Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: NREL Business Systems Enclave
Bureau: U.S. Department of Energy - National Renewable Energy Laboratory, Golden, CO
Project Unique ID:
Date: May 19, 2008

A. CONTACT INFORMATION

1. Who is the person completing this document?

Barbara Stokes, Director, NREL Finance Office, (303)275-4555

2. Who is the system owner?

Barbara Stokes, NREL, Director, Finance Office, is the designated steward of the Business Systems Enclave.

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

Chuck Powers, NREL, Manager, Infrastructure and Operations Group (303) 275-4182 and Marsha Warden, NREL, Manager, Business Technology Solutions Group, (303)275-4056

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

Todd Borandi, NREL, Manager, Cyber Security (303)-275-3625

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

Anna Martinez-Barnish, Privacy Act Officer, Golden Field Office

B. SYSTEM APPLICATION/GENERAL INFORMATION

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, information about sole proprietor vendors is maintained.

c. Is the information about DOE or contractor employees?

Yes, NREL stores information about employees and other workers.

2. What is the purpose of the system/application?

The Business Systems Enclave houses our enterprise business systems, Oracle, Hyperion, data warehousing applications and other business software and analysis tools that enable NREL to operate its business. The Business Systems Enclave contains the personal identifiable information for our workforce population as well as financial, procurement and asset records.

As a result of collecting and maintaining this information within the Business Systems Enclave, NREL is able to process and report financial transactions, produce payroll, provide employee benefits including retirement savings plans and insurances, manage financial and staff resources, contract with and procure goods and services from outside contractors and independent consultants, manage assets and inventories, and meet other NREL business and Human Resource regulatory and reporting requirements.

3. What legal authority authorizes the purchase or development of this system/application?

NREL is operated by Midwest Research Institute under U.S. Department of Energy Contract Prime Contract No. DE-AC36-99GO10337. All information included in the Business Systems Enclave is required under the performance of this contract.

C. DATA IN THE SYSTEM

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

The Business Systems Enclave includes NREL employees, contract workers, other workers, and vendors.

2. What are the sources of information in the system?

Employment applications and other new hire information collection forms, site access requests, IRS forms W-4 and W-9

a. Is the source of the information from the individual or is it taken from another source?

The source of information is from the individual.

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

Not applicable.

c. What tribal, state, and local agencies are providing data for use in the system?

Not applicable.

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

Kenexa, an application service provider, manages our employee recruitment processes and employee applicant flow. The public (applicants) have the ability to create an account, submit their resume/credentials electronically for consideration, as well as complete required on-line forms to provide necessary PII information to finalize the hiring process when identified as the applicant selected for hire.

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

Information collected includes social security numbers, home addresses, emergency contact information, personal bank account information, employment history, date of birth and place of birth.

3. Accuracy, Timeliness, and Reliability

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

Social security numbers are verified through the Social Security Administration employer's secure web site.

b. How will data be checked for completeness?

NREL administrative staff verifies completeness through a review process.

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

Employees and other workers validate data through various reports, including 1099s, W-2s, management information notices, personnel information notices, and electronic notices for the electronic deposit of payroll and expense reimbursements.

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

Yes.

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?

Not applicable.

4. Can the system make determinations about employees/the 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 are being consolidated, what controls are in place to protect the data from unauthorized access or use?

Not applicable.

7. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?

Not applicable.

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 social security number, name and the NREL employee/vendor identification number are used to retrieve data from the Business Systems Enclave. Employee information is retrieved through system access as requested by an appropriate organization manager. Access is granted by a trained system administrator after review of internal controls.

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

Employee reports include:

- Management information notices and personnel information notices provided to line managers and employees to communicate compensation, position and employment status and revisions.
- IRS Form W-2s provided to the IRS and states for income tax reporting.
- Employment tax reports provided to the IRS and states as required by federal, state and local authorities.
- Compensation and benefits statements provided to employees for informational purposes.
- Annual retirement information provided to employees for informational purposes.

Vendor reports include:

- IRS Form 1099 provided to the IRS and states as required to report taxable amounts on an annual basis

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.

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?

Not applicable.

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

Database information is retained on the system indefinitely as there is no purging capability within the applications to remove data, however, system backup tapes are cleared every 180 days.

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?

Storage devices with electronic data containing PII that have been retired and taken out of service will either be re-imaged or cleared to ensure the removal of all PII information before reuse of the device. If the device is to be destroyed, it is put into the approved NREL electronic device shredder.

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. The Business Systems Enclave is access controlled and does not affect 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?

None.

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

Access control is based on a need to know basis. Policy and confidentiality agreements are in place.

9. Under which PA system of records notice does the system operate?

Not applicable.

10. If the system is being modified, will the PA system of records notice require amendment or revision?

Not applicable.

F. ACCESS TO DATA

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

Access to authorized Business System Enclave functional users, data base administrators, and system administrators is based on the user's roles and responsibilities. Access is reviewed by an independent NREL organization on a periodic basis. Information is also transmitted from the Business Systems Enclave to and from the NREL's third-party payroll provider, Ceridian, through a secure system interface which is encrypted via SSL.

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

Access to the Business Systems Enclave is requested through a formal request from an authorized NREL organizational manager, with access granted by an independent NREL system administrator.

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

Business Systems Enclave access is granted with various levels of functional abilities based on the user's role via an approved request by the user's organizational manager.

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

Access to the Business Systems Enclave is restricted to user function. Training is provided annually for all users, including physical and cyber security, annual privacy statements are signed by individuals with system access.

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 included in their contracts and other regulatory measures addressed?

Yes, contracts include provisions related to information security.

6. Do other systems share data or have access to the data in the system? If yes, explain.

No.

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

Barbara Stokes, Chuck Powers, Marsha Warden.

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?

Data is provided to the Internal Revenue Service, the Social Security Administration and various state and local agencies for income tax reporting purposes; and to insurance, pension and retirement benefit providers for administrative purposes.

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

Barbara Stokes is the designated steward of the Business Systems Enclave.

PIA Approval Signatures

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