Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Business Management System (BMS) - RL-2007/Project Hanford Management Contract - PHMC (Fluor)
Bureau: U.S. Department of Energy (DOE)
Project's Unique ID: Business Management System (BMS) as part of OMB Exhibit 300 Identification number: 019-10-01-15-01-1061-00 (RL PHMC - Business Management System (BMS))
Date: August 28, 2007

A. CONTACT INFORMATION:

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

   Pamela R. Edwards
   Information Services
   Fluor Hanford
   P.O. Box 1000 MSIN H7-22
   Richland, WA 99352

2. **Who is the system owner?**

   Dana Kranz
   Chief Information Officer
   U.S. Department of Energy
   Richland Operations Office
   P.O. Box 550 MSIN A2-15
   Richland, WA 99352
   509-376-7594

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 MSIN A2-15
   Richland, WA 99352
   509-376-7594

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 MSIN A6-35

Richland, WA 99352
509-376-2347

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 MSIN A7-75
Richland, WA 99352
509-376-6288

Abel Lopez, Director
FOIA/Privacy Act Group
U.S. Department of Energy
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?** Business Management Systems (BMS) is an integrated business set of modules that manage the following business functions: payroll, human resources, pension, benefits, training, and reporting.

3) **What legal authority authorizes the purchase or development of this system/application?** 42, United States Code (U.S.C.), Section 7101 *et seq.*, and 50 U.S.C. 2401 *et seq.*, the Memorandum of Understanding between the Department of Energy and the Department of Health and Human Services, 56 FR 9701, March 7, 1991, Nuclear Waste Policy Act of 1982 Public Law (Pub.

[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).

L.) 97-425); Nuclear Waste Policy Amendment Act of 1987 Pub. L. 100-203, Government Employees Training Act of 1958, and Title 5, Code of Federal Regulations (CFR) Parts 410 and 412.

C. DATA in the SYSTEM:

1) **What categories of individuals are covered in the system?** Federal and contractor employees, subcontractors, dependents, beneficiaries, and persons requiring training at the Hanford site.

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

   a. **Is the source of information from the individual or is it taken from another source?** The source of data is from the individual to whom it pertains.

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

   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 employee and the public?** Name, social security number, date of birth, and bank account numbers.

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 it is provided. Appropriate legal documents are required when information is initiated or updated. Verification with other applications that collect equivalent information is done on a daily basis.

   b. **How will data be checked for completeness?** Since the data is provided by the individual to whom it pertains, it is determined that the information is completed at the time it is provided. Appropriate legal documents are required when information is initiated or updated. Verification with other applications that collect equivalent information is done on a daily basis.

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

information is current and not out-of-date at the time it is provided. Persons are given the opportunity to update the information that may change with online access or by form. Verification with other applications that collect equivalent information is done on a daily basis.

d. **Are the data elements described in detail and documented?** Yes. The data elements are described in the data schema and Commercial-Off-The-Shelf (COTS) software 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?** 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/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?** No, 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

8) **How will the 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, social security number and internal system identifiers.

9) **What kinds of reports can be produced on individuals?** Recurring reports are generated as a matter of routine business. The authorized user can generate a variety of reports that are used in the conduct of business. Reports may be generated about the individual for training or retiree purposes.

   What will be the use of these reports? Reports will be used to conduct necessary business.

Who will have access to them? Only authorized personnel have access to the reports.

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 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 be maintained in all sites?** The system is not operated in more than one site.

2) **What are the retention periods of data in this system?** Records retention and disposal authorities are contained in the National Archives and Records Administration (NARA) General Records Schedule and DOE record 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 the Records Schedule and established in accordance with NARA General Records Schedule.

4) **Is the system using technologies in ways that the 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 these systems 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-5 "Personnel Records of Former Contractor Employees." and DOE-28 "General Training Records".

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 management. Application and data access is controlled first via a network access logon id and complex password. The majority of software applications have secondary authentication and access controls implemented including role based security controls that require management approval prior to granting. Direct database access is controlled administratively through policy and through reviews of access control lists by management.
Routine uses of records are:

a. A record from this system may be disclosed as routine use to DOE contractors for performance of their contracts.

b. A record from this system may be disclosed as a routine use to Department of Energy or contractors for security clearance.

c. A record from this system may be disclosed to sub-contractors responsible for providing retiree benefits.

2) **How is access to the data by a user determined?** Access is governed on a need-to-know basis approved by the employee manager via a signed access request form.

3) **Will users have access to all data on the system or will the user's access be restricted?** Access is role dependent, as authorized by the job function and approved by management.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** Administrative (procedure), authentication policy, and physical controls are implemented to prevent misuse. Role based access control, management approvals, and audits assist in providing multiple layers of protection.

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 PA contract clauses inserted in their contracts and other regulatory measures addressed?** Yes. Information may be disclosed to contractors and their officers and employees in performance of their contract. Individuals provided this information are subject to the same limitation 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 and the requirements of the DOE Richland Office. The contractor shall ensure that all DOE Richland Office documents and software processed, and the information contained therein, are protect for unauthorized use and mishandling by assigned personnel. All authorized users are required to sign annual non-disclosure agreements.

6) **Do other systems share data or have access to the data in the system? If yes, explain.** Yes. The system interfaces are documented in interface agreements and specification documents. All interfaces documented in Memorandums of Understandings or are required to sign annual non-disclosure agreements. Interfaces include:

    a. Hanford PeopleCORE (HPC) for internal Hanford roster;

    b. Personnel Security Clearance Record (PSCR+) for badge security;

    c. Access Control Entry System (ACES) for Hanford site access; and

    d. Benefits sub-contractors for benefits administration

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

    Gary Loiacono, Director
    Security and Emergency Services Division
    U.S. Department of Energy
    Richland Operations Office
    P.O. Box 550 MSIN A6-35
    Richland, WA 99352

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 Manager**

Harry E Bell (Signature) 8/28/07 (Date)
Name: for Dana Kranz
Title: RL Chief Information Officer

2. **Privacy Act Officer (Field Office)**

(Signature) 8/28/07 (Date)
Name:
Title: Dorothy Fiehle, RL and PA Officer

3. **Privacy Act Officer (Headquarters)**

Abel Lopez (Signature) 9/6/07 (Date)
Name: Abel Lopez
Title: Director, FOIA and Privacy Act Group

4. **Senior Official for Privacy Policy**

Ingrid A.C. Kolb (Signature) 9-7-07 (Date)
Name: Ingrid A.C. Kolb
Title: Director, Office of Management