PRIVACY IMPACT ASSESSMENT
NATIONAL NUCLEAR SECURITY ADMINISTRATION
WEAPON DATA ACCESS CONTROL SYSTEM
PIA Template Version 3 – May, 2009

Affects Members Of the Public? Mark if Applicable

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	December 16, 2009
Departmental Element & Site	National Nuclear Security Administration (DOE Headquarters, Germantown, Room CA-007 server room)
Name of Information System or IT Project	Weapon Data Access Control System
Exhibit Project UID	DP1130020
New PIA [X] **Update** [ ]	

	Name, Title	Contact Information Phone, Email
System Owner	Douglas S. Strack, Chief, Weapon Security and Control Branch, NA-122.12, Nuclear Weapon Surety and Quality Division	(202) 586-8938 douglas.strack@nnsa.doe.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Carolyn Becknell, PAO, NNSA Service Center	(505) 845-4869 cbecknell@doeal.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	James C. Baldree, Cyber Security Site Manager	(301) 903-5523 james.baldree@nnsa.doe.gov
Person Completing this Document	Bonnie M. Carnes, Use Control Site Verifier Nuclear Weapon Surety and Quality Division, NA-122.1	(202) 586-4147 bonnie.carnes@nnsa.doe.gov
Purpose of Information System or IT Project	The purpose of WDACS is to track visits and access approvals to DOE facilities in the Nuclear Security Enterprise (NSE). In order to control dissemination of nuclear weapon data, the data is broken into categories known as "sigma" categories, to which access can be granted on an "as needed" basis. The current system is connected to the DOE's electronic Department of Energy Integrated Security Systems (eDISS+), which provides up-to-date personnel security clearance information.	
Type of Information Collected or Maintained by the System:	X SSN Social Security number ☐ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number X 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	

MODULE I – PRIVACY NEEDS ASSESSMENT

	X Name X Other – dates and locations of weapon data visits within the NSE.

Has there been any attempt to verify PII does not exist on the system? **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.*	NO The system does contain PII.
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Not applicable.

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 X Federal Employees X Contractor Employees

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

MODULE I – PRIVACY NEEDS ASSESSMENT

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

1. AUTHORITY **What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?**	The Atomic Energy Act of 1954, As Amended; DOE Order 452.4-1A, Protection of Use Control Vulnerabilities and Designs, dated March 11, 2004; DOE Order 5610.2, Control of Weapon Data, dated August 1, 1980; and DOE Order 205.1A, Department of Energy Cyber Security Management, dated December 4, 2006.
2. CONSENT **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)?**	Provision of the information is voluntary. However, failure to provide the information will preclude access to classified nuclear weapon data and may prevent entry into any NSE site.

MODULE II – PII SYSTEMS & PROJECTS

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?**	YES. The Privacy Act clauses are included in the contracts and regulatory measures are addressed.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	The use of this system does not affect the public/employee privacy. Restricted access is granted to users and their managers at the NNSA Headquarters. System Administrators will have full access to the database. Read only access will be granted to a limited number of users in the field. The Nuclear Weapon Surety and Quality Division is responsible for assuring proper use of the data.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Data for an individual's visit to the NSE can be retrieved by name, social security number, or a tracking number generated by the system.
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	YES. WDACS operates under DOE-45, Weapon Data Access Control System (WDACS), which was published in the Federal Register dated April 2, 2008.

MODULE II – PII SYSTEMS & PROJECTS	
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	YES. Phase 1 of the system upgrade has been completed. A revision to the SORN is being prepared to reflect the latest changes; for example, the locations for access to the system.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	The source of the information in the system is the individual visitors and data extracted from the eDISS+ system. Department of Energy, NNSA, other Government Agencies, and Department of Defense (DoD) and DoD contractors, and contractor employees provide information as well. All tribal, state, and local agencies provide data for use in WDACS when a classified visit to the NSE is requested.
9. Will the information system derive new or meta data about an individual from the information collected?	YES. The system authorizes entry and access approval to the NSE. The Badge Offices at each site have read only access to the system for their site in order to validate entry and access approval or disapproval. Records older than 5 years are moved out of the production tables into the archive table. The current system is connected to the DOE's eDISS+ system which provides up-to-date personnel security clearance information.
10. Are the data elements described in detail and documented?	YES. Applications which comprise the system use sound business practices and are documented within an internal Memorandum of Understanding between NNSA (Nuclear Weapon Surety and Quality Division) and the DOE (Office of Departmental Personnel Security) on the development, establishment, operation, and maintenance of the WDACS application. There are numerous data protection and access controls which are formally documented in the eDISS+ Information System Security Plan. Examples of data protection controls include: McAfee VirusScan scans are performed on a not greater than monthly basis, and multiple packet-filtering, stateful-inspection firewalls. Examples of access controls include: accounts are managed by the Personnel Security Database Administrator who is designated by the system owner, and user accounts are based on least privilege with roles defined in the eDISS+ Information System Security Plan.

MODULE II – PII SYSTEMS & PROJECTS

DATA USE	
11. How will the PII be used?	The PII data is used to allow visitors to enter the NSE in order to conduct official business on a classified level. In order to control dissemination of nuclear weapon data, the data is broken into categories known as "sigma" categories, to which access can be granted on a "need-to-know" basis. The eDISS+ system provides up-to-date personnel security clearance information.
12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	YES. The system authorizes entry and access approval to the NSE. The Badge Offices at each site have read only access to the system for their site in order to validate entry and access approval or disapproval. Records older than 5 years are moved out of the production tables into the archive table. The current system is connected to the DOE's eDISS+ system which provides up-to-date personnel security clearance information.
13. With what other agencies or entities will an individual's information be shared?	The data collected in WDACS are shared with the NSE only to authorize entry and access approvals.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports identify data associated with the individual's visits to the NSE and may include personal information.
15. What will be the use of these reports?	The reports are used to aid the timely processing and management of visits to the NSE.
16. Who will have access to these reports?	Access to these reports is restricted to appropriately cleared (i.e., Q-cleared) NNSA, DOE, and contractor personnel working in direct support of visitor control activities.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system does not have the capability to locate and monitor individuals.

MODULE II – PII SYSTEMS & PROJECTS	
18. What kinds of information are collected as a function of the monitoring of individuals?	The system collects Social Security Numbers, security clearance information, and identifies dates and locations of weapon data visits with the NSE.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	Not applicable to this system.
DATA MANAGEMENT & MAINTENANCE	
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.	Data for DoD visitors to the NSE are verified for accuracy by an authorized DoD official. Data for visits by Other Government Agency personnel are verified for accuracy by the Security Assistant in the Office of Health, Safety, and Security (HS-1.2). Individual request forms are visually checked for completeness prior to data entry. Internal controls within the system do initial validations at the point of data entry using software controls. The data entered into the system are controlled by the individuals requesting the visit to the NSE, while the need-to-know of sigma information is controlled by the hosting individual.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	Data entry for the system will be performed by the staff of the NNSA Headquarters only; however, other sites will have "read only" access to the system. The "read only" access will be controlled by NNSA Headquarters and will be kept to the minimum necessary.
Retention & Disposition	
22. What are the retention periods of data in the information system?	The data in the system are being maintained permanently in the archive table; however, paper copies of the visit requests are maintained for five years. Department of Energy Order 452.4-1A, Protection of Use Control Vulnerabilities and Designs, dated March 11, 2004, mandates that historical data be maintained of visits to the NSE.
23. What are the procedures for disposition of the data at the end of the retention period?	The data in the system are being maintained permanently in the archive table; however, paper copies of the visit requests are only maintained for five years. A request to the National Archive and Records Administration has been made to officially approve a permanent retention period for the electronic data; no approved Records Inventory and Disposition Schedule exists which covers permanent retention for electronic records.

MODULE II – PII SYSTEMS & PROJECTS

ACCESS, SAFEGUARDS & SECURITY

24. What controls are in place to protect the data from unauthorized access, modification or use?	The certification and accreditation boundary of the system is defined logically. All components are located within and including the eDISS+ firewall at Germantown and are under direct management of the eDISS+ system owner. The eDISS+ Security Plan, dated June 2008, defines the accreditation boundary.
25. Who will have access to PII data?	Data entry for the system will be performed by a minimum number of staff at the NNSA Headquarters only; however, a minimum number of staff at other sites will have "read only" access to the system for their site only. The System Owner is responsible for ensuring that the number of staff with access is kept to the minimum possible. The current access control list is maintained in paper copy as well as electronic on the WDACS.
26. How is access to PII data determined?	The System Administrator will have full access to the system, while "read only" access will be granted to a limited number of users in the field.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	The current system is connected to the DOE's eDISS+ system which provides up-to-date personnel security clearance information. However, eDISS+ cannot extract data from WDACS.
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?	An Interconnection Security Agreement (ISA) is not required since the primary computing elements of WDACS reside within the eDISS+ accreditation boundary. WDACS resides on the HSS server in Germantown.
29. Who is responsible for ensuring the authorized use of personal information?	Data entry for the system will be performed by a minimum number of staff at the NNSA Headquarters only; however, a minimum number of staff at other sites will have "read only" access to the system for their site only. The System Owner is responsible for ensuring that the number of staff with access is kept to the minimum possible. The current access control list is maintained in paper copy as well as electronic on the WDACS.

MODULE II – PII SYSTEMS & PROJECTS

END OF MODULE II