Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Hanford Tank Waste Treatment and Immobilization Plant (WTP) Project - Bechtel National, Inc
Bureau: U. S. Department of Energy (DOE), Richland Operations Office (RL)
Project Unique ID: WTP Foreign National Tracking System (FNTS)
Date: August 28, 2007

A.   CONTACT INFORMATION

1. Who is the person completing this document?

Jerry Hatcher
Manager, Safeguards and Security
Bechtel National
2435 Stevens Center Place
Richland, WA 99354

2. Who is the system owner?

Gary Loiacono
Security and Emergency Services Division
U.S. Department of Energy
Richland Operations Office
P.O. Box 550
Richland, WA 99352

3. Who is the system manager for this system or application?

Dana Kranz
Chief Information Officer
U.S. Department of Energy
Richland Operations Office
P.O. Box 550
Richland, WA 99352

4. Who is the IT Security Manager who reviewed this document?

Harry Bell
U.S. Department of Energy
Richland Operations Office

P.O. Box 550
Richland, WA 99352

5. Who is the Privacy Act Officer who reviewed this document?

Dorothy Riehle
Privacy Act Officer
U.S. Department of Energy
Richland Operations Office
P.O. Box 550
Richland, WA 99352

Abel Lopez, Director
FOIA and Privacy Act Group
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

B. SYSTEM APPLICATION/GENERAL INFORMATION

1. **Does this system contain any information about individuals?**

   a. **Is this information identifiable to the individual?[1] Yes**

   b. **Is the information about individual members of the public? Yes**

   c. **Is the information about DOE or contractor employees? No**

2. **What is the purpose of the system/application?** Application is used to maintain, document and track information on non-U.S. citizens who require access to the Waste Treatment Plant (WTP) at Hanford.

3. **What legal authority authorizes the purchase or development of this system/application?**

   Title 42, United States Code (U.S.C.), Section 7101, et. seq.; and 50 U.S.C 2401, et. seq.

---

[1] "Identifiable Form" – According to the OMB Memo M-03-22, this means information in an IT system or online collections: (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 descriptions).

C. DATA IN THE SYSTEM

1. **What categories of individuals are covered in the system?** Non-U.S citizens that require access to the WTP.

2. **What are the sources of information in the system?**

   a. **Is the source of the information from the individual or is it taken from another source?** Yes, the information is from the individual to who it pertains.

   b. **What Federal agencies are providing data for use in the system?** DOE RL

   c. **What tribal, state, and local agencies are providing data for use in the system?** None.

   d. **From what other third party sources will data be collected?** None.

   e. **What information will be collected from the individual and the public?**

      Name, passport number and expiration date, type of visa and expiration date, and e-mail addresses.

3. **Accuracy, Timeliness, and Reliability**

   a. **How will data collected from sources other than DOE records be verified for accuracy?** Since the data is provided by the individual to whom it pertains, it is determined that the information is accurate at the time is it provided.

   b. **How will data be checked for completeness?** Data is validated upon documents provided by the individual.

   c. **Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?** Since the data is provided by the individual to whom it pertains, it is determined that the information is current and not out-of-date at the time is it provided.

   d. **Are the data elements described in detail and documented?** The data elements for each record in this database are described in the database tables for this application.

D. ATTRIBUTES OF THE DATA

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?** Yes.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? No.

3. Will the new data be placed in the individual's record? N/A

4. Can the system make determinations about employees/the public that would not be possible without the new data? N/A

5. How will the new data be verified for relevance and accuracy? N/A

6. If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use? Data is not being consolidated.

7. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access? N/A

8. How will 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. Yes, data is retrieved by the name of the individual.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? The authorized user can generate routine reports as a matter of routine business. These reports contain the date of request for access to the local area network, approval date for the Foreign National Computer Access Request, name, country of birth, and country of citizenship.

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)? Information is provided by the individual voluntarily and required for access to the site. If the individual declines to provide the necessary information, access will not be granted.

E. Maintenance and Administrative Controls

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites? The system is not operated in more than one site.

2. What are the retention periods of data in the system? Records retention and disposal authorities are contained in the National Archives and Records Administration (NARA) General Records Schedule and DOE records schedules that have been approved by NARA.

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Procedures are documented in

4

the Records Schedule and established in accordance with NARA General Records Schedule.

4. **Is the system using technologies in ways that DOE has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?** No.

5. **How does the use of this technology affect public/employee privacy?** N/A

6. **Will this system provide the capability to identify, locate, and monitor individuals?** No.

7. **What kinds of information are collected as a function of the monitoring of individuals?** N/A

8. **What controls will be used to prevent unauthorized monitoring?** N/A

9. **Under which PA system of records notice does the system operate?** DOE-52, "Access Control Records of International Visits, Assignments, and Employment at DOE Facilities and Contractor Sites".

10. **If the system is being modified, will the PA system of records notice require amendment or revision?** No.

F. **ACCESS TO DATA**

1. **Who will have access to the data in the system?** Only authorized personnel who have a need-to-know and are approved by the data owner.

2. **How is access to the data by a user determined?** Access is governed by a need-to-know basis s verified by access requests.

3. **Will users have access to all data on the system or will the user's access be restricted?** No. User access is controlled by the data owner and information is restricted by a need-to-know basis.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** Data elements for viewing are determined by the data owner in database schemas and are verified by the network authentication for network user access.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?** Yes. **If yes, were PA contract clauses included in their contracts and other regulatory measures addressed?** Information may be disclosed to contractors and their officers and employees in performance of the contract. Individual provided this information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.

Pertinent contract language states that data covered by the Privacy Act may be disclosed to contractors and their officers and employees. Any information that is obtained or viewed shall be on a need-to-know basis. Contractors are required to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE Richland Operations Office. The contractor shall ensure that all DOE documents and software processed, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.

6. **Do other systems share data or have access to the data in the system? If yes, explain.** No.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** N/A

8. **Will other agencies share data or have access to the data in this system?** No

9. **How will the data be used by the other agency?** N/A

10. **Who is responsible for assuring proper use of the data?** N/A

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