Template - January 30, 2009, Version 2

Department of Energy
Privacy Impact Assessment (PIA)

Affects Members Of the Public? ☒

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.

Module I – Privacy Needs Assessment

Date	Original 11/14/08. Redone 3/9/09.	
Departmental Element & Site	National Nuclear Security Administration Pantex Site Office Amarillo, Texas B & W Pantex, M&O Contractor	
Name of Information System or IT Project	U007 Plateau Training Records System	
Exhibit Project UID	019-05-01-11-02-2057-00	
	Name, Title	Contact Information Phone, Email
System Owner	Melynie Greaser, Manager Training Records, B&W Pantex	806.477.3733 mgreaser@pantex.com
Privacy Act Officer	Carolyn Becknell NNSA Privacy Officer	505.845.4869 cbecknell@doeal.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Shane Parsley, ISSM John D. Doggett, DAA/ISOM	sparsely@pantex.com 806.477.6291 jdoggett@pantex.doe.gov 806.477.3194

Module I – Privacy Needs Assessment

Person Completing this Document	Jeffrey Roddahl	(806) 477-4254 jroddahl@pantex.com
Purpose of Information System or IT Project	Plateau Training Records System tracks individual training requirements, training completions and qualification status, in accordance with DOE Order 5480.20A and various State and Federal requirements, including OSHA.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☒ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☒ Employment Information ☐ Criminal History ☒ Name, Phone, Address ☒ Other – Please Specify Training records and qualification to perform work.	
Has there been any attempt to verify Information about an Individual in Identifiable Form does not exist on the system? ***OMB 03-22 defines Information in identifiable form*** as information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) 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).		NO—it clearly does contain such information.
If "Yes," what method was used to verify the system did not contain Information in Identifiable Form? (e.g. system scan)		N/A

Module I – Privacy Needs Assessment

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual members of the public?	YES
4. Is the information about DOE or contractor employees?	YES

If the answer to the **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.

For information systems that collect, maintain or disseminate information in identifiable form from or about members of the public, please complete Modules II and III. 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. This template may not be modified. 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 (and III if necessary).

Module II – System Information for All Systems

Module II – System Information for All Systems	
1. **What categories of individuals are collected or maintained by the information system?**	☒ Federal Employees ☒ Contractor Employees ☒ Members of the Public Individuals in non-employee or contractor context. This includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE. ☒ Other, Please Specify External auditors & visitors who must complete certain safety & security training before coming on site.
2. **What is the source(s) of information about individuals in the information system?**	Employee information is imported from the Human Resources Employee Database; Contractor and Visitor information is provided by the individual.
3. **With what other agencies or entities will an individual's information be shared? How will the information be used?**	None
4. **Is the use of the information in identifiable form both relevant and necessary for the mission of the organization and DOE?**	The information is both relevant and necessary to determine that an individual has received safety and security training. It is also necessary to establish an individual's credentials to work on a nuclear weapon.
5. **Are the data elements described in detail and documented?**	System SQA documentation is on file, as well as an Information System Security Plan (ISSP) as prescribed by NAPs 14.2-C.
REPORTS	
6. **What kinds of reports are produced about individuals or that contain an individual's data?**	Training History, Qualification Status and Training Needed.
7. **What will be the use of these reports?**	These determine what work can be assigned to an individual and when additional training may be needed.
8. **Who will have access to these reports?**	Access is limited to the employee, Supervisor, Training Coordinator and Training Records Administrative Personnel. Access at each level is restricted by need to know and is controlled by system Role security, after documented approval is received for a designed Role level of access. Details are found in the ISSP.

Module II – System Information for All Systems

MAINTENANCE	
9. If the information system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	N/A
10. What are the retention periods of data in the information system?	This data is currently on Epidemiological Moratorium within the DOE Records Management Manual, which means we retain it until told otherwise. When the Epi Moratorium is lifted, various retention periods will take effect, linked to the employee's termination date, plus the content category of the training.
11. What are the procedures for disposition of the data at the end of the retention period?	Printed reports are treated as working documents and are normally destroyed when superseded by a new one. Electronic data will be erased at the end of the retention period.
12. How does the use of this information system affect privacy? Consider also the use of emerging technologies and how those technologies may impact privacy.	Impact to privacy is negligible as the system and reporting focus is on tracking compliance with training requirements. No reports reveal SSN information and the only table that enables SSN lookup is restricted to System Admins and DBAs with a need to know. The system does not share its privacy information with any other systems.
ACCESS	
13. What controls are in place to protect the data from unauthorized access, modification or use?	The Plateau Training Records System hardware is housed in a VTR facility on the Pantex Plant site. Graded levels of both physical and electronic security are also in effect. Access to system information must be authorized in writing by management, and granted by the Data Owner. Complete details can be found in the ISSP for Plateau (U007).
14. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?	N/A

Module II – System Information for All Systems

15. Who will have access to this information system and its data (all data)? Will other agencies share data or have access to the data in this system? How will the data be used by the other agency?	N/A
16. Who will have access to information in identifiable form or and PII?	Access is limited to the employee, Supervisor, Training Coordinator and Training Records Administrative Personnel. Access at each level is restricted by need to know and is controlled by system Role security, after documented approval is received for a designed Role level of access. Details are found in the ISSP.
17. How is access to the data determined?	Access to system information must be authorized in writing by management, and granted by the Application Administrator.
18. 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?	**Yes, the software manufacturer, Plateau LTD, is under contract to provide maintenance of the system. (Contract numbers 45381 and 63799 apply)**
19. Do other information systems share data or have access to the data in the system? If yes, explain.	Several apps use the data as part of access rights determination; others use it to determine eligibility for work or overtime assignments. No Privacy information is shared.
20. For connecting information systems, is there an ISA other agreement between System Owners to ensure the privacy of individuals is protected?	There are no external connections. Plateau receives updates to personnel data via nightly interface from the Pantex Peoplesoft HR system. Plateau populates a static table nightly that several applications come to for updated qualification status information. Several apps use the data as part of access rights determination; others use it to determine eligibility for work or overtime assignments.
21. Who is responsible for assuring proper use of the information system's information in identifiable form?	Melynie Greaser, Training Records Manager

Module III – Systems with Information About Members of the Public

1. **What legal authority authorizes the purchase, development or maintenance of this information system?**	42 U.S.C. 7101 et seq.; 50 U.S.C. 2401 et seq.; Nuclear Waste Policy Act of 1982 (Pub. L. 97-425); Nuclear Waste Policy Amendment Act of 1987 (Pub. L. 100-203); Government Employees Training Act of 1958; and 5 CFR Parts 410 and 412. DOE Order 5480.20A and various State and Federal requirements, including OSHA, require that an accurate, auditable set of Training Records be kept.
2. **Has a Privacy Act System of Records Notice been published in the Federal Register? If "Yes," provide name of SORN and location in the Federal Register.**	No, as no determination has been made yet that Plateau is a "System of Records".
3. **If the information system is being modified, will the SORN require amendment or revision?**	Unknown at this time.
4. **How will data collected from sources other than DOE records be verified for accuracy, relevance and completeness?**	Plateau does not collect information from sources other than internal DOE records.
5. **Are records in the system about individuals current? What steps or procedures are taken to ensure the data is current?**	Training Completion Data are current to within three hours (or less) of receipt at the Records Office. Personal data kept in the Peoplesoft HR system is updated nightly; SSN doesn't change.
6. **Will the information system derive new or meta data about an individual through aggregation from the information collected? How will this be maintained, including verified for relevance completeness, and accuracy?**	Plateau receives daily data inputs documenting training completions which are used to compute qualification status. This data is cumulative and represents the employee training history. It is maintained according to the requirements of the DOE Administrative Records Manual and destroyed according to the RIDS schedule.
7. **Will the new or meta data be part of an individual's record?**	As training is completed initially and annually, this information is added to an individual's training record in the Plateau system.

Module III – Systems with Information About Members of the Public	
8. How will the new or meta data be used? Will it be used to make determinations about members of the public?	Information collected on an individual is training history. From this, reports can be generated on Qualification Status and Training Needed. These determine what work can be assigned to an individual and when additional training may be needed. Access is limited to the employee, Supervisor, Training Coordinator and Training Records Admin Personnel.
9. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.	Data on the individual is normally accessed using Pantex badge number as an input parameter, but can also be searched for using Name (or SSN if provided by the employee). However, a reverse SSN lookup is only possible for the System and Database Administrators. This restriction is tested as part of the System Security plan. SSN does not appear on any public screens or reports. Outside visitors who do not have a Pantex badge number are auto-assigned a "Learning Management System" (LMS) number for lookup and recording of training.
10. 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)?	Providing the information is a condition of employment. In the case of Visitors/Contractors, providing the information is a condition of access to the plant.
11. Will this information system provide the capability to identify, locate, and monitor individuals?	Plateau records do not inherently provide this capability. Location and identification information is uploaded nightly from the PeopleSoft HRIS System.
12. What kinds of information are collected as a function of the monitoring of individuals?	Information collected is training history. From this, reports can be generated on Qualification Status and Training Needed. These determine what work can be assigned to an individual and when additional training may be needed. Access is limited to the employee, Supervisor, Training Coordinator and Training Records Admin Personnel.
13. What controls will be used to prevent unauthorized monitoring?	Only authorized individuals can search or generate reports from the Plateau system. Authorization is granted by the individual's manager, via submission of a written request for access, modification or removal to information systems. Access within the Plateau system at each level is restricted by need to know and is

Module III – Systems with Information About Members of the Public	
	controlled by system Role security after documented approval to a designated Role level of access. Details are found in the Information System Security Plan (ISSP) for Plateau. Learner interface roles are restricted to the employee and their managerial chain. Lower-level Training Records administrative personnel have access to all data except SSN. The System Administrator and the Database Administrator have access to all information, and because of this, are required to be members of the Human Reliability Program (HRP). Other physical and virtual controls are detailed in the ISSP.

SIGNATURE PAGE

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