EPA Classification No.: CIO 2151.0	CIO Approval Date: 9-27-07
CIO Transmittal No.: 07-004	Review Date: 9-10

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

PRIVACY POLICY

1. PURPOSE

The Privacy Policy establishes Agency requirements for safeguarding the collection, access, use, dissemination, and storage of personally identifiable information (PII) and Privacy Act information in accordance with the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), and policy and guidance issued by the President and Office of Management and Budget (OMB). This Policy also establishes the National Privacy Program for EPA which will provide national oversight for administering and ensuring EPA's compliance with its requirements under the Acts. In addition, this Policy informs Agency employees and managers of their roles and responsibilities under those statutes and programs.

2. SCOPE AND APPLICABILITY

This Policy applies to all EPA employees, managers, contractors, and grantees working on behalf of EPA who handle, control, or access documents, records, or information technology (IT) systems that contain Privacy Act and personally identifiable information.

3. AUDIENCE

The audience for this Policy includes all EPA employees, managers, contractors, and grantees working on behalf of EPA who handle, control, or access Privacy Act and personally identifiable information.

4. BACKGROUND

Congress has passed laws that protect the privacy of individuals. These various laws and OMB directives require protection of Privacy Act and personally identifiable information that EPA collects. The Privacy Act of 1974 (5 U.S.C. 552a) sets forth requirements for federal agencies when they collect, maintain or disseminate information about individuals. The Act requires that federal agencies (a) collect minimal information necessary on individuals, (b) safeguard the information, and (c) allow individuals to inspect and correct erroneous information. Congress understood that certain governmental activities were not amenable to the exercise of all the individuals rights provided for in the Privacy Act such as documents relating to criminal investigations. Accordingly, agencies are allowed to exempt certain types of record systems from some of the requirements of the Act. Agencies are required to publish a System of Records Notice (SORN) in the Federal Register upon establishment of or substantial revision of a group of records containing information covered under the Privacy Act. If EPA is involved in a computer matching program (i.e., computer comparison of two or more system of records), 5 U.S.C. 552a(u) requires that EPA establish a Data Integrity Board, consisting of senior officials, to oversee and coordinate among the various agency components the

implementation of a matching program. Without the proper security and access controls, the PII and Privacy Act information collected by agencies is vulnerable to unauthorized access and use.

New information technologies have created additional responsibilities for managing Privacy Act information and PII not covered by the Privacy Act. Agency practices should guard against unauthorized disclosure or misuse of PII (in paper and electronic formats). For example, EPA reviews its use of Social Security numbers (SSNs) in Agency systems and programs to identify instances in which collection or use of the SSN is superfluous.

The E-Government Act of 2002, Section 208, requires agencies to conduct Privacy Impact Assessments when developing Information Technology (IT) that collects, maintains, or disseminates information in an identifiable form or initiates new collection of information that will use IT.

Homeland Security Presidential Directive 12 (HSPD-12) established policy to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing mandatory, Government-wide standards for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.

5. AUTHORITY

A. 5 U.S.C. 552a - Privacy Act - Records maintained on individuals (http://assembler.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html)

B. 5 U. S. C. 552 - The Freedom of Information Act (FOIA) (http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)

C. E-Government Act of 2002 (Public Law 107-347,44 U.S.C. Ch 36) http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107HZEsNo:e1143:

D. 40 C.F.R. Part 16 – Implementation of Privacy Act of 1974: Revision to the Privacy Act Regulations – January 4, 2006 (http://www.epa.gov/fedrgstr/EPA-GENERAL/2006/January/Day-04/g45.htm)

E. 48 C.F.R. 24.1 Federal Acquisition Regulation (FAR), Protection of Individual Privacy (http://acquisition.gov/far/97-06/pdf/24.pdf#search=%22Federal%20Acquisition%20Regulation%2C%20Protection%20of%20Individual%20Privacy%22)

F. 48 C.F.R. 1524.1, EPA Acquisition Regulation (EPAAR), Protection of Individual Privacy (http://www.epa.gov/fedrgstr/EPA-GENERAL/2003/January/Day-22/g1361.htm)

G. 40 FR 28948 – OMB's Privacy Act Implementing Guidelines (http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf)

H. 54 FR 25818 – OMB's Computer Matching and Privacy Protection Act Final Guidance (http://www.whitehouse.gov/omb/privacy/matching.html)

I. Delegation of Authority 1-84 Information Resources Management (http://intranet.epa.gov/rmpolicy/ads/dm/1-84_534.htm)

J. Delegation of Authority 1-33 Privacy Act (http://intranet.epa.gov/rmpolicy/ads/dm/1-33.htm)

EPA Classification No.: CIO 2151.0	CIO Approval Date: 9-27-07
CIO Transmittal No.: 07-004	Review Date: 9-10

6. POLICY

It is the policy of the Environmental Protection Agency to safeguard individuals' privacy in a manner consistent with the Privacy Act, E-Government Act, OMB directives and other federal requirements concerning privacy. EPA hereby establishes a National Privacy Program to oversee privacy policies, procedures, practices, standards or guidance and implementation of the provisions in a manner consistent with these Acts and Directives. This policy does not supersede any other laws or regulations.

A. EPA will appropriately safeguard all personally identifiable information in its possession.

B. EPA will limit the collection of personally identifiable information to only that which is necessary to accomplish an official EPA mission, administrative function, regulatory or statutory requirement or OMB or Homeland Security directives concerning privacy.

C. EPA will manage information and technology to protect PII from unauthorized disclosure and misuse.

D. EPA will provide a Privacy Act Statement to the individual upon the collection of PII that will be maintained in a Privacy Act system of records.

E. EPA will not collect or use a SSN as a personal identifier in connection with any information system or database, unless the collection and/or use is authorized and provided for by law.

F. Privacy Act Officer must approve all forms that collect sensitive PII prior to issuance of an EPA form number.

G. EPA will not disseminate or publish Privacy Act information without the prior consent of the individual, unless provided for by law.

H. EPA will conduct Privacy Impact Assessments (PIAs) in accordance with Section 208 of the E-Gov Act. In addition, all IT system owners will be required to conduct Privacy Threshold Analysis (PTA) utilizing risk-based criteria consistent with federal and Agency standards and requirements and approved by the Senior Agency Official for Privacy, to determine the need for a PIA.

I. EPA will ensure appropriate and prompt notification to affected individuals in the event of a breach of sensitive PII commensurate with risk of harm to the individual(s) and consistent with federal and Agency standards and requirements.

J. EPA will report all incidents involving the security, loss, misuse or unauthorized disclosure of PII regardless of form or format immediately in accordance with established EPA, OMB and US-CERT (U.S. Computer Emergency Readiness Team) security incident reporting procedures and requirements.

K. EPA's determination will be in writing for all requests to access sensitive PII from an offsite location or to take sensitive PII offsite in accordance with established procedures.

L. EPA will employ a risk-based approach to protect PII consistent with federal and Agency standards and requirements and approved by the Senior Agency Official for Privacy, to protect PII.

M. EPA's use of new technologies will support and not diminish the protections provided in statutes related to Agency use, collection and disclosure of personally identifiable information.

EPA employees, managers, contractors, and grantees working on behalf of EPA must adhere to Privacy rules of conduct and are subject to appropriate administrative, civil, or criminal penalties if they knowingly, willfully, or negligently disclose Privacy Act information to unauthorized persons. Each case will be handled on an individual basis with a full review of all pertinent facts. The severity of the violation will determine the action taken.

7. RELATED DOCUMENTS

A. OMB Circular No. A-130 Appendix I to OMB Circular No. A-130 "Federal Agency Responsibilities for Maintaining Records About Individuals" (http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html)

B. OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notifications," September 20, 2006 http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf

C. OMB Memorandum, M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007 (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf)

D. OMB Memorandum, "Reporting Incidents Involving PII and Incorporation of Costs for Security in Agency Information Technology Investments," July 12, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf)

E. OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," June 23, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf)

F. OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," May 22, 2006 (http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf)

G. OMB Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy," September 30, 2003 (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf)

H. OMB Memorandum M-03-18, "Implementation of the Privacy Provisions of the E-Government Act of 2002," August 1, 2003 (www.whitehouse.gov/omb/memoranda/m03-18.pdf)

I. OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003 (www.whitehouse.gov/omb/memoranda/m03-22.html)

J. OMB Memorandum M-01-05, "Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy," December 20, 2000 (http://www.whitehouse.gov/omb/memoranda/m01-05.html)

K. OMB Memorandum M-00-13, "Privacy Policies and Data Collection of Federal Web Sites", June 22, 2000 (http://www.whitehouse.gov/OMB/memoranda/m00-13.html)

L. OMB Memorandum M-99-18, "Privacy Policies on Federal Web Sites," June 2, 1999 (http://www.whitehouse.gov/omb/memoranda/m99-18.html)

M. EPA's Forms Management Policy, CIO Transmittal 06-004, Information Policy 2102 (http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2102.pdf)

N. EPA FOIA Manual, Directive 1550 (http://www.epa.gov/foia/reference.html)

O. Records Management, CIO Transmittal, 06-006, Information Policy 2161 (http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2161.pdf)

P. Records Management Manual, Directive 2160 (http://www.epa.gov/records/policy/2160/)

Q. Agency Network Security Policy, Directive 2195.1 A4 (http://intranet.epa.gov/rmpolicy/ads/orders/2195.1A4.pdf)

R. EPA Information Security Manual, Directive 2195A1 (http://intranet.epa.gov/rmpolicy/ads/manuals/Manual.PDF)

S. Federal Register Document Drafting Handbook (http://www.archives.gov/federal-register/write/handbook/ddh.pdf)

T. FIPS 201, Personal Identity Verification for Federal Employees and Contractors (http://csrc.nist.gov/publications/fips)

U. CIO Transmittal Number 06-012, EPA Order 2100.3A1, Policy on Limited Personal Use of Government Office Equipment (http://intranet.epa.gov/rmpolicy/ads/orders/2100.3A1.pdf)

V. CIO Transmittal 06-012, Information Policy 2191.0, Web Governance and Management Policy (http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2191.pdf)

W. EPA Order 2190.1A1, "Cookies" and Other User Tracking Methods/Waivers (http://intranet.epa.gov/rmpolicy/ads/orders/2190.1A1.pdf)

X. EPA Order 2190.2A1, Children's Privacy and Copyright Issues (http://intranet.epa.gov/rmpolicy/ads/orders/2190.2A1.pdf)

Y. EPA Order1900.1.A, Interacting With Contractors (http://intranet.epa.gov/rmpolicy/ads/orders/1900.1ACHG2.pdf)

Z. Contracts Management Manual, Chapter 3, Section 3.2, Agency's Relationship with Contractors (http://epawww.epa.gov/oamintra/policy/cmm.pdf)

AA. Environmental Protection Agency Acquisition Regulation (http://a257.g.akamaitech.net/7/257/2422/24nov20031845/edocket.access.gpo.gov/cfr_2002/octqtr/pdf/48cfr1524.104.pdf)

BB. Federal Acquisition Regulation
52.224-1 Privacy Act Notification
(http://farsite.hill.af.mil/vffara.htm)

CC. Federal Acquisition Regulation
52.224-2 Privacy Act
(http://farsite.hill.af.mil/vffara.htm)

8. ROLES AND RESPONSIBILITIES

A. The **EPA Administrator** has delegated authority to the Chief Information Officer, presently the Assistant Administrator for the Office of Environmental Information (OEI), to approve the establishment or amendment of an EPA Privacy Act system of records. (Delegation of Authority 1-84 Information Resources Management (http://intranet.epa.gov/rmpolicy/ads/dm/1-84_534.htm)

B. The **Assistant-Administrator for OEI and Chief Information Officer (CIO)** is the designated Senior Agency Official for Privacy in accordance with the E-Government Act; and has 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, such as the Privacy Act; and

1. designates the Privacy Act Officer; and
2. approves Agency level privacy policies, procedures, standards, and guidelines;
3. approves and signs systems of records notices for publication in the Federal Register;
4. approves the establishment or amendment of EPA Privacy Act systems of records according to the Administrator's delegation;

5. ensures that appropriate changes are made in a timely manner to privacy policies, procedures, standards, and guidelines based on the oversight results reported by the Office of Information Collection as well as updates from OMB, changes in regulations, changes in roles and responsibilities, etc.;
6. convenes the Data Integrity Board to carry out computer matching responsibilities pursuant to the Privacy Act;
7. ensures that accountability guidance which identifies positions/job types with key Privacy Program responsibilities and appropriate sample cascading goals and objectives that managers can use to establish accountability within their respective offices are developed and communicated;
8. ensures the Agency conducts periodic reviews to promptly identify deficiencies, weaknesses, or risks;
9. participates in assessing the impact of technology on the privacy of personal information; and
10. ensures that the Agency takes appropriate steps to remedy compliance issues identified.

C. The **Office of the General Counsel (OGC)**:

1. interprets the Privacy Act and other privacy-related regulations statutes, and requirements;
2. reviews related privacy notices, regulations and policy statements for legal form and substance;
3. decides on written appeals from initial denials of Privacy Act information to an individual, including denial of a request for correction or amendment of a record pursuant to the Privacy Act, 5 U.552a, has been delegated to OGC under EPA Delegation 1-33;
4. participates in computer matching programs as required; and
5. participates in Agency responses to breaches of PII, as appropriate.

D. The **Office of the Inspector General (OIG):**

1. carries out the appeal responsibilities related to decisions made on OIG Privacy Act records;
2. participates in computer matching programs as required; and
3. conducts criminal investigations related to a breach of sensitive PII or disclosure of PII if circumstances warrant such an investigation.

E. The **Office of Administration & Resources Management, (OARM)** ensures that:

1. ensures appropriate privacy related language is included in contracts, grants, and interagency agreements using the proper Federal Acquisition Regulations and Environmental Protection Agency Acquisition Regulations clauses related to privacy regulations and responsibilities; and
2. reviews and approves sample privacy cascading goals and objectives developed by OEI for managers to use to establish accountability within their respective offices included in accountability guidance developed by the National Privacy Program Manager.

F. The **Office of Public Affairs (OPA):**
   1. protects Privacy Act information by monitoring the content of EPA's public access Web site, EPA printed publications, and other EPA information media; and
   2. Participates in the response to breaches of PII as appropriate.

G. The **Office of Information Analysis and Access (OIAA)** in OEI is responsible for assisting the Office of Public Affairs (OPA) in protecting Privacy Act information by monitoring the content of the Web site.

H. The **Office of Technology Operations & Planning (OTOP)** in OEI :
   1. supports privacy policies through its planning, operational, training and oversight responsibilities for IT;
   2. assists in recommending and developing appropriate technical solutions to protect the privacy information collected or maintained within IT systems; and
   3. supports activities in response to breaches of PII.

I. The **Office of Information Collection (OIC)** in OEI is responsible for implementing the Privacy Program at EPA. In this capacity, OIC:
   1. establishes key goals and objectives associated with the Agency's Privacy Program;
   2. establishes and tracks performance measures associated with the key goals and activities associated with the Agency's Privacy Program and measures the progress of the Privacy Program;
   3. establishes performance measurement report(s) for tracking the Agency's Privacy Program progress;
   4. provides annual performance measurement reports showing the progress of the Agency's Privacy Program to the Senior Agency Official for Privacy and makes the reports available to the EPA offices and regions responsible for implementing the Privacy Program;
   5. reviews/approves Privacy Impact Assessments in accordance with Provisions of Section 208 of the E-Government Act of 2002;
   6. leads Agency efforts to protect PII used for Agency operations;
   7. performs oversight of the implementation of the Agency level privacy policies, procedures, standards, and guidelines within the Program and Regional Offices to ensure they are properly executed, consistently applied, and effective;
   8. reports the oversight results to the Senior Agency Official for Privacy, the Agency's Assistant and Regional Administrators and the Agency's Senior Information Officers;
   9. reports quarterly and annually on the implementation of the Privacy Act within the FISMA report;
   10. monitors the content of the Privacy Web site and EPA printed publications to ensure that non-public information about EPA employees is protected from public view; and
   11. manages the network of Liaison Privacy Officials.

J. The **National Privacy Program Manager** is the Agency's Privacy Act Officer who:

1. develops Agency level privacy policies, procedures, standards, and guidelines, as needed develops accountability guidance which identifies positions/job types with key Privacy Program responsibilities and appropriate sample cascading goals and objectives that managers can use to establish accountability within their respective offices;

2. provides overall privacy management and policy guidance;

3. provides oversight of system managers' activities to ensure all privacy-related, statutory, regulatory and EPA requirements are met;

4. implement changes in a timely manner to Agency level privacy policies, procedures, standards, and guidelines based on the results of National Privacy Program Manager's oversight of system managers' activities, the monitoring and oversight results reported by OIC, as well as updates from OMB, changes in regulations, changes in roles and responsibilities, etc.;

5. develops and implements response procedures to be followed in the event of a breach of sensitive PII;

6. coordinates privacy-related activities and responses to breaches of sensitive PII with Agency managers as appropriate;

7. publishes Federal Register notices for systems of records as required by the Privacy Act;

8. reviews privacy impact assessments as required by the E-Government Act;

9. establishes the network of Liaison Privacy Officials (LPOs);

10. develops and implements an annual privacy awareness training program;

11. advises and trains system managers and other EPA personnel on privacy requirements;

12. monitors EPA privacy activities, including quality and timeliness of responses to Privacy Act requests;

13. submits system of records notices for publication in the Federal Register; transmits letters to Congress and OMB;

14. compiles a biennial report on the computer matching activities of the Agency to submit to the OMB;

15. reports privacy data specified by OMB quarterly and annually on the FISMA Report to OMB; and

16. reviews and approves forms that collect sensitive PII prior to number issuance.

K. **Senior Information Official (SIO)** is responsible for:

1. oversight, coordination, and management of information technology utilized in fulfilling their organization's business needs and mission;
2. establishing appropriate policies and procedures within their respective offices to implement the Agency level policies, procedures, standards and guidelines;
3. monitoring and performing oversight of the implementation of the program or regional privacy policies and procedures to ensure they are properly executed, consistently applied, and effective;
4. making appropriate changes in a timely manner to program or regional privacy policies and procedures based on the monitoring and oversight results, and recommending changes to Agency level policies and procedures as appropriate;
5. ensuring that guidance which identifies positions/job types with key Privacy Program responsibilities along with appropriate sample cascading goals and objectives is applied within their respective offices;
6. designating the LPOs;
7. ensuring that a PIA has been completed prior to establishing a new or significantly modified collection of Privacy related information;
8. reviewing and making written determinations, concerning all requests to access sensitive PII from a remote location or take sensitive PII off site;
9. periodically reviewing existing databases containing sensitive PII to determine if data elements are still required;
10. ensuring compliance with federal regulations and Agency policies and procedures for protecting data in mobile devices used to transport or access PII.
11. maintaining a documented record of all approved remote access, transport of sensitive PII, downloads and/or local storage on a computer not located within EPA space;
12. ensuring all sensitive PII approved to be stored off site is erased within 90 days;
13. ensuring coordination with agency managers, including but not limited to Assistant Administrators, Chief Financial Officer, Chief Information Officer, Chief Technology Officer, Senior Agency Information Security Officer, Computer Security Incident Response Center, Office of Inspector General, Office of Public Affairs, and Office of General Counsel in response to a breach of sensitive PII.

L. **System Managers** in Program Offices and Regions apply privacy requirements, policies, procedures and guidance to Privacy Act systems of records and systems subject to the E-Gov Act and other privacy related systems. Specifically, system managers:

1. establish safeguards to ensure security and confidentiality;
2. authorize privacy documentation for new and/or revised systems;
3. terminate systems when no longer maintained in accordance with proper destruction/transfer procedures;
4. approve initial determinations on access to information;
5. account for access, amendments and disclosures;
6. recommend the designation of an LPO;
7. ensure that a Privacy Threshold Analysis is conducted for newly developed systems and/or systems that undergo substantial revisions; and
8. ensures completion of a PIA for any system that collects Privacy Act information.

M. **Liaison Privacy Officials (LPOs)** which are designated by the SIO**:**

1. administer the day-to-day activities and responsibilities of privacy in their specific program and regional areas;
2. ensure proper training for individuals in their area of responsibility, including monitoring on-line training for the employees; and
3. attend annual training for LPOs.

N. The **Freedom of Information Act (FOIA) national staff** acknowledges tracks and reports annually on Privacy Act access requests.

O. The **Data Integrity Board** is comprised of EPA's CIO, Principal Deputy General Counsel and Inspector General. The board reports annually to Congress and OMB on computer matching programs and provides guidance to EPA concerning computer matching.

P. **All individuals** who are defined by the audience of this policy must comply with the provisions of the Privacy Act and Agency Privacy Act regulations and must adhere to all Federal and Agency privacy statutes and requirements. Individuals are responsible for reporting incidents involving the security, loss, misuse or unauthorized disclosure of Privacy Act information and PII regardless of form or format in accordance with Agency incident reporting procedures.

9. DEFINITIONS

Agency. For the purposes of disclosing records subject to the Privacy Act among EPA components, EPA is considered a single Agency.

Computer Matching. Means any computerized comparison of **(A)** two or more automated systems of records or a system of records with non-federal records for the purpose of— **(I)** establishing or verifying the eligibility of (or continuing compliance with statutory and regulatory requirements by) applicants for cash or in-kind assistance or payments under federal benefit programs, or recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments or **(II)** recouping payments or delinquent debts under such federal benefit programs or **(B)** two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.

Individual. A citizen of the United States or an alien lawfully admitted to the United States whose name or other personal identifier is used to retrieve records from a system of records.

Maintain. Includes collect, use or disseminate.

Official Use. Managers and employees of an EPA component who use any record or the information contained therein to perform their official duties.

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual.

Privacy Act. Sets forth requirements for federal agencies when they collect, maintain or disseminate information about individuals.

Privacy Act Information. Data about an individual that is retrieved by name or other personal identifier assigned to the individual.

Privacy Impact Assessment. An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an

electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Threshold Analysis (PTA). A survey of questions that is prepared for all new systems and any other investment that undergoes substantial modifications. The PTA determines if the investment will be collecting any PII data elements and if a full Privacy Impact Assessment is required.

Record. In the context of the Privacy Policy, any item, collection or grouping of information about an individual maintained by an agency, e.g., the individual's education, financial transactions and medical, criminal or employment history; and that contains the individual's name, or any identifying number, symbol or particular assigned to the individual.

Risk-based Approach. An activity, mechanism, or methodology that is designed to provide "adequate security" (as defined in OMB Cir. A-130, Appendix III) for the affected IT and /or information resources. In the context of this policy, this applies principally to the security objective of confidentiality.

Routine Use. Any outside disclosure of Privacy Act information in which the use is compatible with the purpose for which the information was collected. Routine uses must be included in the published notice for the system of records involved.

Sensitive Personally Identifiable Information (PII). Social Security numbers, or comparable identification numbers; financial information associated with individuals; and medical information associated with individuals. Sensitive PII, a subset of PII, requires additional levels of security controls.

System of Records. A group of records under the control of an EPA component from which information is retrieved by the individual's name or some identifying number, symbol, or other identifying particular assigned to the individual. Notices for all Privacy Act systems of records must be published in the Federal Register.

System Manager – A Division Director or equivalent who is responsible for the implementation of the Privacy Act within their respective areas.

10. WAIVERS

Any request for a waiver to this policy must be submitted to the Chief Information Officer for determination.

11. RELATED PROCEDURES, STANDARDS AND GUIDANCE

In order for the Agency to comply with the Privacy Policy, the following procedures and guidance are provided:

- Privacy Act Manual (Directive 2190) – (http://www.epa.gov/privacy/policy/2190/index.htm)
- Privacy Impact Assessments - (http://www.epa.gov/privacy/assess/index.htm)
- System of Records Notice (SORN) - 5 USC 552a (e)(4)(A) - (I) (http://assembler.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html)
- Privacy Act statement (PAS) for forms used in the collection of personally identifiable information (PII) at 5 USC 552a (e)(3)(A) - (D) (http://assembler.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html)
- Guidance for Establishing Rules of Behavior (RoB) for Information Security Plans, November 6, 2003 (http://intranet.epa.gov/itsecurity/guidance/rob_ver_1_2_rev-20031106.pdf)

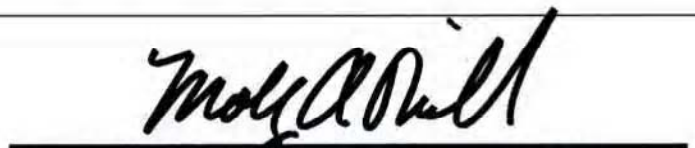
- CIO Policy Transmittal 06-11: Interim Policy and Procedures for Protecting Personally Identifiable Information – (http://intranet.epa.gov/oei/imitpolicy/qic/transmittal/transmittal-06-011.pdf)
- IT Security: Incident Reporting – (http://intranet.epa.gov/itsecurity/training/incidents.html)
- Agency Guidance on Incident Response Handling and Information Security Officer Handbook - (http://intranet.epa.gov/otop/security/CSIRC/CSIRC_Handbook.pdf)

12. MATERIAL SUPERSEDED

Information Resources Management (IRM) Policy Manual 2100, Chapter 11, Privacy

13. ADDITIONAL INFORMATION

For further information about this Policy, please contact the Records, FOIA and Privacy Branch in the Collection Strategies Division of the Office of Information Collection, Office of Environmental Information.



Molly A. O'Neill, Assistant Administrator
and Chief Information Officer
Office of Environmental Information