Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Oak Ridge Office (ORO) SharePoint (Microsoft SharePoint Server)
Bureau: Department of Energy (DOE)
Project's Unique ID: 019-60-02-00-01-5000-04
Date: September 20, 2007

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Samuel Mashburn
Information Technology Support Services Contractor
U.S. Department of Energy
200 Administration Road
Oak Ridge, TN 37830
865-576-2594

2) Who is the system owner?

Bobby Price, Director
U.S. Department of Energy
Information Resources Management Division
200 Administration Road
Oak Ridge, TN 37830
865-576-5103

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

Gwen Senviel
U.S. Department of Energy
Information Resources Management Division
200 Administration Road
Oak Ridge, TN 37830
865-576-3331

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

Qui Nguyen
U.S. Department of Energy
Materials Control and Accountability
and Information Security Team
200 Administration Road

Oak Ridge, TN 37830
865-576-1600

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

Amy Rothrock
U.S. Department of Energy
Office of Chief Counsel
200 Administration Road
Oak Ridge, TN 37830
865-576-1216

Abel Lopez, Director
U.S. Department of Energy
FOIA and Privacy Act Group
1000 Independence Avenue, SW
Washington, DC 20585
202-586-5958

B. SYSTEM APPLICATION/GENERAL INFORMATION:

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

Yes.

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?**

Yes.

2) **What is the purpose of the system/application?**

[1] "Identifiable Form" - According to the OMB Memo M-02-22, this means 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 descriptor).

The ORO SharePoint system provides a single, integrated intranet location where employees can efficiently collaborate with team members, find organizational resources, search for experts and corporate information, manage content and workflow, and leverage business insight to make better-informed decisions. The system facilitates information sharing and provides access to information that is essential to meeting ORO missions/goals through *work group* sites for specific content publishing, content management, or business intelligence needs.

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.; 50 U.S.C. 2401 et seq.; the Freedom of Information Act, 5 U.S.C 552; and the Privacy Act of 1974, 5 U.S.C. 552a.

C. DATA IN THE SYSTEM:

1) **What categories of individuals are covered in the system?**

The categories of individuals covered by the system are the members of the public, federal and contractor employees.

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 source of Personally Identifiable Information (PII) is from individual members of the public, DOE ORO employees, or contractors making requests, claims or inquiries of the government. Information may be gathered from various other sources.

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

Currently, no other federal agencies are providing data for use in the system. However, the system is a centralized Intranet and collaboration tool for the ORO which allows "work groups" to share and collaborate within the groups to accomplish their assigned missions. Information may be gathered from various sources including other federal agencies.

c. **What Tribal, State and local agencies are providing data for use in the system?**

Currently, no Tribal, State, or local agencies are providing data for use in the system. However, the system is a centralized Intranet and collaboration tool for the ORO which allows “work groups” to share and collaborate within the groups to accomplish their assigned missions. Information may be gathered from various sources including Tribal, State, and local agencies if necessary to accomplish the mission.

d. From what other third party sources will data be collected?

Currently, no data from other third party sources is collect. However, the system is a centralized Intranet and collaboration tool for the ORO which allows “work groups” to share and collaborate within the groups to accomplish their assigned missions. Information may be gathered from various sources if necessary to accomplish the mission.

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

The FOIA and Privacy Act requires a requester to provide their name, mailing address, telephone number and a description of the requested documents. This information is necessary to process the request under the appropriate statute and provide the requested information within the time limits as required by the statues and DOE regulations.

Congressional inquiries require the Congressional representative to provide the name of the constituent, mailing address, telephone number and the nature of the inquiry. This is information is necessary to respond to the representative or constituent in a timely manner.

However, the system allows for any authorized user (work group) to input documents. Work groups may request any type information from any source necessary to accomplish their various missions.

4) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?

Data is not obtained from other sources for FOIA and Privacy Act requests and Congressional inquiries systems. Data obtained from the individual is considered to be accurate. Also, the system allows for any authorized user (work group) to input documents. The user is responsible for the accuracy of the input.

b. **How will data be checked for completeness?**

Data obtained from the individual is determined that the data is complete. However, the system allows for any authorized user (work group) to input documents. The user also is responsible for the completeness of the input.

c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?**

Data obtained from the individual is determined to be current. However, the system allows for any authorized user (work group) to input documents. The user is responsible for the currency of the input.

d. **Are the data elements described in detail and documented?**

There are no "documented" data elements. Data is retrieved via Sharepoint's document content and keyword search capability.

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, the system will not derive new data.

3) **Will the new data be placed in the individual's record?**

N/A

4) **Can the system make determinations about employees/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 is 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, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

Processes are not being consolidated.

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.**

Data is retrieved via SharePoint's document content and keyword search capability. Data that pertains to FOIA and Privacy Act requests may be retrieved by the name of the individual and assigned control number. Congressional inquiries may be retrieved by the name of the constituent or the name of the Member of Congress. However, documents may be retrieved by other information contained within the document.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

All system users are ORO IRMD Enclave users. The security system is designed to use a logical security system to allow only restricted access to the documents. The user defines the reports and is responsible for the usage of the data produced on the report.

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)?**

The information is required. It is provided voluntarily by the individual to process request, inquiries and claims. However, work groups may request any type information from any source necessary to accomplish their various missions.

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 are maintained in all sites?**

The system is used only within the ORO IRMD Enclave boundaries. All system users are ORO users.

2) **What are the retention periods of data in the system?**

   The records retention periods are in accordance with applicable National Archives Records Administration (NARA) and DOE record schedules. Information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.

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? Where are the procedures documented?**

   The records disposition procedures are in accordance with applicable NARA and DOE record schedules. Information can be obtained at http://cio.energy.gov/records-management/adminrs.htm.

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?**

   Not applicable.

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?**

   The system is run under the functional and administrative controls for the ORO Information Resource Management Division (IRMD) Enclave. The ORO IRMD Enclave is classified as "Moderate" according to Federal Information Security Management Act (FISMA) and has the appropriate controls to identify and stop misuse of the systems within it. The system limits access to the documents based on functional roles and user ID. No user is permitted access to the documents for monitoring purposes without ORO and IRMD management direction.

9) Under which Privacy Act system of records notice does the system operate?

Presently there is not a Privacy Act system of records notice for this cross-cutting collection of information. However, the system will be evaluated to determine if a Privacy Act system of records is needed. If it is determined that a Privacy Act system of records notice is required, one will be established.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision?

The system will be evaluated to determine if a Privacy Act system of records is needed. If it is determined that a Privacy Act system of records notice is required, one will be established.

F. <u>ACCESS TO DATA:</u>

1) Who will have access to the data in the system?

All system users are ORO users. Access is strictly controlled based on user group, job responsibility and function. User-name and password are required to access data.

2) How is access to the data by a user determined?

Access to data is determined by Group. The account structure that implements ORO SharePoint Site has been designed to limit access to a site or site module by Group and or through a direct account. To modify users' permissions the group must submit a request to the site administrator through the SharePoint Access Request function.

3) Will users have access to all data on the system or will the user's access be restricted?

Access is determined through account access procedures.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

The ORO SharePoint system has been implemented with a role-based security process that is applied to each user account. A user must be granted permission to view document by Group. The account structure that implements ORO SharePoint system has been designed to limit access to a site or site module by Group and or through a direct account.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?**

Contractors are involved in the design, development, and maintenance of the system. Personal information from systems maintained by the Information Technology Support Services Contractor may be disclosed as a routine use to these contractors and their officers and employees in performance of their contracts. Those individuals provided information under this routine use 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. 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 other systems share the ORO SharePoint Site data.

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 data is shared from this data source.

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

The Following Officials Have Approved this Document

1) System Manager

Gwen Senviel (Signature) 9/22/07 (Date)

Name: Gwen Senviel
Title: Software Engineering Project Manager

2) Systems Owner

(Signature) 10/25/07 (Date)

Name: Bobby Price
Title: Director of Information Resources Management Division

3) Cyber Security Manager

Qui Nguyen (Signature) 10/25/07 (Date)

Name: Qui Nguyen
Title: Cyber Security Manager

4) Privacy Act Officer

Amy Rothrock (Signature) 10/25/07 (Date)

Name: Amy Rothrock
Title: Privacy Act Officer

DOE Privacy Officer

Kevin T. H (Signature) 11/8/07 (Date)

Name: Kevin T. Hagerty
Title: Director, Office of Information Resources

DOE Senior Official for Privacy Policy

Ingrid Kolb (Signature) 11-8-07 (Date)

Name: Ingrid Kolb
Title: Senior Officer for Privacy Policy