



PRIVACY IMPACT ASSESSMENT: **ORG NAME – SYSTEM NAME**
 PIA Template Version 3 – May, 2009

Affects Members Of the Public?	Mark if Applicable w/ an X
--------------------------------------	----------------------------------

Department of Energy
 Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, *Department of Energy Privacy Program*, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: <http://www.directives.doe.gov/pdfs/doe/doetext/newword/206/o2061.pdf>

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	Date the assessment was completed.	
Departmental Element & Site	The official list of Departmental Elements can be accessed at https://www.directives.doe.gov/references/DOEDepartmentalElements.pdf Please also list the site location of the system with as much specificity as possible (e.g. DOE Headquarters, Forrestal, 1G-053 server room).	
Name of Information System or IT Project	Enter the name of the information system. If the system is part of an enclave or general support system (GSS), please include the name of the enclave or GSS along with the name identifying the application or subsystem being assessed.	
Exhibit Project UID	Enter the project unique identifier used for capital planning (eCPIC) or the contract name that provides the funding for the system.	
New PIA <input type="checkbox"/>	Please indicate whether this is a new PIA or an update to an existing PIA. List the name of the PIA being updated.	
Update <input type="checkbox"/>		
Name, Title		Contact Information Phone, Email
System Owner	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). System	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

	owners may be Federal or contractor employees.	
Local Privacy Act Officer	Privacy Act Officers or Privacy Points of Contact (PPoCs) are designated by the Head of the Departmental Element. PAOs and PPoCs advocate and promote Privacy program activities within their Departmental Elements, as well as advise and provide Privacy Act subject matter expertise to their Departmental Elements, specifically with regard to conducting PIAs and completing the SORN process.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	System Owners must engage cyber security experts to review this PIA prior to submission to the Privacy Office. Each organization may have these responsibilities assigned a little differently (i.e. Information System Security Officer (ISSO) or other cyber security professional).	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Person Completing this Document	Name and title of the person(s) completing this document.	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
Purpose of Information System or IT Project	Describe the purpose of this system, specifically as it relates to the organization's mission. For example, "The Acuity system is used by DOE Headquarters to process employee payroll for Federal employees." Please provide a sufficient level of detail to cover all purposes of the system. This information is included when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act Systems of Records. It also is included in the Privacy Act Systems of Records Notice (SORN) published in the Federal Register. If the system has a SORN, the response to this question should reflect the information in the narrative and notice.	



MODULE I – PRIVACY NEEDS ASSESSMENT

Type of Information Collected or Maintained by the System:	<input type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input type="checkbox"/> Financial Information e.g. credit card number <input type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DoB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input type="checkbox"/> Name, Phone, Address <input type="checkbox"/> Other – Please Specify
Has there been any attempt to verify PII does not exist on the system? <i>DOE Order 206.1, Department of Energy Privacy Program, defines 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.</i>	YES or NO Some systems employ software tools to scan content (information or data) to search for types of data such as Social Security numbers.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Tools, processes, types of information is scanned for, and frequency of the scanning.
Threshold Questions	
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES or NO
2. Is the information in identifiable form?	YES or NO
3. Is the information about individual Members of the Public?	YES or NO



MODULE I – PRIVACY NEEDS ASSESSMENT

(If “Yes,” place an “X” in the box at the top of first page.)

Member of the Public refers to individuals in a non-employee or DOE contractor context. *Members of the Public* includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE

YES or NO (If Yes, select with an “X” in the boxes below)

4. Is the information about DOE or contractor employees?

- Federal Employees
- Contractor Employees

If the answer to **all** four (4) Threshold Questions is “No,” you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is “Yes.” All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner’s best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT



MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>What statute, regulation, Executive Order or Departmental authority authorizes the collection and maintenance of personal information to meet an official program mission or goal?</p> <p>As provided in DOE O 206.1, "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."</p>
<p>2. CONSENT</p> <p>What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?</p>	<p>Describe mechanisms and/or processes available for the individual to accept or decline the personal information being provided and if there are any penalties if the information is not provided.</p>
<p>3. CONTRACTS</p> <p>Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>Answering this question typically requires checking with the local Contracting Officer to ensure the DOE Privacy Order Contractor Requirements Document was incorporated in the contract.</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>Please describe how the use of this system and its technologies may impact an individual's privacy.</p> <p>Consider also the use of emerging technologies and how those technologies may impact privacy.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>A system with data on individuals that is retrieved by a name or personal identifier may constitute a Privacy Act System of Records and require a Notice (or an amended notice) be published in the <i>Federal Register</i>.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>The Privacy Act requires publication of a notice in the Federal Register describing each System of Records subject to the Act. Any officer or employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a (e)(4)) is guilty of a misdemeanor and may be fined up to \$5,000.</p> <p>If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act System of Records. Organizations must consult with their local Privacy Act Officer and/or General Counsel as appropriate to make this determination.</p> <p>Systems of Record must comply with all data management practices described in the SORN.</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>YES, NO, N/A</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>For example: individual-provided; other Federal agency; tribal, state or local government entity; named third party, other (please identify). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g. informant, an internet service provider, a neighbor or friend, etc.).</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>What is meant by derived and aggregation? All enhanced or modernized systems most likely will derive new data and create previously unavailable data about an individual from the information collected through aggregation.</p> <p>Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.</p> <p>Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data.</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Is there a document that describes the data elements? For example: a database schema that describes the elements and shows the data relationships?</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>Describe how the information will be used by the Department.</p>
<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>Describe the use of the new or meta data.</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>Name of the Federal agency; tribal, state or local government entity; named third party.</p>
<p>Reports</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>For example, employee time and expense history.</p>



MODULE II – PII SYSTEMS & PROJECTS

15. What will be the use of these reports?	For example, the employee time and expense history may be used by the human resources department to manage payroll and reimbursement of expenses.
16. Who will have access to these reports?	<u>List Roles Only</u> of individuals who will have access to the reports. Point to current access control list(s) (include version), but <u>Please Do Not List Names Here</u> . Include other agencies and governmental organizations.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	Indicate whether tools and/or methods are used to track or monitor individuals.
18. What kinds of information are collected as a function of the monitoring of individuals?	Identify types of information collected. For example, Social Security numbers.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Please refer to these controls at a high level.

DATA MANAGEMENT & MAINTENANCE



MODULE II – PII SYSTEMS & PROJECTS

<p>20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.</p>	<p>The Privacy Act of 1974 requires that each agency that maintains a System of Records “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” (5 U.S.C. 552a (e)(5)). If the data does not meet any one of these components, fairness in making any determination is compromised.</p> <p>The information must have some form of verification for accuracy because of the Privacy Act provision that requires that only relevant and accurate records should be collected and maintained about individuals. Data accuracy and reliability are important requirements in implementing the Privacy Act.</p> <p>Data must also be complete before that the data is deemed accurate. Therefore, this section should state the steps the agency has taken to ensure the data is complete.</p> <p>If the system derives meta data, how will this be maintained, including verified for relevance completeness, and accuracy?</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>System Owners and information owners are responsible for ensuring information is used and managed consistently for its stated purpose in support of the organization. Please describe processes, procedures, software tools, etc. that are used to support this goal.</p>
<p>Retention & Disposition</p>	
<p>22. What are the retention periods of data in the information system?</p>	<p>Please contact your organization’s records manager to determine the appropriate response.</p>
<p>23. What are the procedures for disposition of the data at the end of the retention period?</p>	<p>Please contact your organization’s records manager to determine the appropriate response.</p>

ACCESS, SAFEGUARDS & SECURITY



MODULE II – PII SYSTEMS & PROJECTS

24. What controls are in place to protect the data from unauthorized access, modification or use?	Please refer to your organization’s implementation of DOE Cyber Security Directives and Senior DOE Management Program Cyber Security Plans (PCSP). For example: "The System Owner has implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system was certified and accredited (provide date(s)) and found to have mitigated risk to an acceptable level."
25. Who will have access to PII data?	<u>List Roles Only</u> of individuals who will have access to the PII data. Point to current access control list(s) (with version), but <u>Please Do Not List Names Here.</u>
26. How is access to PII data determined?	For example, will users have access to all data on the information system or will the user’s access be restricted?
27. Do other information systems share data or have access to the data in the system? If yes, explain.	Many information systems interconnect and share data. Please identify all systems that connect to and access information on this system.
28. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?	Interconnection Security Agreements (ISA) outline the responsibilities and expectations associated with system interconnection. ISAs specify security requirements and controls necessary for interconnection and compliance.
29. Who is responsible for ensuring the authorized use of personal information?	<u>List Roles Only</u> of individuals who are responsible for ensuring the authorized use of personal information. Point to current access control list(s) (with version), but <u>Please Do Not List Names Here.</u>

END OF MODULE II



SIGNATURE PAGE

	Signature	Date
System Owner	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Local Privacy Act Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
<i>Jerry Hanley</i> Chief Privacy Officer	<hr/>	<hr/>
	<hr/>	<hr/>