



PRIVACY IMPACT ASSESSMENT TRAINING



Transformation
through Partnerships

Department of Energy
2012 Information Management Conference

Jerry Hanley
Chief Privacy Officer

- Background
- What is a PIA?
 - Who? When? Why?
- PIA Process Overview
- Guidelines
- Completing the PIA
 - Module I – PNA
 - Module II – PII Systems & Projects
 - Signature & Submission

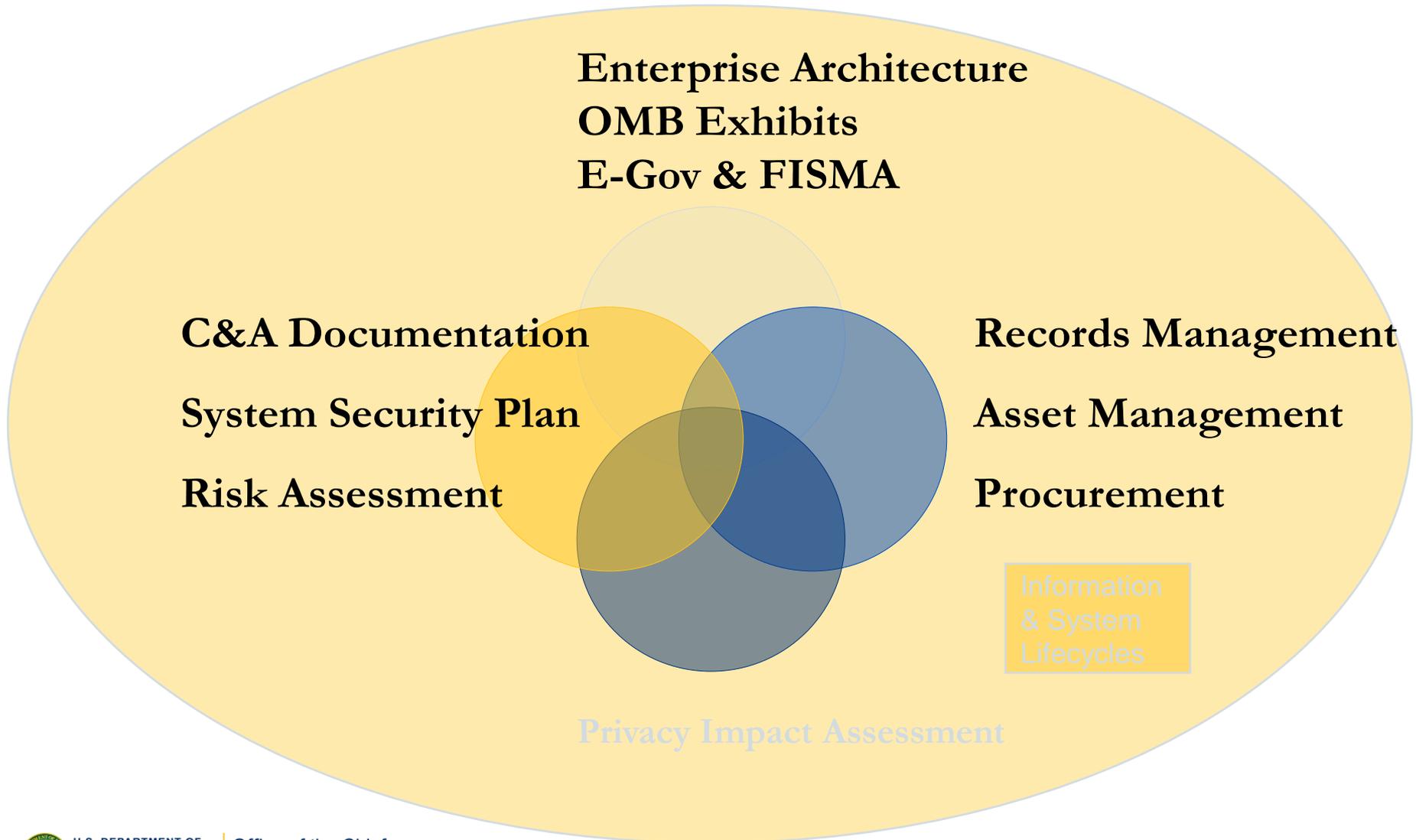
Legislative and Executive Branch Drivers

- Privacy Act of 1974
- E-Government Act, Sec. 208
- OMB Memoranda

DOE O 206.1, Department of Energy Privacy Program

4. e. “All unclassified information systems shall have a Privacy Impact Assessment (PIA)

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. (OMB M-03-22)

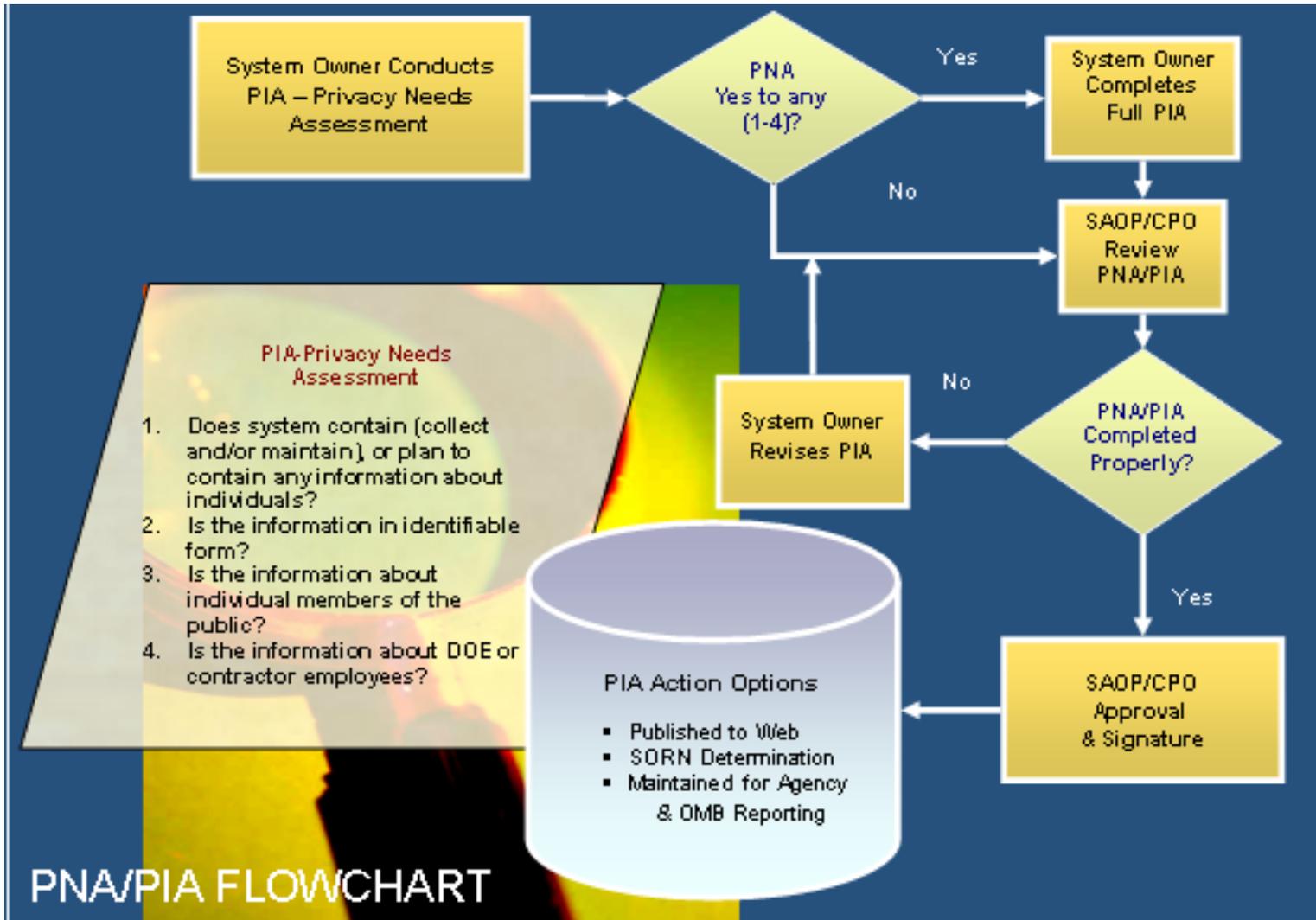


- **Lifecycle Approach**
- **Risk-based Approach**
- **Context is Key** – If DOE is collecting PII as part of its mission, it is required to safeguard and maintain accurate information.
- **Report Breaches Immediately** – Whether suspected or confirmed.

1. Designing or procuring IT systems
2. Initiating a new electronic collection of information in identifiable form
3. Significant modification of an existing information system.
4. Prior to using a social media third-party website or application

The PIA is the System Owner's responsibility. Collaboration is Key.

- The System Owner must work with the system developers (for new systems), data owners, and the Privacy Act Officer to complete the PIA.
- PIAs require collaboration with program experts as well as experts in the areas of information technology, cyber security, legal, records management, procurement and asset management.



1. Submit Completed PIAs to CPO
 - Copy relevant program staff
2. CPO Works with System Owner to address issues
3. CPO Coordinates Review, Approval and Posting of PIAs

- **Please Do Not Modify the PIA Template**
- Answer all questions and **remove guidance text from template**
- Organizations may add content to the PIA for their internal use only.
- Date and obtain System Owner signature before submitting to the CPO .

Please Do Not Disclose Sensitive Information

- Refer to other security documents, such as the System Security Plan.
- Use version numbers & maintain local copies of all supporting documentation.

Please Complete the PIA Electronically

- Please do not submit completed PIAs that have been hand written.

System Owners are required to complete this 1st step of the DOE PIA.



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

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/doi/doetext/neword/206%2061.pdf>

Please complete electronically; 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 www.directives.doe.gov/pdfs/reftools/org-list.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 (eCPIIC) or the contact 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"/>							
	<table border="1"> <thead> <tr> <th>Name, Title</th> <th>Contact Information Phone, Email</th> </tr> </thead> <tbody> <tr> <td>System Owner</td> <td>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 owners may be Federal or contractor</td> </tr> <tr> <td></td> <td>Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov</td> </tr> </tbody> </table>	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 owners may be Federal or contractor		Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov
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 owners may be Federal or contractor						
	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov						

PRIVACY PROGRAM 1



Write in plain language at a high level so PIAs are easily understood by the public.



- See Guidance on *Defining Information Systems*

- Unique ID (UID)

MODULE I – PRIVACY NEEDS ASSESSMENT		
Date	Date the assessment was completed.	
Departmental Element & Site	The official list of Departmental Elements can be accessed at www.directives.doe.gov/pdfs/reftools/org-list.pdf . Please also list the site location of (e.g. DOE Headquarters, Forresta	
Name of Information System or IT Project	Enter the name of the information general support system (GSS), pl with the name identifying the appl	
Exhibit Project UID	Enter the project unique identifier name that provides the funding fo	
New PIA <input type="checkbox"/>	Please indicate whether this is a n 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 system under their purview to ensure compliance with this Order. System Owners are responsible for the overall management, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s). System owners may be Federal or contractor	Use the full phone number and email. For example (202) 555-1212 John.doe@hq.doe.gov

System Owner has Ultimate Responsibility!

- Indicate all Information types.
- Applicability of any software tools, such as Data Leak Prevention or Redaction technologies?

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? <small>DOE Order 208.1, 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.</small>	<p>YES or NO</p> <p>Some systems employ software tools to scan content (information or data) to search for types of data such as Social Security numbers.</p>
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	<p>Tools, processes, types of information is scanned for, and frequency of the scanning.</p>

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?

The PNA is designed to ensure privacy is addressed for all information systems in an efficient manner by asking four threshold questions.

If the answer to ALL Threshold Questions is “No,” proceed to the signature page.

Submit the completed PNA (Module I) with signature page to the CPO.

SIGNATURE PAGE		
	Signature	Date
System Owner	<hr/> (Print Name) <hr/> (Signature)	<hr/>
Local Privacy Act Officer	<hr/> (Print Name) <hr/> (Signature)	<hr/>
<i>Jerry Hanley</i> Chief Privacy Officer	<hr/>	<hr/>
<i>Ingrid Kolb</i> Senior Agency Official for Privacy (SAOP)	<hr/>	<hr/>

The PNA helps to efficiently determine whether additional assessment is necessary. If there is doubt, complete Module II.

Module II - PII Systems &

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.



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

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	
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>

✓ You must reference an Authority.
Consent is preferred, but not always required.

3. CONTRACTS

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?

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.

4. IMPACT ANALYSIS:

How does this project or information system impact privacy?

Please describe how the use of this system and its technologies may impact an individual's privacy.

Consider also the use of emerging technologies and how those technologies may impact privacy.

DOE's mission is primarily fulfilled by contractors.
Impact Analysis is the heart of the PIA.

NOTICE

- What is a SORN?
- Must I reference a SORN?

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 <i>Federal Register</i> 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>

DATA SOURCES & DATA USE

- Where does the PII come from?
- Who and How will it be used?

MODULE II – PII SYSTEMS & PROJECTS	
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	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.). Will this system derive, "tag" or markup the data (e.g. via HTML or XML), or aggregate data from multiple sources to create new data about individuals?
9. Are the data elements described in detail and documented?	Is there a document that describes the data elements? For example: a database schema that describes the elements and shows the data relationships?
DATA USE	
10. How will the PII be used?	Describe how the information will be used by the Department.
11. With what other agencies or entities will an individual's information be shared?	Name of the Federal agency; tribal, state or local government entity; named third party.
Reports	
12. What kinds of reports are produced about individuals or contain an individual's data?	For example, employee time and expense history.
13. 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.
14. 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 Please Do Not List Names Here . Include other agencies and governmental organizations.

DATA USE Monitoring

- Health
- Legal
- Investigation

MODULE II – PII SYSTEMS & PROJECTS	
Monitoring	
15. 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.
16. What kinds of information are collected as a function of the monitoring of individuals?	Identify types of information collected. For example, Social Security numbers.
17. Are controls implemented to prevent unauthorized monitoring of individuals?	Please refer to these controls at a high level.

MANAGEMENT & MAINTENANCE

- Accuracy
- Relevance
- Completeness
- Minimization
- Retention
- Disposition

DATA MANAGEMENT & MAINTENANCE	
<p>18. 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 new data about individuals, how will this data be maintained, including verified for relevance completeness, and accuracy?</p>
<p>19. 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>
Retention & Disposition	
<p>20. What are the retention periods of data in the information system?</p>	<p>Please describe policies, processes and procedures (if any) for retaining data in the system.</p>
<p>21. What are the procedures for disposition of the data at the end of the retention period?</p>	<p>Please describe policies, processes and procedures (if any) for destroying data in the system, including paper reports, artifacts and other media that contain data which has reached the end of its retention period.</p>

ACCESS, SAFEGUARDS & SECURITY

- Security Enables Privacy
- Use High-level Language
- Refer to Security Plans: include dates & versions

ACCESS, SAFEGUARDS & SECURITY	
22. 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."
23. 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 Please Do Not List Names Here .
24. 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?
25. 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.
26. 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.
27. 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 Please Do Not List Names Here .
END OF MODULE II	

May Submit PIA
Electronically
or by Mail

Process Times

PRIVACY IMPACT ASSESSMENT: **ORG NAME - SYSTEMNAME**
PIA Template Version 3 - May, 2009

SIGNATURE PAGE		
	Signature	Date
System Owner	_____ (Print Name) _____ (Signature)	_____
Local Privacy Act Officer	_____ (Print Name) _____ (Signature)	_____
Jerry Hanley Chief Privacy Officer	_____	_____
Ingrid Kolb Senior Agency Official for Privacy (SAOP)	_____	_____

PRIVACY PROGRAM 11

Jerry Hanley
Chief Privacy Officer
U.S. Department of Energy

(202) 586-0483

privacy@hq.doe.gov

DOE Privacy Website:

From energy.gov click on Privacy Program at bottom of the DOE homepage.

Employee Orientation

Guide to Privacy

We Are All Privacy Stakeholders

Privacy is an Essential Trust Shared by the American People

PRIVACY PROGRAM

U.S. Department of Energy
Chief Privacy Officer

What Every Employee Needs to Know About Safeguarding Privacy

Identity theft harms millions of Americans every year. Breaches of personally identifiable information (PII) across the government have been well publicized and costly for individuals and Federal agencies. These breaches have prompted the Administration and Congress to take action to improve the protection of personal information.

As Department of Energy employees and contractors, you have a responsibility to protect all PII. PII includes Social Security numbers, personal financial information and health information, clearance information and other information that uniquely identifies individuals.

Privacy Act

The Privacy Act of 1974 (5 U.S.C. 552a) establishes controls over what personal information is collected and maintained by the Executive Branch and how that information is used.

The Privacy Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.

All DOE employees and contractors are subject to the Privacy Act and must comply with its provisions. Non-compliance with the Privacy Act carries criminal and civil penalties.