# U.S. Department of Energy
## Washington, D.C.

**ORDER**

**DOE O 206.1**

Approved: 1-16-09

**SUBJECT:** DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.

   b. Establish a Departmental training and awareness program for all DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for—

      (1) safeguarding Personally Identifiable Information (PII) and

      (2) complying with the Privacy Act.

   c. Provide Departmental oversight to ensure compliance with Federal statutes, regulations and Departmental Directives related to privacy.

2. CANCELLATION. DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*, dated 10-09-07, is canceled. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor requirement documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to all Departmental Elements, including those created after the Order is issued. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental Elements.)

      The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Order.

   b. DOE Contractors. Except for the exclusions in paragraph 3c, the CRD (Attachment 1) sets forth contractor requirements. The CRD will apply to the extent set forth in each contract.

   c. Exclusions. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511, and to

ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS. The following privacy requirements apply to all Departmental Elements.

a. Safeguarding Personally Identifiable Information (PII).

(1) OMB has defined PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

(2) Employees are required to prevent the unauthorized breach of PII.

(3) Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees must immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 (doecirc@doecirc.energy.gov) and through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*.

(4) Types of breaches that must be reported include, but are not limited to the following:

(a) loss of control of DOE employee information consisting of names and Social Security numbers,

(b) loss of control of Department credit card holder information,

(c) loss of control of PII pertaining to the public,

(d) loss of control of security information (e.g., logons, passwords, etc.),

(e) incorrect delivery of PII,

(f) theft of PII, and

(g) unauthorized access to PII stored on Department-operated web sites.

(5) Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the Chief Privacy Officer (CPO) is notified of all incidents involving the breach of PII within one hour of receiving notification.

(6) PII, regardless of whether it is in paper or electronic form, must be protected from unauthorized access or disclosure throughout its lifecycle.

(7) DOE employees shall limit the use of PII to only that information which is specifically needed to carry out their duties.

b. The Privacy Act.

(1) The Privacy Act governs a Federal agency's ability to maintain, collect, use, or disseminate a record about an individual.

(2) Any grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph is considered a record for the purposes of the Privacy Act.

(3) The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President.

(4) Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR).

(5) A SOR has the following two key distinctions:

(a) an indexing or retrieval capability built into the system and

(b) the Department retrieves records about individuals by reference to a personal identifier, such as the individual's name or Social Security number.

(6) The Privacy Act requires agencies to publish a System of Records Notice (SORN) in the Federal Register and report to Congress when a new SOR

is proposed or significant changes are made to a previously established system.

(7) Each SORN must contain the following information:

(a) name and location of the system;

(b) categories of individuals on whom records are maintained in the system;

(c) categories of records maintained in the system;

(d) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(e) policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(f) title and business address of the agency official who is responsible for SOR;

(g) agency procedures whereby an individual can be notified at the individual's request if the SOR contains a record pertaining to the individual; and

(h) agency procedures whereby an individual can be notified at the individual's request how he/she can gain access to any record pertaining to him/her contained in the SOR, and how he/she can contest its content; and categories of sources of records in the system.

(8) Under the Privacy Act, with limited exceptions, no agency or person shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

(9) For each SOR, DOE must not permit information collected about an individual for one purpose to be used for another purpose without giving notice to or getting the consent of the subject of the record and unless the record is being used subject to a routine use.

(10) Non-compliance with the Privacy Act carries **criminal and civil** penalties. An employee may be liable if he or she knowingly and willfully—

(a) obtains or requests records under false pretenses,

(b) discloses privacy data to any person not entitled to access, or

(c) maintains a "system of records" without meeting Federal Register notice requirements.

c. Recognizing differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, employees must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.

d. DOE employees must receive yearly training on privacy and data protection policies.

e. Privacy Impact Assessment. All unclassified information systems shall have a Privacy Impact Assessment (PIA) approved by the Senior Agency Official for Privacy (SAOP) or designated official. PIAs must be reviewed and updated at least annually (see Appendix A).

f. Collection and use of Social Security numbers. Collection and use of Social Security numbers not required by statute, regulation or an intended Departmental purpose shall be eliminated, in practice and in form, from DOE information systems and programs, whether in electronic or paper media.

g. Senior DOE Management, as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06, may add to these requirements for their own organizations, based on assessment of risk, so long as any additional direction is consistent with these requirements.

5. RESPONSIBILITIES.

a. Senior Agency Official for Privacy. Oversees, coordinates, and facilitates the Department's compliance with authorities governing privacy protection.

b. Director, Office of Information Resources. Appoints the Chief Privacy Officer.

c. Chief Privacy Officer.

(1) Manages the Department's Privacy Program.

(2) Reviews Department's PIAs.

(3) Advises and provides subject matter expertise to the Director, Office of Information Resources in the promulgation of guidance on privacy.

(4) Coordinates with the Chief Information Officer (CIO); the Chief Health, Safety and Security Officer; General Counsel (GC); and Heads of Departmental Elements to ensure compliance with the requirements of this Order.

d. Secretarial Officers/Heads of Departmental Elements.

(1) Have responsibility and accountability for ensuring the Departmental Elements' implementation of privacy protections in accordance with Federal laws, regulations, Departmental policies and Directives.

(2) Ensure completion of Privacy Impact Assessments (PIAs) of all unclassified information systems within their purview, including systems that only collect or maintain information about DOE employees and DOE contractors, in accordance with the requirements of this Order and all appendices.

(3) At a minimum, Departmental Elements must implement the following safeguards:

(a) Implement Cyber Security Controls outlined in DOE Directives and Office of the Chief Information Officer (OCIO) guidance for the protection of PII.

(b) Ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities.

(c) Ensure personnel minimize the collection of PII to only that which is required to conduct business operations necessary for the proper performance of a documented DOE function.

(d) Identify systems that process PII and ensure access is limited to only those individuals whose work requires access.

(e) Use sealable, opaque envelopes for mailing PII. Mark envelope to the person's attention.

(4) Post privacy policy statements on DOE websites in accordance with Federal law, regulations, and OMB directives.

(5) Appoint site Privacy Act Officers or points of contact for their Departmental Elements.

(6) Implement their Elements' plans to eliminate the unnecessary collection and use of Social Security numbers.

e. Chief Information Officer.

(1) Advises and provides cyber security and information technology subject matter expertise to the CPO to identify ways in which the Department can safeguard privacy information.

(2) Provides current threat information regarding the compromise of PII and information systems containing PII.

(3) Reports incidents involving breaches of PII to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives and ensures the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification.

f. Privacy Incident Response Team (PIRT).

(1) Convened by the SAOP.

(2) Responds to major incidents involving the breach of PII as determined by the SAOP.

(3) Conducts assessments of incidents involving breaches of privacy data, including evaluating the scope, degree of compromise, impact and risks resulting from the breach.

(4) Coordinates with the SAOP for internal and external agency notification including law enforcement.

g. Privacy Act Officers.

(1) Advocate and promote Privacy program activities within their Departmental Elements.

(2) Advise and provide Privacy Act subject matter expertise to their Departmental Elements, specifically with regard to conducting PIAs and completing the SORN process.

(3) Facilitate compliance reporting for their Departmental Elements.

(4) Manage the process for resolving privacy complaints for their Departmental Elements, including—

(a) documentation of factual circumstances surrounding unresolved complaints and

(b) notifying the CPO of unresolved written complaints.

h. Contracting Officers.

(1) Once notified by the affected Heads of Departmental Elements or their senior level designees regarding which contracts are subject to this Order, incorporate the CRD into affected contracts as directed.

(2) Ensure that contracting officers' representatives (CORs) and/or contracting officers' technical representatives (COTRs) are aware of provisions within this Order and any changes to their respective contracts.

(3) Ensure Privacy Act clauses contained in Federal Acquisition Regulations at 52.224-1 and 52.224-2 are included in all solicitations and in any awarded contracts.

i. DOE Employees.

(1) Are responsible for safeguarding PII and for reporting suspected or confirmed incidents involving the breach of PII, in printed or electronic form, in accordance with the requirements provided in Appendix B.

(2) Are responsible for complying with the Privacy Act.

j. System Owners.

(1) System Owners are Departmental Element officials responsible for monitoring the information systems under their purview to ensure compliance with this Order. System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s).

(2) System Owners must file a SORN, if applicable, and must complete the entire Federal Register review period before the system will be permitted to operate in the production environment.

(3) System Owners must submit documentation in support of a new or revised SOR or significant alteration to an existing SOR to the CPO. All privacy documentation must be in electronic format and submitted via e-mail to privacy@hq.doe.gov. The CPO, in consultation with General Counsel, will post a SORN in the Federal Register providing interested persons the opportunity to comment on the SOR.

(4) System Owners must submit documentation to the CPO in sufficient time for the CPO, in consultation with GC, to review prior to placing a SOR in operation.

(5) For each SOR a System Owner maintains, the System Owner must—

(a) Maintain only personal information considered relevant and necessary for the legally valid purpose for which it is obtained;

(b) Where possible, collect information directly from the individual;

(c) Prepare documentation for the publication of notice in the Federal Register, when a SOR is established or revised;

(d) Update SORNs prior to any significant change occurring to a System that affects the privacy information kept in the System;

(e) Maintain records with accuracy, relevance, timeliness, and completeness to ensure fairness to the individual of record;

(f) Employ appropriate security controls for the system to protect confidentiality, integrity, and available of records; and

(g) Require persons involved in the design, development, operation, or maintenance of any SOR, or in maintaining any record to sign a Rules of Behavior for each SOR to which they are granted access.

k. General Counsel.

(1) Provides legal review and concurrence before publishing any Departmental SORN in the Federal Register.

(2) Provides legal expertise to all DOE elements in interpreting and applying privacy issues including privacy law, compliance, and training.

6. REFERENCES.

a. Federal Laws and Regulations.

(1) Privacy Act of 1974, as amended at 5 U.S.C. §552a, P.L. 93-579.

(2) E-Government Act of 2002, P.L. 107-347.

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

(4) DOE Privacy Act Regulation, 10 CFR Part 1008.

(5) The Freedom of Information Act (FOIA), 5 U.S.C. §552.

(6) DOE Regulations Implementing the FOIA, 10 CFR Part 1004.

b. Office of Management and Budget Circulars and Memoranda.

(1) OMB Circular A-130, Management of Federal Information Resources.

(2) OMB Memorandum (M) 99-05, Privacy and Personal Information in Federal Records.

(3) OMB M-99-18, Privacy Policies on Federal Web Sites.

(4) OMB M-00-13, Privacy Policy and Data Collection on Federal Web Sites.

(5) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

(6) OMB M-05-08, Designation of Senior Officials for Privacy.

(7) OMB M-06-15, Safeguarding Personally Identifiable Information.

(8) OMB M-06-16, Protection of Sensitive Agency Information.

(9) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.

(10) OMB M-07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information.

c. Department of Energy Directives.

(1) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

(2) DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06.

(3) DOE N 221.14, *Reporting Fraud, Waste, and Abuse*, dated 12-20-07.

(4) DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 4-19-08.

(5) DOE O 221.2A, *Cooperation with the Office of Inspector General*, dated 2-25-08.

7. DEFINITIONS.

a. Accuracy. Ensuring, within sufficient tolerance for error, the quality of the record in terms of its use in making a determination.

b. Availability. Ensuring timely and reliable access to and use of information or an information system. For example, a loss of availability is the disruption of access to or use of information or an information system.

c. Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users—and for other than an authorized purpose—have access to or potential access to PII, whether in physical or electronic form.

d. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

e. Data Breach Analysis (for incidents involving the breach of PII). The process of assessing what, if any, Privacy information was compromised, the significance of such losses or intrusions, and how to prevent future occurrences.

f. Identity Theft. Per section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a), "a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation."

g. Information in Identifiable Form. Information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (2) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e. indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.

h. Information Technology (IT). As defined in the Clinger-Cohen Act, Pub. L. No. 104-106, IT refers to any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

i. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

j. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

k. Major Information System. An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

l. National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which—

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system;

(5) is critical to the direct fulfillment of military or intelligence missions, not including systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(6) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

m. Necessary. A threshold of need for an element of information greater than mere relevance and utility. A Federal agency should maintain in its records only such information about an individual as is relevant and reasonably necessary to ensure fairness to the individual and to accomplish a purpose of the agency that is required by statute or by Executive Order.

n. Personally Identifiable Information (PII). Any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

o. Personal Identifier. An identifier such as a Social Security number, fingerprint, name, etc. that uniquely identifies an individual.

p. Privacy Act Information. Information that is required to be protected under the Privacy Act of 1974.

q. Privacy Act Request. A request to an agency to gain access to an individual's record, such as by another Federal agency or law enforcement as required by statute; a request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system.

r. Privacy Impact Assessment (PIA). An analysis of how information is handled to—

(1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and

(3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

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

t. Relevance. A limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

u. Routine Use. With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

v. System of Records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

w. System of Records Notice (SORN). Notice published in the Federal Register prior to an agency's collection, maintenance, use or dissemination of information about an individual.

x. Timeliness. Sufficiently current to ensure that any determination based on the record will be complete, accurate and fair.

8. NECESSITY FINDING STATEMENT. In compliance with Sec. 3174 of P.L. 104-201 (50 U.S.C. 2584 note), DOE hereby finds that this Order is necessary for the fulfillment of current legal requirements and conduct of critical administrative functions.

9. CONTACT. Questions concerning this Order should be addressed to the Chief Privacy Officer (202) 586-0483.

BY ORDER OF THE SECRETARY OF ENERGY:

JEFFREY F. KUPFER
Acting Deputy Secretary

# APPENDIX A. PRIVACY IMPACT ASSESSMENTS

## Why are DOE organizations required to conduct PIAs?

The E-Government Act of 2002 requires Federal agencies to perform Privacy Impact Assessments (PIAs), an analysis of how information is handled, in order: (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.

The DOE PIA process helps to ensure privacy protections are considered and implemented throughout the system life cycle.

## Step 1 – The Privacy Needs Assessment

System Owners are required to complete the first step of the DOE PIA for all unclassified information systems including contractor systems operated for or on behalf of the agency. This first step of the DOE PIA process is the Privacy Needs Assessment (PNA). The PNA is designed to ensure privacy is addressed for all information systems in an efficient manner by asking four threshold questions:

1. Does the information system collect or maintain information about individuals?

2. Is the information in identifiable form?

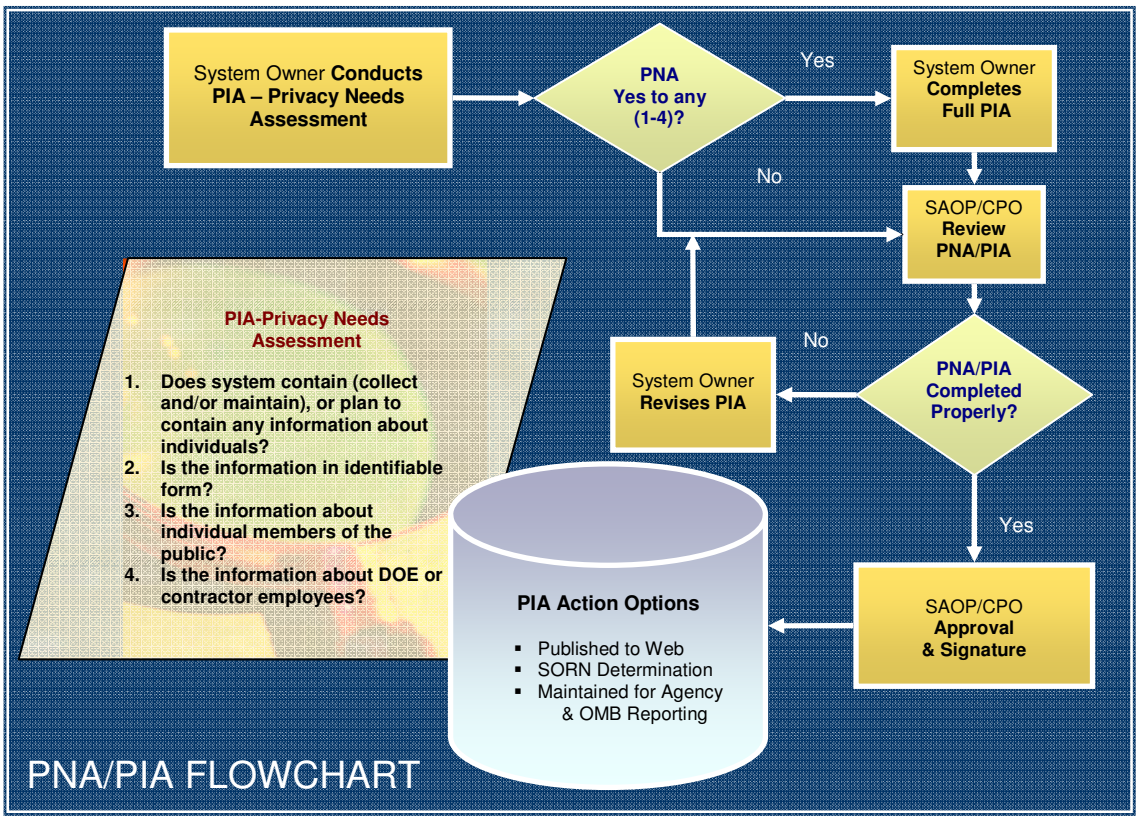
3. Is the information about individual members of the public?

4. Is the information about DOE or contractor employees?

If the answer to any of these questions is "Yes," System Owners must complete a full PIA.

**If the answer to <u>all</u> the threshold questions in the PNA is "No," no further sections of the PIA must be completed. The System Owner signs the PIA certifying to the CPO that the system does not contain PII.**

System Owners and their Privacy Act Officers must sign the PNA and submit the PNA to the DOE CPO. The PNA/PIA Flowchart illustrates this process.




If the answer to any of the questions in the PNA is "Yes" and a full PIA is required, the System Owner, in collaboration with the Privacy Act Officer must—

- Complete applicable elements of the PIA and
- Sign and submit the PIA to the CPO, copying the Head of the Departmental Element (HDE) staff.

If there are issues with the submitted PIA that need to be addressed, the CPO will coordinate with the System Owner to ensure there is an understanding of any deficiencies in the PIA so corrective action may be taken. The SAOP approves and signs the PIA. The CPO provides a signed copy of the PIA to the System Owner. PIAs affecting members of the public will be posted to the DOE Privacy Website in accordance with applicable laws and regulations. The System Owner may also be required to publish a System of Records Notice in the Federal Register.

**When to Conduct a Privacy Impact Assessment**

Privacy, like security, should be considered at all stages of the system's lifecycle. Departmental Elements must also consider the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect an individual's privacy. PIAs should be conducted as part of the certification and accreditation process. At a minimum, PIAs must be conducted when—

1. Designing, developing or procuring information systems or IT projects that collect, maintain or disseminate information in identifiable form.

2. Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons.

3. Significantly modifying an information system.

PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy. Examples of these changes include the following:

- **Conversions** - when converting paper-based records to electronic systems.

- **Anonymous to Non-Anonymous** - when functions applied to an existing information collection change anonymous information into information in identifiable form.

- **Significant System Management Changes** - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

- **Significant Merging** - when organizations adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

- **New Public Access** - when authentication technology (e.g., password, digital certificate, biometric) is newly applied to an information system accessed by members of the public.

- **Commercial Sources** - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources (merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement).

- **New Interagency Uses** - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA.

- **Internal Flow or Collection** - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

- **Alteration in Character of Data** - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

- **Changed Authorities or Business Processes -** when there are changes in information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

**Who Completes the Privacy Impact Assessment?**

The PIA is the System Owner's responsibility. The System Owner, system developer, data owners and the Privacy Act Officer must work together to complete the PIA.

System Owners must identify data that is collected and maintained in the information system, as well as individuals who will access that data. The Privacy Act Officer must assess whether there are any threats to privacy. PIAs require collaboration with program experts as well as experts in the areas of information technology, cyber security, records management and privacy.

**Privacy Impact Assessment Document Review and Approval Process**

The completed PIAs must be submitted to the CPO, copying the Heads of Departmental Elements' staff. The CPO submits the PIAs to the SAOP for approval and signature.

If the Chief Privacy Officer indicates corrective action is necessary for a PIA, the PIA will be returned to the System Owner. The System Owner is responsible for identifying and implementing corrective actions prior to resubmitting the PIA to the CPO.

# Steps for Completing the DOE Privacy Impact Assessment

| Step | Responsible Individual(s) | Actions |
|---|---|---|
| **1** | **System Owner** | **PIA Template**<br>Obtain current DOE PIA template from the Privacy Website. The System Owner has the overall responsibility and accountability for completing the PIA. Privacy should be considered at all stages of the system lifecycle. At a minimum, the PIA should be conducted as part of the certification and accreditation of the system and reviewed at least annually. |
| **2** | **System Owner**<br>**Privacy Act Officer** | **Complete PNA portion of the PIA**<br>A. If the answer to <u>all</u> questions on the PNA section of the PIA is "No," the System Owner and Privacy Act Officer must sign and submit the PNA to the CPO, copying the HDE staff. Upon receiving the approval of the SAOP, the PIA is now complete.<br>B. If the answer to <u>any</u> of the questions on PNA is "Yes," proceed to step 3. |
| **3** | **System Owner**<br>▪ Privacy Act Officer<br>▪ System Administrators<br>▪ Data Owners<br>▪ Program Managers<br>▪ Subject Matter Experts<br>▪ Information System Security Officer<br>▪ Security: Cyber & Physical Security<br>▪ Operations | **Conduct Full PIA**<br>Complete full PIA using DOE PIA template. The template is available from the Privacy Website, and may not be modified. System Owners and Privacy Act Officers must Sign the PIA. |
| **4** | **System Owner**<br>**DOE CPO**<br>**DOE CIO** | **Submit PIA to CPO**<br>System Owner submits PIA to CPO for review. The CPO may consult with subject matter experts and GC. If there are any issues with the PIA, the CPO will coordinate with the System Owner to ensure deficiencies are identified. The System Owner corrects deficiencies and resubmits the PIA. Depending on the scope and number of deficiencies, the System Owner may develop a plan of action and milestones for correcting the PIA. Once all deficiencies and concerns have been addressed, the System Owner resubmits the PIA to the DOE CPO. |
| **5** | **DOE CPO**<br>**SAOP** | **DOE CPO Submits to SAOP**<br>Having reviewed the PIA, the CPO submits the PIA to the SAOP for signature. |
| **6** | **SAOP**<br>**DOE CPO**<br>**System Owner** | **SAOP Signature and Approval**<br>The SAOP approves and signs the PIA. Copies of the signed PIA are maintained with the CPO and provided to the System |

| Step | Responsible Individual(s) | Actions |
|---|---|---|
| | | Owner for their records. The System Owner should maintain these records for conducting certification and accreditation and for preparing OMB Exhibits 300 and 53. |
| **7** | **SAOP**<br>**CPO**<br>**General Counsel**<br>**System Owner**<br>**Privacy Act Officer** | **System Requires Web Posting and Reporting**<br>If the PIA identifies the system as a system affecting members of the public in accordance with the E-Government Act, the following actions are taken:<br>▪ CPO posts the signed PIA affecting members of the public to the DOE Privacy website;<br>▪ Publishes System of Records Notice in the Federal Register, if applicable;<br>▪ Reports PIAs affecting members of the public to OMB.<br>NOTE: Not all PIAs require a SORN; therefore, there will not be a one-to-one (1:1) ratio of PIAs to SORNs. |
| **8** | **System Owner**<br>**Privacy Act Officer** | **Ongoing Monitoring**<br>The System Owner and local Privacy Act Officer will ensure the PIA is reviewed at least annually or whenever there is a change to the system that would impact the risk to privacy. If required, the PIA is updated. |

**Department of Energy**
**Privacy Impact Assessment Privacy Needs Assessment**

| **<SAMPLE ONLY>** | | |
|---|---|---|
| **Date** | | |
| **Departmental Element** | | |
| **Name of Information System or IT Project** | | |
| **Exhibit Project UID** | | |
| | Name, Title | Contact Information<br>Phone, Email |
| **System Owner** | | |
| **Privacy Act Officer** | | |
| **Purpose of Information System or IT Project** | | |
| **Type of Information Contained (Collected or Maintained)** Use NIST SP 800 60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance. | | |
| **Has there been any attempt to verify Information in Identifiable Form does not exist on the system (e.g., system scan)?** | | |
| **If "Yes," what method was used to verify the system did not contain Information in Identifiable Form?** | | |

| **Threshold Questions** | |
|---|---|
| **1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?** | |
| **2. Is the information in identifiable form?** | |
| **3. Is the information about individual members of the public?** | |
| **4. Is the information about DOE or contractor employees?** | |
| If the answer to the **all** four (4) key threshold questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO. | |

# APPENDIX B. RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION

The purpose of this appendix is to define notification requirements and procedures for incidents involving breaches of PII.

**REQUIREMENTS**.

**Identifying and Reporting Incidents Involving Breaches of PII**

1. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees will immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 (doecirc@doecirc.energy.gov) and through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in to DOE O 205.1A, *Department of Energy Cyber Security Management*.

2. Types of breaches that must be reported include, but are not limited to the following:

   a. loss of control of DOE employee information consisting of names and Social Security numbers;

   b. loss of control of Department credit card holder information;

   c. loss of control of PII pertaining to the public;

   d. loss of control of security information (e.g., logons, passwords, etc.);

   e. incorrect delivery of sensitive PII;

   f. theft of PII; and

   g. unauthorized access to PII stored on Department operated web sites.

3. Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification.

4. Additionally, the Senior Agency Official for Privacy may convene the Privacy Incident Response Team (PIRT) chaired by the Senior Agency Official for Privacy, and comprised of senior-level representatives from the Offices of the Chief Information Officer; Public Affairs; General Counsel; Office of Management; Office of Health, Safety and Security; National Nuclear Security Administration; and the DOE Program Offices impacted by a PII breach when the PII breach is significant, crosses DOE organizational boundaries, or as needed. The PIRT will coordinate with the Office of

Inspector General (IG) to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation

The following considerations will apply in determining the impact of a PII breach resulting in lost, stolen or improperly accessed data:

a. the nature and content of the data (e.g., the data elements involved, such as name, Social Security number and/or date of birth, etc.);

b. the ability of an unauthorized party to use the data, either by itself or in conjunction with other data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects;

c. ease of logical data access to the data given the degree of protection for the data (e.g., unencrypted, plain text, etc.);

d. ease of physical access to the data (e.g., the degree to which the data is readily available to unauthorized access);

e. evidence indicating that the data may have been the target of unlawful acquisition;

f. evidence that the same or similar data had been acquired from other sources improperly and used for identity theft;

g. whether notification to affected individuals through the most expeditious means available is warranted; and

h. whether further review and identification of systematic vulnerabilities or weaknesses and preventive measures are warranted.

5. Upon conclusion of any risk analysis by the party leading the investigative effort (i.e. respective Under Secretary, his or her designees, or the PIRT), if there is a finding of reasonable risk for potential misuse of any PII involved, that information along with any supporting material will be shared with both the Senior Agency Official for Privacy and the Chief Information Officer.

6. If the Senior Agency Official for Privacy and the Chief Information Officer concur that the data breach does not pose a reasonable risk of harm, the Department will take no further action.

7. Conversely, if there is no concurrence, both parties will present their views to the Deputy Secretary, who will then decide what, if any, further action is necessary.

8. The Senior Agency Official for Privacy may provide notice to subjects of a data breach and/or offer them Credit Protection Services prior to the completion of any risk analysis. This decision will likely hinge upon the information available to the Department at the

time of the data breach, and whether the information suggests there is an immediate and substantial risk of identity theft or other harm.

9. The Head of the Departmental Element in which the breach occurred will provide notification to the affected individuals once there is a finding by the PIRT that a reasonable risk exists for potential misuse of any sensitive personal information involved in the data breach. The notification will be signed, and include the following elements as appropriate:

    a. a brief description of what happened, including the dates of the data breach and of its discovery, if known;

    b. to the extent possible, a description of the personnel information that was involved (e.g., full name, Social Security number, date of birth, home address, account numbers, etc.);

    c. a brief description of actions taken by the Department to investigate, mitigate losses and protect against any further breach of data;

    d. contact procedures to ask further questions or learn additional information, including a toll-free telephone number, email address, web site, and/or postal address;

    e. steps that individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts, if appropriate, and instructions for obtaining other credit protection services (NOTE: Alerts may include key changes to fraud reports and on-demand personal access to credit reports and scores); and

    f. a statement of whether the information was encrypted or protected by other means, when it is determined such information would be beneficial and would not compromise the security of any Departmental systems.

10. When there is insufficient or inaccurate contact information that precludes written notification to an affected individual, an alternative form of written notice may be provided.

    a. This alternative notice may include a conspicuous posting on the home page of the Department's web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals are likely to reside.

    b. The media notice will include a toll-free telephone number for an individual to contact in order to learn whether or not his/her personal information is possibly included in the data breach.

11. When the SAOP determines that urgent action is required because of possible imminent misuse of PII, the SAOP may provide information to affected individuals by telephone or other means, as appropriate.

12. Notwithstanding the foregoing requirements, notification may be delayed upon lawful requests to protect data or computer resources from further compromise or to prevent interference with the conduct of lawful investigation, national security, or efforts to recover data.

    a. A lawful request should be made in writing to the Secretary of Energy or SAOP by the Federal agency responsible for the investigation regarding security concerns or data recovery efforts that may be adversely affected by providing notification.

    b. The SAOP must be notified of a delay notification request.

    c. Any lawful request for delay in notification must state an estimated timeframe after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover data.

    d. Any delay should not increase risk or harm to any affected individuals.

    e. The Secretary or other Agency official designated by the Secretary will keep the Senior Agency Official for Privacy and the Chief Information Officer informed on the status of any investigation or recovery efforts.

13. Individuals who routinely access PII and their supervisors must sign a document annually describing their responsibilities and the consequences for failure to protect PII.

14. Departmental Elements and their sites should maintain a log which tracks all activities—including dates and times of events, decisions and corrective actions—for incidents involving breaches of PII.

15. The Departmental Element program responsible for the breach of PII shall incur and be responsible for all costs associated with remediation including notification of affected or potentially-affected individuals.

**CONTRACTOR REQUIREMENTS DOCUMENT**
**DOE O 206.1, *DEPARTMENT OF ENERGY PRIVACY PROGRAM***

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) site/facility management contractors whose contracts involve the design, development or operation of a Privacy Act System of Record. In addition, the Personally Identifiable Information (PII) requirements in this CRD apply to any site management contractor that handles PII.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's or subcontractor's compliance with the requirements.

1. GENERAL REQUIREMENTS.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, and take appropriate actions to assist DOE in complying with Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.

   b. Ensure that contractor employees are aware of their responsibility for—

      (1) safeguarding Personally Identifiable Information (PII) and

      (2) complying with the Privacy Act.

2. SPECIFIC REQUIREMENTS. The contractor must do the following:

   a. Ensure contractor employees are made aware of their roles and responsibilities for reporting suspected or confirmed incidents involving the breach of PII.

   b. Ensure contractor employees are cognizant of the following DOE Privacy Rules of Conduct. At a minimum, ensure contractor employees—

      (1) are trained in their responsibilities regarding the safeguarding of PII;

      (2) do not disclose any PII contained in any SOR except as authorized;

      (3) report any known or suspected loss of control or unauthorized disclosure of PII;

      (4) observe the requirements of DOE directives concerning marking and safeguarding sensitive information, including, when applicable, DOE O 471.3, *Protecting and Identifying Official Use Only Information*;

(5) collect only the minimum PII necessary for the proper performance of a documented agency function;

(6) do not place PII on shared drives, intranets or websites without permission of the System Owner; and

(7) challenge anyone who asks to see the PII for which they are responsible.

c. Ensure that contractor employees complete the Annual Privacy Training and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.

d. Ensure contractor employees are cognizant of the fact that all personal information collected, maintained, used, or disseminated on behalf of the Agency must be maintained in a Privacy Act SOR.

e. Ensure that contractor employees recognize differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, contractors must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.

f. Ensure contractor employees are cognizant of the fact that non-compliance with the Privacy Act carries criminal and civil penalties.