Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: eTrack
Bureau: Department of Energy
Project's Unique ID: eTrack
Date: August 6, 2008

A. CONTACT INFORMATION:

1) Who is the person completing this document?
Name: Pam Gunter
Title: Technical Lead
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7022
         Oak Ridge, TN. 37831-7022

2) Who is the system owner?
Name: Kathryn McKay
Title: Functional Lead
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1310-FA, MS 7021
         Oak Ridge, TN. 37831-7021

3) Who is the system manager for this system or application?
Name: David D. Newton
Title: Applications Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7022
         Oak Ridge, TN. 37831-7022

4) Who is the IT Security Manager who reviewed this document?
Name: David Rose
Title: Cyber Security & Compliance Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1007, MS 7022
         Oak Ridge, TN. 37831-7022

5) Who is the Privacy Act Officer who reviewed this document?
Name: Amy Rothrock
Title: Privacy Act Officer
Organization: Department of Energy/Oak Ridge Operations
Address: 200 Administration Rd.
         Oak Ridge, TN. 37830

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 eTrack application is Bechtel's corporate time-and-attendance software for jobsites. eTrack is used to collect and document site attendance data, track employee data, prepare daily timesheets, export payroll files to payroll applications (like Timberline and MicroPayroll), and create reports and export files for all time-and-attendance retained data.

3) What legal authority authorizes the purchase or development of this system/application?
Department of Energy

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?
Contractor and former contractor (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?
    Some data comes directly from individuals and some information comes from other applications within the boundary. Timekeeper manually enters employee information based on I9s, W4s and direct-hire sheets (all completed prior to hire-in). There is a direct feed for additional information from HR to include DOB, Clearance Level, Race. Prox card numbers and badge #s are entered when the record is created.

    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?
This application collects (from employees) the following:
SSN, date of birth, med history (maintained by medical department), employment history (maintained by HR), bank account numbers (maintained by Payroll), security clearance history (maintained by Wackenhut). No information from any public record is received.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?
BJC functional personnel have processes in place to ensure accuracy of the data. SSNs are bumped to the IRS annually by the CFO Organization.

b. How will data be checked for completeness?
BJC applications require a complete set of data for processing purposes. Procedures and processes are in place to ensure the completeness of the data. All information required from the employee has to be complete in order for payroll to function and for a salary to be distributed to the employee.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?
BJC organization (CFO and HR) personnel have processes and procedures in place to ensure the accuracy of the data. Employees are responsible for reporting any changes to personal records such as addresses, phone numbers, last name, etc. HR maintains a Human Resource Information System that records current data. Payroll verifies changes through HRIS.

d. Are the data elements described in detail and documented? Yes,
Change of address: BJCF-47
Change of name: BJCF-144

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? N/A

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 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.
eTrack System Administrators and Timekeepers can retrieve and modify data via the current eTrack application. Data can be retrieved by name, badge #, Prox #, or etrack#.

9) What kinds of reports can be produced on individuals?
Numerous business-related reports are available with information about individuals (employees and subcontractors). Reports are not available for subcontractors. For BJC, all time-related reports can be generated to include times in and out, location of crew, crew ID, badge #s, Prox card #s, etc . Clearance levels, SSN, hire dates, addresses, county, and race.

What will be the use of these reports?
Reports are used for the business of the BJC (CFO, HR, EEO) Personal information such as SSN, Hire Date also available and used primarily for termination use. For EEO information, addresses, county, and race are often required.

Who will have access to them?
Reports are available to functional staff (Timekeepers, HR, Payroll) as needed to perform their job.

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)?
Individuals are not required to provide their home phone numbers but must supply a contact number (cell phone or otherwise) for emergency situation.

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 applications do not cross Accreditation Boundaries.

2) **What are the retention periods of data in the system?**
Indefinitely – production databases considered live.

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?**
Disposition of the data for the BJC D&D Contract will occur at the end of the contract. At that time, data will be turned over to DOE or designated Contractor. Data will be archived or deleted at the end of the contract based on DOE guidelines for retaining records.

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

6) **Will this system provide the capability to identify, locate, and monitor individuals?**
Yes, it identifies the employee by badge # and Prox card #, crew ID, shift, location, time and attendance.

7) **What kinds of information are collected as a function of the monitoring of individuals?**
Time and attendance, crew ID, location.

8) **What controls will be used to prevent unauthorized monitoring?**
No monitoring is possible outside of normal applications usage.

9) **Under which Privacy Act system of records notice does the system operate?** N/A

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

F. Access to Data:

1) Who will have access to the data in the system?
Access to data is controlled by the applications administrators for each application.

2) How is access to the data by a user determined?
Access to data is approved by the application owners and granted by the application administrator on a need-to-know basis.

3) Will users have access to all data on the system or will the user's access be restricted?
User access is controlled by the system administrators by granting roles to individuals. Roles are restricted to see only the functionality/data required by that role.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?
Application owners enforce separation of responsibilities to only allow access to functionality/data necessary to perform job functions.

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, DOE Privacy Act clauses are included.

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?
Any applications that process Privacy Act data are classified as "Protected" by the BJC Cyber Security Manager. Those applications then document and test the controls necessary to protect the interfaces/data.

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.

PIA Approval Signatures

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