



PRIVACY IMPACT ASSESSMENT: INL INGS2009
PIA Template Version 3 – May, 2009

Affects Members Of the Public?	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/neword/206/o2061.pdf>

Please complete electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	June 16, 2009	
Departmental Element & Site	Idaho National Laboratory	
Name of Information System or IT Project	10th International Nuclear Graphite Specialists Meeting registration web site.	
Exhibit Project UID	Enterprise Architecture Application ID - 223419	
New PIA <input type="checkbox"/>	DOE PIA -.doc	
Update <input checked="" type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Matt Stoddard DBA/Developer	208-526-2453 Matt.stoddard@inl.gov
Local Privacy Act Officer	Dale Clafin	208-526-1199 Dale.Clafin@inl.gov
Cyber Security Expert reviewing this document (e.g. ISSM,	Daniel Jones Technical Lead, Cyber Security	208-526-6477 Daniel.Jones@inl.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

CSSM, ISSO, etc.)		
Person Completing this Document	Matt Stoddard DBA/Developer	208-526-2453 Matt.stoddard@inl.gov
Purpose of Information System or IT Project	<p>This registration site is used for gathering registration data for the activity.</p> <p>In order to communicate with registrants, certain information is requested by the registration site including the registrant's name, address, phone number and email, and their affiliation. If they are not a U.S. citizen, additional specific information is collected so that a security plan can be created to allow on-site visiting.</p>	
Type of Information Collected or Maintained by the System:	<p><input checked="" type="checkbox"/> SSN – If a person does not have a DOE badge and they are a U.S. citizen they input a social security number</p> <p><input checked="" type="checkbox"/> Medical & Health Information</p> <p><input type="checkbox"/> Financial Information</p> <p><input type="checkbox"/> Clearance Information</p> <p><input type="checkbox"/> Biometric Information</p> <p><input type="checkbox"/> Mother's Maiden Name</p> <p><input checked="" type="checkbox"/> DoB, Place of Birth</p> <p><input checked="" type="checkbox"/> Employment Information</p> <p><input type="checkbox"/> Criminal History</p> <p><input checked="" type="checkbox"/> Name, Phone, Address</p> <p><input checked="" type="checkbox"/> Other – If a registrant is a foreign national, they input the data required by the Security Foreign National Visit form including Visa information, Passport number, Green Card number, etc. Data is encrypted at rest and while in transit.</p>	
Has there been any attempt to verify PII does not exist on the	Yes	



MODULE I – PRIVACY NEEDS ASSESSMENT

<p>system?</p> <p>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.</p>	
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	<p>Manual Verification</p>

Threshold Questions

<p>1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?</p>	<p>YES</p>
<p>2. Is the information in identifiable form?</p>	<p>YES</p>
<p>3. Is the information about individual Members of the Public?</p>	<p>YES</p>
<p>4. Is the information about DOE or contractor employees?</p>	<p>YES <input checked="" type="checkbox"/> Federal Employees <input checked="" type="checkbox"/> Contractor Employees</p>

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.



MODULE I – PRIVACY NEEDS ASSESSMENT

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>DOE O 206.1</p> <p>Contract #DE-AC07-05ID14517</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>If users decline to provide required information, they will NOT be registered for the activity.</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>NO</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>If the system was tampered with and the information was accessed by an unauthorized user or was not destroyed properly, upon meeting the disposition authority, it could compromise the claimant's Social Security Number.</p>
<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>Data can be retrieved by name, SSN, passport number (if recorded)</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>DOE-51</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>NO</p>
<p>DATA SOURCES</p>	
<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>Individual registrants input data as they register.</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>NO</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>A PDF data dictionary is created of the database for this activity.</p>

DATA USE

<p>11. How will the PII be used?</p>	<p>Information is necessary for completing a Site Security Plan for on-site visitors.</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>N/A</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>Data is not shared outside of activity sponsors.</p>

Reports

<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>a) An excel spreadsheet can be created containing data about foreign nationals.</p> <p>b) A PDF file is created containing the name, affiliation, phone number, email address, and activity plans.</p>
<p>15. What will be the use of these reports?</p>	<p>a) The data will be used to complete the security plan for foreign nationals.</p> <p>b) This file is used to complete conference planning.</p>
<p>16. Who will have access to these reports?</p>	<p>Activity Sponsor</p> <p>DBA/Developer</p>

Monitoring



MODULE II – PII SYSTEMS & PROJECTS

<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>The system can be used to locate individuals in order to contact them with information relevant to the conference. Security will use data applicable to foreign nationals to determine whether or not they will be given access to facilities requested in the security plan. No monitoring of individuals is possible.</p>
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>N/A</p>

DATA MANAGEMENT & MAINTENANCE

<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>During the initial registration process, the data is current and updates are the responsibility of the individual registrant. Update capability is removed after activity is over.</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>Application is internet based and hosted at just one location.</p>

Retention & Disposition

<p>22. What are the retention periods of data in the information system?</p>	<p>The data will be removed from the system 3 or less months after the end of the activity, unless specifically requested by activity sponsor.</p>
<p>23. What are the procedures for disposition of the data at the end of the retention period?</p>	<p>Procedures are documented in the Records Retention Schedule and established in accordance with approved DOE records schedules.</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?	Procedural and physical controls are implemented to prevent misuse. Role-based access control and management approvals assist in multiple layers of protection.
25. Who will have access to PII data?	Activity Administrator, Database Administrator, Security Office Personnel.
26. How is access to PII data determined?	Need-to-know basis in performance of official duties.
27. Do other Information systems share data or have access to the data in the system? If yes, explain.	NO
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?	N/A
29. Who is responsible for ensuring the authorized use of personal information?	Activity Administrator

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
PIA Approval Signatures	Original Copy Signed and On File with the DOE Privacy Office	