Section I

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: ETTP Security Access Control System
Bureau: Department of Energy
Project's Unique ID: ESACS
Date: August 6, 2008

A. CONTACT INFORMATION:

1) Who is the person completing this document?
Name: Lynn Harder
Title: Senior Applications Programmer
Organization: Software Control International
Address: P.O Box 4699, Building 1007, MS 7022
Oak Ridge, TN. 37831-7022

2) Who is the system owner?
Name: Douglas Brown
Title: Security Systems Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1652, MS 7350
Oak Ridge, TN. 37831-7350

3) Who is the system manager for this system or application?
Name: Douglas Brown
Title: Security Systems Manager
Organization: Bechtel Jacobs Company LLC
Address: P.O Box 4699, Building 1652, MS 7350
Oak Ridge, TN. 37831-7350

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 ESACS application is an access control system to control and authorize access to security areas at ETTP. The system is required by DOE Order M473.1-1. Use of the information provides a unique methodology of differentiating between individuals with similar names.

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?
Federal (DOE), prime contractor (BJC), other prime contractors (Y-12, ORNL, Paducah, etc.), subcontractors, and 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?
Some data comes directly from individuals and some information comes from other applications within the boundary.

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

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

c. What information will be collected from the individual and the public?
This application collects (from employees) the following: SSN and Date of Birth

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOE records be verified for accuracy?
BJC Security and Emergency Management personnel have processes in place to ensure accuracy of the data.

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.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date?
Yes, BJC Security and Emergency Management personnel have processes and procedures in place to ensure the accuracy of the data.

d. Are the data elements described in detail and documented?
Data is provided by the person being enrolled. That information is gathered either directly from the individual or from a Badge Request form submitted by the individual's employer. Any errors that could exist in ESACS are due to human error during the enrollment process or incorrect information provided by the individual or by the employer. Every effort that is available to the enrollment personnel is taken to ensure the data inputted into ESACS is correct. The Clearance Office also performs a quality assurance review of the data when updating an individual's clearance information.

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, required by DOE Order M473.1-1.

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.
Data can be retrieved by any badge record attribute stored in the system.

9) What kinds of reports can be produced on individuals?
Numerous business-related reports are available with information about individuals (employees and subcontractors). Generally, the reports do not include privacy information.

What will be the use of these reports?
Reports are used for the business of the BJC Security and Emergency Management Organization.

Who will have access to them?
Reports are available to certain security staff personnel on an as-need 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?
The applications do not cross Accreditation Boundaries.

2) What are the retention periods of data in the system?
Seventy (70) 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?**

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. Currently reports are maintained only as long as the information is required.

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?**

No. The system authorizes access into security areas.

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?**

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. System manager, administrators, and operators have access to the system.

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.
Yes. The data is dumped nightly to three servers: bjcprod1prod, bjcprod1qa, and udbdev01bjcd. GLINES, HRIS, and UCAMS have access to data required by their system.

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.