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 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. For further discussion to ensure compliance of electronic records, see MD 12.5.

## 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 Section 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 PA Officer, CSD, OIS.

### A. Federal Register Notices

1. 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.
2. Each *Federal Register* notice for a system of records must include the following information:
  - (a) Name and location of the system and the location(s) of any duplicate systems of records;
  - (b) Categories of individuals on whom records are maintained;
  - (c) Categories of records in the system;
  - (d) Routine uses that permit disclosures of records in the system to someone outside the agency;
  - (e) Agency policies and practices regarding storage, retrieval, safeguards, retention, and disposal of the records in the system;

- (f) Sources of records in the system;
  - (g) Title and business address of the agency official(s) who is (are) responsible for the system;
  - (h) 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; and
  - (i) Any exemptions for nondisclosure that have been adopted by rulemaking to apply to the system.
3. Employees shall notify the 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 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:
- (a) Increases or decreases in the number or types of individuals on whom records are maintained (other than normal growth),
  - (b) Increases in the types or categories of information maintained,
  - (c) Changes to the purpose for which information is used or to whom the information is disclosed,
  - (d) 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,
  - (e) Substantially greater access to the records resulting from changes in the equipment configuration (either hardware or software),
  - (f) Deletion of an existing exemption contained in Title 10 of the *Code of Federal Regulations* (CFR) Section 9.95, "Specific Exemptions," or the addition of a new exemption, and
  - (g) 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.

#### **B. Disclosure From Systems of Records**

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:

1. To agency employees who "need to know" the record to perform their official duties.

2. In response to a request under the Freedom of Information Act (FOIA) when no FOIA exemption permits withholding. See MD 3.1, "Freedom of Information Act," and contact the agency's FOIA Officer for additional information.
3. For a routine use, as stated in the published *Federal Register* notice for that system of records.
4. To the Bureau of the Census for purposes of planning or carrying out a census or a survey or a related activity.
5. 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.
6. 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.
7. 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—
  - (a) The activity is authorized by law, and
  - (b) 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.
8. To a third person if compelling circumstances have been shown that affect the health or safety of an individual and disclosure notification is transmitted to the last known address of the subject individual. The notice shall be issued within 5 days of the disclosure and contain—
  - (a) The nature of the information disclosed,
  - (b) The name of the person or agency to whom the information was disclosed,
  - (c) The date of the disclosure, and
  - (d) The compelling circumstances justifying the disclosure.
9. To either House of Congress or, to the extent the matter is within its jurisdiction, any committee or subcommittee, any joint committee of Congress, or subcommittee of any joint committee.
10. To the Comptroller General, or any of his or her authorized representatives, in the course of the performance of the duties of the Government Accountability Office.

11. Pursuant to the order of a court of competent jurisdiction.
12. To a consumer reporting agency pursuant to the Debt Collection Act.

### **C. Unauthorized Disclosures From Systems of Records**

1. The unauthorized disclosure of any information from a system of records by any means of communication to any person, or to another agency, should be promptly reported to the following agency representatives to determine further action:

Executive Director for Operations  
Inspector General  
cc: System Manager

2. There are special reporting requirements for the unauthorized disclosure/inadvertent release of **personally identifiable information (PII)**. These reporting requirements, along with the latest guidance addressing PII, are available on NRC's internal Web site, "Personally Identifiable Information (PII) Project," at <http://www.internal.nrc.gov/PII/index.html>.

### **D. Accounting for Disclosures**

1. Disclosures from a system of records include disclosures by written, oral, electronic, or visual means.
2. 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.
3. 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.
4. Individuals can request access to an accounting of their disclosures from any system of records by filing a written request with the FOIA Officer or PA Officer.

### **E. Government Contractors**

When an agency issues a contract for the design, development, or operation of a system of records on individuals ("operation" meaning the performance of any of the activities associated with maintaining a system of records, including the collection, use, and dissemination of records) to accomplish an agency function, the agency will ensure that the wording of each contract makes the provisions of the Privacy Act binding on the

contractor and his or her employees by incorporating the following citations into the contracts:

1. Federal Acquisition Regulation (FAR) 52.224-1 Privacy Act Notification.
2. FAR 52.224-2 Privacy Act.

### **III. INDIVIDUAL ACCESS TO AND CORRECTION OF RECORDS**

#### **A. Access to Records Maintained in a System of Records**

1. 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:
  - (a) Verification of the existence of a record on the individual;
  - (b) Access to his or her own records;
  - (c) Access to his or her accountings of disclosures; and
  - (d) Amendment, correction, or deletion of his or her records when they are not accurate, relevant, timely, or complete.
2. 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 these records. Employees may direct questions to the FOIA Officer, CSD, OIS.

#### **B. Privacy Act Exemptions**

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 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.

**C. Criminal Penalties**

1. The Privacy Act provides criminal penalties and fines up to \$5,000 for any officer or employee of an agency, including certain contractor employees, who willfully—
  - (a) Discloses information from Privacy Act records when he or she knows that the disclosure is prohibited.
  - (b) Maintains a system of records without first publishing a system notice in the *Federal Register*.
2. 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.

**D. Civil Penalties**

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

**IV. COLLECTION OF INFORMATION FROM OR ABOUT AN INDIVIDUAL****A. Restrictions on Collecting or Maintaining Information About Individuals**

1. Only information about an individual that is relevant and necessary to accomplish a purpose of NRC required by statute or Executive order may be maintained in an NRC system of records.
2. 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.

**B. Collection of Information Directly From an Individual**

1. 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.
2. NRC employees or system managers shall ensure that individuals from whom information is collected about themselves for a system of records are informed of—
  - (a) Reasons for requesting the information,
  - (b) Authority that authorizes the solicitation of the information,
  - (c) Type of disclosure (i.e., mandatory or voluntary),

- (d) Use of the information, and
  - (e) Consequences, if any, of not providing the information.
3. 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.
  4. 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.

### **C. Privacy Act Statement**

1. 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 PA Officer, CSD, OIS.
2. 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 PA Officer for guidance on preparing or updating Privacy Act statements. The 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.
3. 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.

## **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.

### **A. Responsibilities of System Managers**

1. 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.
2. 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.
3. 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.
4. Ensure that collection of information from individuals is conducted as required in Section IV of this handbook.
5. Establish guidelines and procedures consistent with this MD 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.
6. Maintain an accounting of disclosures, required by Section 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 FOIA.
7. 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.
8. Provide a copy of their records list, if applicable, during the biennial systems of records review.
9. 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.

10. 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 PA Officer will be sent a copy of this guidance as notification that this action has been completed.
11. Log all computer-readable data extracts from any system in their control holding PII and verify that each extract, including PII, has been erased within 90 days or that its use is still required. For systems that cannot automatically generate logs of data extracts, manual logs must be maintained.
12. Obtain, when necessary, from the PA Officer, advice and assistance on requests made in person to gain access to, or to correct or amend, records.
13. Notify the 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 Congress and OMB.
14. Provide the PA Officer with an initial determination as to whether to grant an individual access to his or her records or to amend these records and whether to extend the date of initial determination concerning requests for access to or amendment of records under the Privacy Act.

#### **B. Responsibilities of Custodians**

1. 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 Section III of this handbook. It is assumed that each office or branch maintains general personnel, travel, training, 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.
2. Must comply with all requirements applicable to system managers stated above in Section V.A of this handbook.

#### **C. Responsibilities of NRC Employees**

1. Collect no information about individuals unless authorized to collect it in the scope of their official duties.
2. Collect only that information about individuals that is relevant and necessary to NRC functions or responsibilities.

3. Collect information, wherever possible, directly from the individual to whom it relates.
4. Provide individuals from whom information about themselves is collected, whether orally, electronically, or in writing, with a Privacy Act statement as specified in Section 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—
  - (a) The authority for collection,
  - (b) The purpose for collecting the information,
  - (c) The uses that will be made of the information,
  - (d) Whether the disclosure is mandatory or voluntary, and
  - (e) The effects, if any, of not furnishing the information.
5. 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*.
6. 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 Sections II.A and B of this handbook.
7. 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.
8. Maintain an accounting of disclosures, as specified in Section II of this handbook, when information about an individual is disseminated from a system of records.
9. Maintain and process information concerning individuals in a manner that will ensure no inadvertent or unauthorized disclosures are made of the information.
  - (a) Do not leave information in open view of others, either on your desk or computer screen.
  - (b) Use an opaque envelope when transmitting information through the mail.
  - (c) Information from a system of records should be stored in accordance with the system notice.
  - (d) If unsure whether information about an individual is part of a system of records, safeguard it at a minimum in a **locked drawer/cabinet or password-protected/restricted access file**. Placing information about individuals on a shared network drive is not recommended. However, if it is necessary to place information about individuals on a shared network drive, it is important to institute access controls.

10. Staff is prohibited from removing electronic PII from NRC-controlled space on mobile computers or devices unless the PII is encrypted.
11. Staff is prohibited from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted. In cases in which it is necessary to take unredacted documents outside NRC controlled space, office directors or regional administrators or their designees may issue exceptions. However, the exceptions must be in writing, describe why unredacted documents are necessary, and describe how the documents will be protected while outside NRC-controlled space. These exceptions should be granted infrequently and a copy of the written exception must be provided to the Director of OIS. This direction does not prohibit the removal or use of emergency contact information outside NRC-controlled space; an exception is not required.
12. Staff is prohibited from placing PII pertaining to NRC official business on personally owned hard drives, removable media, and other stand-alone storage devices.
13. Staff is prohibited from the use of personally owned computers for processing or storing PII of individuals pertaining to NRC official business other than themselves.
14. NRC remote broadband access through Citrix is approved.
15. Staff is prohibited from storing on or downloading to mobile remote access devices PII pertaining to NRC official business unless these mobile remote access devices are password protected, and where possible, lock out after 30 minutes (or less) of user inactivity.
16. Staff is prohibited from sending e-mail containing PII outside the agency except where necessary to conduct agency business. Effective privacy protections are essential to all NRC information technology (IT) systems, especially those that contain substantial amounts of PII. The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal, including to and from BlackBerry hand-held devices interacting within NRC's e-mail system.
17. Bring to the attention of the responsible system manager—
  - (a) Any information in a system of records used by NRC to make a determination about an individual that appears inaccurate, irrelevant, untimely, or incomplete.
  - (b) Any changes contemplated or being developed on an existing system of records that might require a revision to the published system notice.
  - (c) Any duplicate systems of records.

18. Advise the 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.
19. 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.

## VI. PRIVACY IMPACT ASSESSMENT

- A. The E-Government Act of 2002 requires that agencies prepare a privacy impact assessment (PIA) before developing or procuring IT that collects, maintains, or disseminates personal information in identifiable form about members of the public who are not Government employees or when initiating, consistent with the Paperwork Reduction Act, a new electronic collection of personal information in identifiable form from 10 or more persons. However, agencies are encouraged to conduct PIAs for all existing electronic information systems or ongoing collections of information in identifiable form, including those about Government personnel.
- B. A PIA is 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 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 is designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and records management requirements through a series of questions that, when completed, will describe the data in the system, access to the data, attributes of the data, and maintenance of administrative controls.
- C. Offices are responsible for preparing a PIA for each IT project/system they sponsor and submitting the PIA to OIS for review and approval. PIA templates and guidance are available on the internal Web site, at [http://www.internal.nrc.gov/CSO/System\\_Authorization.html](http://www.internal.nrc.gov/CSO/System_Authorization.html).

## VII. SOCIAL MEDIA

The use of selected social media and Web-based interactive technologies, including blogs, wikis, and social networks, is a way to enhance public and stakeholder participation in NRC activities and to enable NRC employees to network and interact with professional

colleagues. Refer to “Interim Guidance on the Use of Social Media” that describes how and when NRC employees may represent the agency or use agency assets to engage in social media activities and defines the NRC’s expectations for conducting these interactions, available on the NRC internal Web page at <http://www.internal.nrc.gov> and in the Agencywide Documents Access and Management System (ADAMS) (Accession No. ML103060402). This interim guidance also addresses OMB M-10-22, “Guidance for Online Use of Web Measurement and Customization Technologies,” available at [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-22.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf) and OMB M-10-23, “Guidance for Agency Use of Third-Party Websites and Applications,” available at [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-23.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf). Also, see MD 5.5, “Public Affairs Program,” <http://www.internal.nrc.gov/policy/directives/toc/md5.5.htm>.

#### **A. Third Party Privacy Policies**

Before NRC uses any third-party Web site or application to engage with the public, the NRC must examine the third party’s privacy policy to evaluate the risks and determine whether the Web site or application is appropriate for the NRC’s use. The site owner of these third-party Web sites would need to submit a PIA or Privacy Threshold Analysis (PTA) to allow OIS to examine the privacy policy. In addition, the Site Owner should monitor any changes to the third party’s privacy policy and periodically reassess the risks and update the PIA/PTA, as necessary.

#### **B. Privacy Impact Assessment**

OMB requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party technologies to engage with the public. A PIA is required to be conducted **before** using third-party Web sites and applications, and must be updated as needed to address significant changes. This also applies when NRC relies on a contractor (or other non-Federal entity) to operate a third-party Web site or application to engage with the public on the agency’s behalf. The PIA should clearly describe:

1. Specific purpose of the NRC’s use of the third-party Web site or application,
2. Any PII that is likely to become available to the NRC through public use of the third-party Web site or application,
3. NRC’s intended or expected use of the PII,
4. With whom the NRC will share the PII,
5. Whether and how the NRC will maintain the PII, and for how long,
6. How the NRC will secure the PII that it uses or maintains,

7. What other privacy risks exist and how the NRC will mitigate those risks, and
8. Whether the NRC's activities will create or modify a "system of records" under the Privacy Act.

### **C. Profiles**

Profiles created for social media site accounts used for NRC official presence and external involvement are restricted to NRC employee work and office-related information. No personal information, including PII, is permitted. For additional details, see Interim Guidance on the Use of Social Media (Accession No. ML103060402).

### **D. Federal Guidance**

For more information on social media see <http://www.digitalgov.gov/category/socialmedia/>.

### **E. External Links**

If NRC posts a link that leads to a third-party Web site or any other location that is not of an official government domain, the NRC must provide an alert to the visitor explaining that they are being directed to a non-government Web site that may have different privacy policies from those of the NRC.

### **F. Information Collection**

If PII is collected through the NRC's use of a third-party Web site or application, the NRC should collect only the minimum necessary to accomplish a purpose required by statute, regulation, or Executive order.

### **G. NRC Privacy Policy**

OIS will ensure that the NRC Privacy Policy describes the NRC use of any third-party Web sites and applications, to include the following:

1. The specific purpose of the NRC's use of the third-party Web sites or applications,
2. How the NRC will use PII that becomes available through the use of the third-party Web sites or applications,
3. Who at the NRC will have access to PII,
4. With whom PII will be shared outside the NRC,
5. Whether and how the NRC will maintain PII and for how long,
6. How the NRC will secure PII that it uses or maintains,
7. What other privacy risks exist and how the NRC will mitigate those risks, and

8. Whether the NRC's activities will create or modify a "system of records" under the Privacy Act.

#### **H. Privacy Notice**

1. To the extent feasible, NRC should post a Privacy Notice, described below, on the third-party Web site or application itself.
  - (a) Explain that the Web site or application is not a government Web site or application, that it is controlled or operated by a third party, and that the NRC Privacy Policy does not apply to the third party.
  - (b) Indicate whether and how the NRC will maintain, use, or share PII that becomes available through the use of the third-party Web site or application.
  - (c) Explain that by using the Web site or application to communicate with the NRC, individuals may be providing nongovernment third parties access to PII.
  - (d) Direct individuals to the NRC's official Web site.
  - (e) Direct individuals to the NRC Privacy Policy as described above in Section VII.G of this handbook.
2. NRC should take all practical steps to ensure that its Privacy Notice is conspicuous, clearly labeled, written in plain language, and prominently displayed at all locations where the public might "make PII available" to the NRC.
3. The term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the Web site or application. "Associate" can include activities commonly referred to as "friending," "liking," joining a "group," becoming a "fan," and comparable functions.

### **VIII. 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 these programs.

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—
  - (a) Matches done to produce statistical data without any personal identifiers;
  - (b) Matches done to produce background checks for security clearances of Federal personnel or Federal contractor personnel;
  - (c) Matches done by the Office of the Inspector General for certain criminal or civil law enforcement purposes;
  - (d) 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
  - (e) 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 Section 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.

### **Personally Identifiable Information (PII)**

The current definition of PII can be found at NRC's internal Web page "Personally Identifiable Information (PII) Project," <http://www.internal.nrc.gov/PII/index.html>, along with the latest guidance addressing PII. Only PII that is part of a Privacy Act system of records will be protected by the provisions of the Privacy Act. Therefore, while some PII may be considered Privacy Act information, not all of it is. PII that is contained in documents, files, or databases not part of a system of records will not receive the specific benefits of this legal protection but is to be treated in accordance with applicable agency policy for handling sensitive information.

**Privacy Impact Assessment (PIA)**

An analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

**Privacy Notice**

While a Privacy Policy is a statement about an agency's general practices, the term "Privacy Notice" refers to a brief description of how the agency's Privacy Policy will apply in a specific situation. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on a specific Web page or application where individuals have the opportunity to make PII available to the agency.

**Privacy Policy**

A single, centrally located statement that is accessible from an agency's official home page. The Privacy Policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official Web site and its other online activities.

**Privacy Threshold Analysis (PTA)**

A PTA can be used to determine whether a PIA is needed. Some information systems will not require a PIA if the system will not collect, maintain, or disseminate information about individuals. To assist in determining whether a PIA is required, a program manager or system owner can use the PTA to help determine if a PIA is required. If a review of the PTA determines that information about individuals will *in fact* be collected, maintained, or disseminated by the system, the Privacy Act Program Analyst will instruct the program manager or system manager to complete a PIA. If a PIA is not required, the system will have an official privacy analysis on file documenting the determination which will be required for the Certification and Accreditation (C & A) process.

**Record**

Any item, collection, or grouping of information about an individual that is maintained by 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, including a fingerprint, voiceprint, 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 a record 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 Section V of this handbook.

**Systems of Records**

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

**Third-Party Web Sites or Applications**

Web-based technologies that are not exclusively operated or controlled by a government entity, or Web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a “.com” Web site or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official Web site.