Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Oak Ridge Office (ORO) Document Management System (Hummingbird DM)
Bureau: Department of Energy (DOE)
Project's Unique ID: 019-60-02-00-01-5000-04
Date: 9/20/2007

A. CONTACT INFORMATION:

1) **Who is the person completing this document?**

Samuel Mashburn
Information Technology Support Services Contractor
U.S. Department of Energy
Oak Ridge Operations Office
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?**
   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?**

The ORO Document Management system was established to provide for a centralized Document Management system to manage and control correspondence and other documents necessary to the ORO mission. Correspondence may be sent to and received from Members of Congress; other government agencies, state and local governments, members of DOE Advisory committees, other DOE programs, ORO employees, and the public.

The system is a state-of-the-art tool that aids in the tracking of correspondence and other documents to efficiently manage the workload of the ORO. It provides enterprise-wide access to information quickly and with consistent results, capitalizes on technology for better full-text and index search and retrieval, and ensures that users are able to locate all of the electronic documents they are entitled to see.

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 include individuals making requests of the Government, members of DOE Advisory Committees, Members of Congress, representatives of organizations, Federal, State, and local agencies, members of the general public, DOE ORO Employees, 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?**

Information is obtained from the individual who submits the correspondence/document.

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

None.

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?

Categories of information include name, business contact data (work address, work phone number, type of business or organizational affiliation), personnel contact information (home address and home phone number) social security number, and date of birth.

3) Accuracy, Timeliness, and Reliability

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

Documents scanned into the Hummingbird DM repository are considered accurate at the time they are entered.

b. How will data be checked for completeness?

The system does not check for completeness. Documents scanned into the Hummingbird DM repository are considered complete at the time they are entered.

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

The system does not verify currency of the information. Documents scanned into the Hummingbird DM repository are considered current at the time they are entered. There is no requirement to update the documents.

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

Yes. A Document Profile, which serves as the index to the document (similar to a library catalog card), is created for every item entered into the system. The Profile contains information about the document such as subject (title), originator (author), and date. However, there are no specific data elements that pertain to PII. Any data that is PII is restricted to the image or file being stored. The data elements are described and documented in the Document Online Coordination System (DOCS) Systems and Design Document and the Hummingbird Document Management (DM) - Training Material (ORO-QSTR-DMM001).

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. All documents in the system are relevant and necessary for the ORO to effectively and efficiently perform its responsibilities.

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?**

   Not applicable.

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

   Not applicable.

5) **How will the new data be verified for relevance and accuracy?**
   Not applicable.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   The Hummingbird DM system does not consolidate data. However, users may access the records and manually initiate actions such as save, print, and send to others. Therefore, the system has been implemented with a Role Based security process that is tied to each User Account. The user must be granted permissions to view documents by Group. The folder structure that implements the Hummingbird Security has been designed to limit access to a Record Collection by Group. No PII data is visible or modifiable without explicit permissions of the Group Admin for that collection. To modify user's permissions the group must submit a request to the Hummingbird administrator through the ORO Helpdesk. Users receive annual cyber security training and acknowledge awareness of User Responsibilities.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

   The Hummingbird DM system does not consolidate data. However users may access the records and manually initiate actions such as save, print, and send to others. Therefore, the system has been implemented with a Role Based security process that is tied to each User Account. The user must be granted permissions to view documents by Group. The folder structure that implements the Hummingbird Security has been designed to limit access to a Record Collection by Group. No PII data is visible or modifiable without explicit permissions of the Group Administrator for that collection. To modify user's permissions the group must submit a request to the Hummingbird administrator through the ORO Helpdesk. Users receive annual cyber security training and acknowledge awareness of User Responsibilities.

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.**

The system is designed specifically for easy document retrieval. Profile fields allow for retrieval of known elements of the document. These fields include From and To fields, the subject field, date fields. However, all text within the document is searchable via the context search capability of the system.

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

No reports are produced on individuals.

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)?**

None. The data is provided voluntarily.

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 with 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 NARA and DOE record schedules. Additional 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 periods are in accordance with applicable NARA and DOE record schedules. Additional information can be 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?**

Not applicable.

8) **What controls will be used to prevent unauthorized monitoring?**

The system is subject to the functional and administrative controls for the Information Resources Management (IRMD) Enclave. The 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 Identification Number. 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. ACCESS TO DATA:

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 the system 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 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?**

Technical and Administrative controls are in place to prevent the misuse of the information. The 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 the 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 Hummingbird DM data.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Not Applicable.

8) **Will other agencies share data or have access to the data in this system?**

The documents are of Department of Energy documents only. No data is shared directly from this data source.

9) **How will the data be used by the other agency?**

Not Applicable.

10) **Who is responsible for assuring proper use of the data?**

Not Applicable.

The Following Officials Have Approved this Document

1) System Manager

Gwen Senviel (Signature) 10/22/07 (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

(Signature) 11/8/07 (Date)
Name: Kevin T. Hagerty
Title: Director, Office of Information Resources

DOE Senior Official for Privacy Policy

(Signature) 11-8-07 (Date)
Name: Ingrid Kolb
Title: Senior Officer for Privacy Policy