Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: HS Web Services (HSWS)
Bureau: Department of Energy
Project's Unique ID: 019-20-01-22-02-3012-00
Date: August 20, 2008

A. CONTACT INFORMATION

1) **Who is the person completing this document?**
Steve Simon, Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Ave., S.W., Washington, D.C. 20585, 301-903-5615
2) **Who is the system owner?**
Steve Simon, Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Ave., S.W., Washington, D.C. 20585, 301-903-5615
3) **Who is the system manager for this system or application?**
Raymond Holmer, Director, Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Ave., S.W., Washington, D.C. 20585, 301-903-7325
4) **Who is the IT Security Manager who reviewed this document?**
Vinh Le, Office of Information Management, Office of Health, Safety and Security, U.S. Department of Energy, HS-1.22, 1000 Independence Ave., S.W., Washington, D.C. 20585, 301-903-4648
5) **Who is the Privacy Act Officer who reviewed this document?**
Jerry G. Hanley, Chief Privacy Officer, Office of Information Resources, Office of Management, U.S. Department of Energy, MA-90, 1000 Independence Avenue, S.W., Washington, DC 20585, 202-586-0483

B. SYSTEM APPLICATION/GENERAL INFORMATION

1) **Does this system contain any information about individuals?**
No. This system contains names, business phone numbers and email addresses of individuals associated with documents or information which a person is requesting for. The system does not request nor contain social security numbers, dates of birth, or any privacy information.
   a. **Is this information identifiable to the individual?** [1]
   Yes. However, the system does not request nor contain social security numbers, dates of birth, or any privacy information.
   b. **Is this information about individual members of the public?**

[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).

Yes. However, the system does not request nor contain social security numbers, dates of birth, or any privacy information.

c. **Is the information about employees?**
Yes.

2) **What is the purpose of the system/ application?**
The purpose of the system is to provide Office of Health, Safety and Security documents, data and information to DOE and its stakeholders.

3) **What legal authority authorizes the purchase or development of this system/application?**
In response to the E-Government Act of 2002, the Web Services investment maximizes the sharing and efficient use of data and information in support of the DOE HSS. These services ensure that needed information is obtained in a timely manner in support of these management strategic goals. Specifically, the investment supports the DOE Strategic Plan by ensuring the safety and health of the DOE workforce and members of the public, and the protection of the environment in all Departmental activities.

C. DATA IN THE SYSTEM

1) **What categories of individuals are covered in the system? (e.g., agency employees, contractor employees, visitors, volunteers, etc.)**
The categories of individuals covered in the system include DOE employees, contractor employees and members of the public.

2) **What are the sources of the information in the system?**
The main source of publicly-accessible information in the system will be subject matter experts (SMEs) within HSS. The SME's will submit documents / information to be posted on the public and/or restricted web sites, as applicable. The sources of information for the database applications are individuals such as DOE employees, contractors or stakeholders in support of the mission and functions of HSS.

a. Is the source of the information from the individual or is it taken from another source?
HTML and PDF documents posted to the HSS web sites are provided by DOE HSS subject matter experts. In the database applications, the source of the information is submitted from the individual. No information is taken from other sources.

b. What Federal Agencies are providing data for use in the system?
Department of Energy personnel provide data for posting on the web sites. Workers at other federal agencies may submit data to one or more database applications, depending upon its function (conference registration, document account request, etc.). No Federal Agency is required to provide data to any database applications.

c. What Tribal, State and local agencies are providing data for use in the system?
No Tribal, State or local agencies provide data for posting on the web sites. No state or local agencies are required to provide data in any database applications.

d. From what other third party sources will data be collected?
No third party sources provide data for posting on the web sites. No other third party sources are required to provide data in any database applications.

e. What information will be collected from the individual and the public?
For the web sites, information pertaining to the mission and functions of HSS, such as reports, memorandums and documents will be posted on the web for public access. Information collected in database applications will vary depending upon the requirements. In general, the

database applications collect names, phone numbers, work addresses and email addresses for conference registrations or access account requests. A Privacy Act Notice is linked to every page on the web site and is included in Appendix A.

3) **Accuracy, Timeliness, and Reliability**

All data posted on the HSS web sites is reviewed for accuracy and completeness before posting. Data submitted to database applications is reviewed on a per-application basis, depending upon the application requirements.

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

All documents and information are reviewed before posting on the HSS web site. Data posted to database applications is verified on a per-application basis, depending upon the application requirements.

b. How will data be checked for completeness?

All documents and information are reviewed before posting on the HSS web site. Data submitted to database applications is reviewed for completeness on a per-application basis, depending upon the application requirements.

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

Periodic web site content reviews by subject matter experts and content owners ensure that the data is current. Data submitted to database applications is reviewed for its currency on a per-application basis, depending upon the application requirements.

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

This question is not applicable for web site content such as HTML or PDF documents. Data elements in database applications are described and documented on a per-application basis in the project documentation.

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?**

The system is designed to disseminate the HTML and PDF data posted on its web sites. The database applications are designed for various purposes, including the collection and dissemination of information. Data collected in database applications is relevant and necessary to the purpose of the application.

2) **Will the system create new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

This question is not applicable regarding the web sites. The database applications will not create new data or create previously unavailable data about an individual through aggregation from the information collected.

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

N/A, the system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

N/A, the system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

5) **How will the new data be verified for relevance and accuracy?**
N/A, the system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

6) **If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
N/A. Data is not being consolidated in this system. All database applications maintain separate database instances.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**
N/A. Processes are not consolidated in this system. All database applications maintain separate processes.

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.**
This is not applicable to the HSS web site. The database applications use various methods of retrieving and reporting data, including last names, employer/work location, and federal employee/contractor.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
This is not applicable to the HSS web site. Some database applications produce reports on individuals depending upon the functional requirements of the application. In general, the reports are used as lists to show the attendees of a conference, the people that have access to certain document sets, etc. All applications providing reports of this nature provide access controls for these reports so that the application owner or their designees have access to the information.

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)?**
This question is not applicable to the HSS web sites. In the database applications, mandatory form fields are denoted as "required". Voluntary fields may or may not be filled out at the discretion of the user. It is assumed by the information submitter that their submission will be used for the specific purpose of the application (i.e., registration for a conference). Although HSS never uses submitted data for anything other than its intended purpose, there is no documentation on any database application interface stating that fact.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) **If the system is operated at more than one site, how will consistent use of the system and data be maintained in all sites?**
The system is operated at one site (DOE HQ).

2) **What are the retention periods of data in the system?**
Retention of web site documents and information is at the discretion of the data owners and content managers. Period web site content reviews ensure that web site information is current and relevant. Retention of data in the database applications vary depending on the requirements of the application. For a conference registration system, the retention period is a few months to one year. For an document account administration system, the retention period may be several years. In all cases, data within the database applications is subject to periodic review to ensure that the data is still current and relevant.

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?**
Data maintenance and disposition for the records is conducted in accordance with the DOE Administrative Records Schedule 6: Accountable Officers Accounts Records, dated 6/17/02.

4) **Is the system using technologies in ways that the DOE has not previously employed?**
No.

5) **How does the use of this technology affect public/employee privacy?**
N/A. The system is not using technologies in ways that the DOE has not previously employed.

6) **Will this system provide the capability to identify, locate, and monitor individuals?**
No. The system will not provide the capability to identify, locate, and monitor individuals.

7) **What kinds of information are collected as a function of monitoring of individuals?**
N/A. The system is not used for monitoring individuals.

8) **What controls will be used to prevent unauthorized monitoring?**
N/A. The system will not be used for monitoring.

9) **Under which Privacy Act system of record notice does the system operate?**
The system does not currently operate under a Systems of Record notice because certain information to be maintained in the system is deemed to be sensitive under Section 208 (b)(1)(C) of the E Government Act of 2002 and not subject to (1)(B) (iii)requirements that the Privacy Impact Assessment be made publicly available through the agency web site, publication in the Federal Register, or other means. In addition, under Section 208 (b)(2)(B)(VII), a system of records is not being created under section 552a of Title 5, USC (commonly referred to as the 'Privacy Act'). Under Section 552 (a) (5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or some identifying number, symbol or other identifying particular assigned to the individual. This system will not retrieve information by the name of the individual or any other identifying number or symbol. This is **not** a system of records.

10) **If the system is being modified, will the Privacy Act system of record require amendment or revision?**
N/A.

F. ACCESS TO DATA

1) **Who will have access to the data in the system?**
The public will be able to view the information on the web sites. System Administrators and web site content managers will be able to add, revise and delete documents, reports and information on the web sites. In the database applications, the application administrators and their designees will be able to view the data in their respective applications.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Access to public web site information via HTTP is open to everyone. Access to restricted document collections is determined by the document collection owners. Processes are in place to enable timely reviews and verifications of applicant information before an account is issued. Access to database application data is determined by the application owner/administrator and is documented in the application requirements before development.

3) **Will users have access to all data on the system or will the user's access be restricted?**
Users will have access to all data on the public web sites. Access to restricted document collections and data within database applications will be restricted to account holders.

4) **What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?**
No controls are in place to prevent the misuse of data by users having access. The public may download and use any information from the public web sites. Use or misuse of the data is difficult to detect or prevent. It is assumed that account holders for restricted document collections and database applications are aware of the rules for proper use of the data.

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?**
No

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

7) **Who will be responsible for protecting the privacy rights of the employees affected by the interface?**
N/A, the system does not share data with another system.

8) **Will other agencies share data or have access to the data in the system?**
The data on the public web sites will be accessible by other agencies via HTTP. The data in restricted document collections or in database applications will not be accessible by other agencies, unless a user account is applied for and granted by the application owner.

9) **How will the data be used by the agency?**
N/A. The data on the web sites is publicly accessible, non-sensitive and non-PII in nature. The data will be used at the discretion of the agency. Use of the data in a restricted document collection or in a database application will be agreed upon prior to an access being granted.

10) **Who is responsible for assuring proper use of the data?**
N/A. The data on the public web sites is publicly accessible, non-sensitive and non-PII in nature. The use of the data is at the discretion of the user. Proper use of the data in a restricted document collection will be assured by the document collection owner or database application owner.

PIA Approval Signatures

Original copy signed and on file with the DOE Privacy Office.