Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Environmental Molecular Sciences Laboratory (EMSL) User System (ESU)
Bureau: Department of Energy (DOE)
Project's Unique ID:
Date: September 17, 2007

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Linda Connell
EMSL User System Manager
Battelle, Pacific Northwest National Laboratory
509-375-4353
linda.connell@pnl.gov

2) Who is the system owner?

Allison Campbell
Director, Environmental Molecular Sciences Laboratory
Battelle, Pacific Northwest National Laboratory
509-376-6688
allison.campbell@pnl.gov

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

Linda Connell
EMSL User System Manager
Battelle, Pacific Northwest National Laboratory
509-375-4353
linda.connell@pnl.gov

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

Andrew Korson
Security Specialist
Battelle, Pacific Northwest National Laboratory
509-372-6968
andrew.korson@pnl.gov

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

Michael Talbot
Pacific Northwest Site Office
509-372-4365
michael.talbot@pnl.gov

Abel Lopez, Director
FOIA and Privacy Act Group
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
202-586-5955
abel.lopez@hq.doe.gov

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?

The William R. Wiley Environmental Molecular Sciences Laboratory (EMSL) is a DOE national scientific user facility located at Pacific Northwest National Laboratory (PNNL) in Richland, Washington. EMSL provides integrated experimental and computational resources for discovery and technological innovation in the environmental molecular sciences to support the needs of DOE and the nation.

Users from around the world may visit the EMSL facility to use scientific instruments such as magnetic resonance instruments, mass spectrometers, spectroscopy instrumentation, and high-performance computers. Visitors are given access to EMSL and its facilities and equipment at no cost as long as they share their results in the open literature. Requests for access to EMSL start with the submission of a proposal by the individual or group who would like to use EMSL resources.

[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 EMSL User System (ESU) is a web-based system that allows the general public, scientific and engineering communities to submit proposals for access to the site to conduct experimental and theoretical molecular-level environmental studies and research using existing equipment at any of the six EMSL facilities. The six research facilities are 1) Chemistry and Physics of Complex Systems; 2) Environmental Spectroscopy and Biogeochemistry; 3) High-Field Magnetic Resonance; 4) High-Performance Mass Spectrometry; 5) Interfacial and Nanoscale Science; and 6) Molecular Science Computing.

The EUS manages the entire EMSL visit, including the proposal submission by participants throughout the world; the proposal review and approval process; the signing of non-proprietary use agreements; the identification and management of hazards; the visit to the facility; and follow-up activities such as solicitation of survey responses, requests for summaries of the science accomplished, and requests for resulting publications. Once a visit is approved, information about the visitor must be exported to other PNNL-managed systems, including the Badge Request System, used to process badges for U.S. citizens; and the Foreign National Visits/Assignment (FNVA) System, used to process and badge foreign nationals.

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.*

C. <u>DATA in the SYSTEM:</u>

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

All persons requesting to use the EMSL are listed as participants in the EUS, including both PNNL staff and members of the public.

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 from members of the public is obtained from the proposal submitted by the individual or group requesting access to the EMSL facilities for the purpose of conducting research studies. PNNL staff information is obtained by existing PNNL-owned and maintained databases.

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?

The following information is currently being collected in the EUS for all requesters: name; country of citizenship; profession; business telephone number, fax telephone number, electronic mail address; name of institution, department, address of institution, city, state/province, postal code, country.

The following additional information will be collected for all U.S. citizens listed on fully approved proposals: gender; city of birth; primary citizenship; social security number; home address and phone (for onsite visits).

Information about the visitor must be exported to other PNNL-managed systems, including the Badge Request System, used to process badges for U.S. citizens

For foreign nationals the following information will be collected: full name; also known as (AKA); gender; place of birth; city; country; date of birth; date of last visit to country of birth; passport number; passport; expiration date of passport; immigration status; type of visa and expiration date; country of current residence and how long at current residence; language interpretation needs, work phone; electronic mail address and fax telephone number; name of current employer; place of work, street, city state, zip code, country; position title or description requesters duties.

The information collected from foreign nationals includes all currently required data in the Foreign National Visits/Assignment (FNVA) System. This information will be removed from the EUS after being transferred to the FNVA System.

3) Accuracy, Timeliness, and Reliability

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

Follow-up contacts are made with all participants via electronic mail and telephone numbers submitted, thus validating contact information. Participants are required to submit proper identification when they come to EMSL before receiving a badge for access to the facilities. Background checks on foreign nations are managed by the PNNL Foreign National Visitors' Office. The information collected from foreign nationals will be electronically transmitted to that office for validation.

b. How will data be checked for completeness?

Validation is implemented on all required input fields. Required information is identified on each web page, and the proposal will not be successfully submitted until all required information is completed and correctly formatted. Missing or incorrectly formatted data is identified for the participant on failed submissions.

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

EMSL proposals and its data are reviewed and extended each year by EMSL administrative staff. Each proposal submitted by the requester has a maximum 3-year duration, but many are shorter. If a participant would like to continue using the EMSL facilities a new proposal must be submitted once an existing proposal has expired.

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

A data dictionary was developed when the EUS was first implemented. A database schema is available that shows database structure and data elements. A configuration document further describes the use of the data in the EUS system, including the databases used and how they are accessed.

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, the data is both relevant and necessary to have access to EMSL facilities and equipment.

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?

No new data will be derived.

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

No new data will be derived.

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?

N/A. The 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?

N/A. 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.

Yes, personal identifiers are used. The EUS database creates and uses a unique identifier for each EMSL user. Since EMSL visitors often return, the identifier is used to track that visitor's information for subsequent visits.

A second unique identifier, called a Hanford identifier (Hanford ID), is maintained in some of the PNNL business systems. PNNL is located adjacent to the Hanford site, which involves other DOE contractors. The Hanford ID is an identifier historically shared by all contractor employees to identify anyone visiting the Hanford site. Since visitors often come to Hanford and PNNL for different reasons and for multiple visits, the Hanford ID is used to facilitate subsequent visits and badging for these visitors. It also is used in PNNL-managed training applications to verify a visitor has received the proper training required for each visit.

A visitor's own data is available to them (the originator of this data). To access their own data, they must log into the EUS using their email address and a password they are asked to create. Thus, their email address and password together form a unique identifier that is stored in the EUS database. The personal data is accessible only by the visitor (the originator of the data) and is provided over a secure network using HTTPS protocol.

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

Reports containing participant information can be created internally by EMSL and PNNL staff; however, none of the newly proposed information will be included in these reports. The reports provide demographic information about visitors coming to EMSL. Some reports provide statistical information, such as how many visitors used EMSL in a given time period.

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)?

EMSL proposal submission is a voluntary process and the information is necessary for access to EMSL facilities and equipment. There is a Security and Privacy link on the EUS home page identifying visitor rights and stating that the data collected is for the sole stated purpose. Once a proposal is fully approved, all participants will receive by electronic mail a link to the EUS where the additional information identified in Section C.2e will be collected. The electronic mail will explain that the individual may alternatively submit this information via the existing procedure which involves completion of a hard-copy form that is faxed back to EMSL administrative staff.

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 only being operated at the EMSL facility.

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

The duration of an EMSL proposal ranges from 1 month to 3 years. When a proposal has expired, the information about that proposal and its corresponding visitors will be entered into EMSL's Records Inventory and Disposition (RIDS) system under disposal authority N1-434-96-9.1A2. Under this authority, records are retained for at least 25 years.

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?

PNNL records disposition scheduling follows schedules identified in the following sources: Disposition of Federal Records: A Records Management Handbook http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/index.html and NARA Schedules http://www.archives.gov/records-mgmt/ardor/records-schedules.html.

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 The system does not use technology in new ways that affect public/employee privacy.

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 No monitoring is being done.

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

N/A

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

In accordance with clause H-15 of the PNNL contract (DE-AC05-76RL01830), portions of the system collect data that is exported to the Foreign Information system of records DOE-52 "Access Control Records of International Visits, Assignments, and Employment at DOE facilities and Contractor Sites." These data records are disposed after they are transferred to the Foreign Information system of record. Information on U.S. citizens is maintained in DOE-43 "Personnel Security Files."

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

No, the systems of records are not being amended or modified.

F. Access to Data:

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

Participants and only a small set of developers, system administrators and PNNL staff will have access to the data. Peer reviewers have access to general information about participants listed on the proposal they are reviewing. This information is limited to the name of the participant, country of citizenship, profession, business information and information about the institution they are affiliated with.

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

Data is accessed only through a password-protected web-based application. External users (i.e., users that are not PNNL staff) log into the application using their electronic mail address and unique, user-generated password. PNNL staff log into the application using their PNNL credentials, which are also used to log into the PNNL network.

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

Participants will only have access to their own submitted data. The PNNL staff is granted access based on their role in processing the visitor. The data accessed by PNNL staff is restricted based on job function. This restriction is enforced by role-based access managed by the application.

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

All access to data is password protected. External users receive a temporary password via email. The temporary password and the user's email are used to access a web form which requires them to create a permanent, user-generated password. The PNNL staff credentials (user name and password) are maintained by PNNL. These passwords are changed frequently and have strict security policies.

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?**

Yes, PNNL staff will be involved with the design, development, and maintenance of the system. Individuals provided this access are subject to applicable requirements of the PNNL Contract DE-AC05-76RL01830, internal PNNL operating procedures regarding the protection of sensitive unclassified information and records, and the 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 they may obtain in accordance with the provisions of the Privacy Act and the requirements of DOE. The contractor shall ensure that all PPNL 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.**

U.S. citizen participant information will be exported to the PNNL Badge Request System. Foreign national participant information will be exported to the PNNL Foreign National Visit/Assignment (FNVA) business system. Both the Badge Request and FNVA Systems are located inside the PNNL network and are not externally accessible.

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

Responsibility for privacy rights of participants will be shared by:

Allison Campbell, EMSL Director
Nancy Foster-Mills, EMSL User Administration Office Manager
Linda Connell, EUS System Manager

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

The Following Officials Have Approved this Document

1) System Owner

(Signature) 9/20/07 (Date)

Name: Alison Campbell

Title: EMSL Director

2) System Manager

Linda Connell (Signature) 9/20/07 (Date)

Name: Linda Connell

Title: Technical Group Manager

3) Privacy Act Officer

(Signature) 9/28/07 (Date)

Name: Abel Lopez

Title: Director, Freedom of Information Act and Privacy Act Officer

4) Senior Agency Official for Privacy

(Signature) 9-28-07 (Date)

Name: Ingrid A.C. Kolb

Title: Senior Agency Official for Privacy