Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: SEC-2
Bureau: US Department of Energy (DOE)
Project Unique ID: DOE-ID Security clearance work tracking and budget system.
Date: April 4, 2008

A. CONTACT INFORMATION

1. **Who is the person completing this document?**
Name: Jeffrey R. Lascheid
Title: Program Manager
Organization: Westech International, Inc.
Address: 1955 N. Fremont Ave, MS 1170
Idaho Falls, ID 83415

2. **Who is the system owner?**
Name: M. Christine Ott, Chief Information Officer
US DOE, Idaho Operations Office
DOE-ID Security and Emergency Management Division
Address: 1955 N Fremont Ave, MS 1170
Idaho Falls ID 83415

3. **Who is the system manager for this system or application?**
Name: Robert L. Green, Director
Security and Emergency Management Division
Address: 1955 N Fremont Ave, MS 1203
Idaho Falls ID 83415

4. **Who is the IT Security Manager who reviewed this document?**
Name: Randall Lillie
US Department of Energy
Address: 1955 N Fremont Ave, MS 1240
Idaho Falls ID 83415

5. **Who is the Privacy Act Officer who reviewed this document?**
Name: Nicole Brooks
Title: Privacy Act Officer
US Department of Energy
Address: 1955 N Fremont Ave, MS 1203
Idaho Falls ID 83415

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 SEC2 application is used to track security clearance work tracking, clearance status and budgets for the Idaho Operations Office.

3. **What legal authority authorizes the purchase or development of this system/application?** 42 U.S.C. 7107 *et seq.*, and 50 U.S.C. 2401 *et seq.*

C. DATA IN THE SYSTEM

1. **What categories of individuals are covered in the system?** Persons holding or applying for a DOE security clearance at the Idaho Site. Includes former clearance holders and applicants.

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?** The source of the data is from the individual, outside investigative sources (such as the Office of Personnel Management (OPM) or the FBI), or internal inquiries conducted by the Idaho National Laboratory (INL).

   b. **What Federal agencies are providing data for use in the system?** DOE-ID, INL, OPM, FBI, or other investigative agencies, as appropriate. The US State Department may provide data from foreign countries.

   c. **What tribal, state, and local agencies are providing data for use in the system?** Local data is usually obtained by the OPM or the FBI and provided to DOE. However, local law enforcement provides additional data, as requested by the DOE-ID personnel security organization. This data may be directly obtained from any Federal, state, local or tribal law enforcement agency or court in the United States.

[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).

d. **From what other third party sources will data be collected?** None.

e. **What information will be collected from the individual and the public?** Name, address, telephone numbers, social security number, place and date of birth, relative information, criminal history, credit history, personal history, employment history, security clearance history (including special access history), drug use history, medical/psychological history.

3. **Accuracy, Timeliness, and Reliability**

a. **How will data collected from sources other than DOE records be verified for accuracy?** Much of the information will be collected from the individual, and is determined to be accurate when the information is provided. Information is also obtained from investigative sources such as the OPM or the FBI, and is determined to be accurate when provided by the agency.

b. **How will data be checked for completeness?** Since the data is provided by the individual or authorized Federal investigative agencies, it is deemed complete at the time it is provided.

c. **Are the data current? What steps or procedures are taken to ensure the data are current and not out-of-date?** Since the data is provided by the individual or authorized Federal investigative agencies, it is deemed complete at the time it is provided.

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?** Yes.

3. **Will the new data be placed in the individual's record?** Yes.

4. **Can the system make determinations about employees/the public that would not be possible without the new data?** No.

5. **How will the new data be verified for relevance and accuracy?** The information will be collected from authorized investigative agencies, and aggregated by an authorized personnel security employee. The information is deemed to be accurate when provided by the agency. Relevance is determined via the clearance adjudication process.

6. **If the data are being consolidated, what controls are in place to protect the data from unauthorized access or use?** Only authorized individuals are allowed access to the data. Access is controlled by user names and passwords. Access can only be gained within the INL computing network. There is no external access to the data permitted.

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

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 data will be retrieved by the name, social security number, or the DOE clearance identifying number.

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 are created as needed by the data users. Information in the report may include identifying information, adjudicative information, or historical information of any data collected or maintained on the individual.

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)?** An individual may decline to provide any information requested by DOE. The information contained in the database is Official Use Only, and may not be released without review by a Privacy Act Officer, a DOE Classification Officer, or Derivative Classifier.

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?** N/A. The data is not used by other sites.

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

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.

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-43

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 have access to this system. In addition, individuals who have access to this system all hold a current DOE security clearance. Application data access is controlled via network logon ID and complex password. Additional software authentication is required with logon ID and a complex password. Direct database access is limited through policy and through reviews of access control lists by management.

2. **How is access to the data by a user determined?** Access is governed by a need-to-know basis as verified by the approving manager.

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 approving manager.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** Procedural and physical controls are implemented to prevent misuse. Role based access control and management approvals assist in 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 included in their contracts and other regulatory measures addressed?** Yes, contractors are involved in the design, development and maintenance of the system. 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 of 1974, 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 documents and software process, 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.** No.

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

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

(Signature) 5/13/08 (Date)
Name: Robert L. Green
Title: Director, Security and Emergency Management Division, DOE-ID

2. Privacy Act Officer (Field Office)

Nicole Brooks (Signature) 5/13/08 (Date)
Name: Nicole Brooks
Title: Privacy Act Officer, DOE-ID

3. Privacy Act Officer (Headquarters)

(Signature) 6/12/08 (Date)
Name: Kevin Hagerty
Title: Director, FOIA and Privacy Act Group

4. Senior Official for Privacy Policy

Ingrid Kolb (Signature) 6-13-08 (Date)
Name: Ingrid A.C. Kolb
Title: Director, Office of Management