

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: Oak Ridge Office Safeguards and Security Clearance Tracking System (SAS) and Visitor Control System (VISCON)
Bureau: Department of Energy (DOE)
Project's Unique ID: 019-60-02-00-01-5000-04-139
Date: September 5, 2007

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Samuel Mashburn
Information Technology Support Services Contractor
U.S. Department of Energy
Oak Ridge Operations Office
200 Administration Road
Oak Ridge, TN, 37830
865-576-2594

2) Who is the system owner?

Diane Patterson, Chief,
Access Authorization Branch
U.S. Department of Energy
Oak Ridge Operations Office
200 Administration Road
Oak Ridge, TN 37830
865-576-0925

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

Gwen Senviel
Information Resources Management Division
Oak Ridge Operations Office
U.S. Department of Energy
200 Administration Road
Oak Ridge, TN 37830
865-576-3331

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

Qui Nguyen, OS-203
Materials Control and Accountability
and Information Security Team
U.S. Department of Energy
200 Administration Road
Oak Ridge, TN 37830
865-576-1600

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

Amy Rothrock
Office of Chief Counsel
U.S. Department of Energy,
200 Administration Road
Oak Ridge, TN 37830
865-576-1216

Abel Lopez, Director
FOIA and Privacy Act Group
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585
202-586-5955

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.

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).

c. Is the information about DOE or contractor employees?

Yes.

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

The purpose of the system is to use and maintain records by the DOE ORO as an official record of all information gathered and evaluated to determine an individual's initial and continued DOE ORO access authorization eligibility and, if applicable, an individual's eligibility for participation in DOE ORO sensitive activities or for access to Sensitive Compartmented Information.

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

Title 42, United States Code (U.S.C.), Section 7101 *et. seq.*; 50 U.S.C. 2401; Title 10, Code of Federal Regulations (CFR), Part 710, subparts A and B; Executive Orders (E.O.) 10450 and 12968; 5 CFR Part 732; DOE Order 470.4 "Safeguards and Security Program dated August 26, 2005; Personnel Security Manual DOE M 470.4-5 dated August 26, 2005; and Director of Central Intelligence Directive 1/14 dated January 22, 1992.

C. DATA IN THE SYSTEM:

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

Applicants for DOE ORO employment; DOE employees, including assignees and detailees, agents and consultants with the DOE ORO, DOE contractors and subcontractors; DOE access permittees processed for DOE ORO access authorizations to classified matter or special nuclear matters; other Federal agency contractor and subcontractor applicants for employment, and their employees, detailees, agents and consultants processed for DOE ORO access authorizations; and other individuals processed for DOE access authorizations as determined by the Secretary.

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 information is obtained from the applicant. Additional information is obtained during the investigation and adjudication processes by Investigative and Personnel Security staff.

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

Investigative information is provided by the U.S. Office of Personnel Management (OPM) and the Federal Bureau of Investigation (FBI).

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?

Name, social security number, date of birth and employer information is collected from the applicant.

3) Accuracy, Timeliness, and Reliability

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

Investigation results are subject to a rigorous adjudication process before a clearance is granted or denied. Employees are provided the chance to address questions that arise from the investigation.

b. How will data be checked for completeness?

Validation routines in the system software applications ensure that data is complete and non-contradictory.

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

Yes. The data is current and updated daily with any changes, whether employee initiated or via request from other DOE sources.

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

Yes, data elements are described in the data dictionary.

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, the data is necessary to maintain adequate personnel security, including an accurate database of security clearances.

- 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 is retrieved by the name of the individual, social security number, and badge number assigned to each applicant.

- 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 identify data associated with the individual's DOE access authorization and may include personal information. Access to these reports is restricted to appropriately cleared (i.e., Q-cleared) DOE and contractor personnel working in direct support of personnel security activities. The reports are used to aid the timely processing and management of DOE clearances.

- 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 data is required for clearance processing. The individual provides the information 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 used only within the DOE ORO IRMD Enclave General Support Services (GSS) boundaries.

- 2) **What are the retention periods of data in the system?**

Data retention procedures are in accordance with DOE Administrative Records Schedule N1-434-98-21 "Security, Emergency Planning and Safety Records." This information can be obtained at <http://cio.energy.gov/records-management/adminrs.htm>.

- 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?**

Data disposition procedures are in accordance with DOE Administrative Records Schedule N1-434-98-21 "Security, Emergency Planning and Safety Records." This information can be obtained at <http://cio.energy.gov/records-management/adminrs.htm>.

- 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?

N/A

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?

The system is subject to the functional and administrative controls for the Information Resource Management Division (IRMD) Enclave. The IRMD Enclave is classified as "Moderate" according to the Federal Information Security Management Act (FISMA) and has the appropriate controls to identify and stop misuse of the systems within it. The system limits access to the documents based on functional roles and user identification. No user is permitted access to the documents for monitoring purposes.

9) Under which Privacy Act system of records notice does the system operate?

DOE-43 "Personnel Security Files" and DOE-46 "Administrative Review Files."

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

No.

F. ACCESS TO DATA:

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

Restricted access is granted only to users and their managers. System administrators have full access.

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

Roles with degrees of access are determined by the system owner. Procedures, controls and responsibilities for assigning system access are documented.

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

Access is restricted by predefined user roles. The ORO SAS system has a role based security process that is connected to each user account. A user must be granted permissions to view documents by group. The account structure that implements the system has been designed to limit access to a site or site module by group and or through a direct account. No personally identifiable information data can be seen, accessed, or modifiable without explicit permissions of the Group Administrator for that site or module. To modify a user's permissions, the group must submit a helpdesk request to the system administrator through the ORO Helpdesk. The system owner must provide prior approval for any new accounts or deletions.

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

Application user roles limit access by users to the minimal subset of data that is required for their positions. Database audit tables log all users actions and data changes to help ensure data integrity.

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. Contractors were involved with the design and development of the system and will be involved with the 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, 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 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 DOE ORO documents and software

processed, 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 other systems share the system data.

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?

Clearance request data is shared with the appropriate investigating agency.

9) How will the data be used by the other agency?

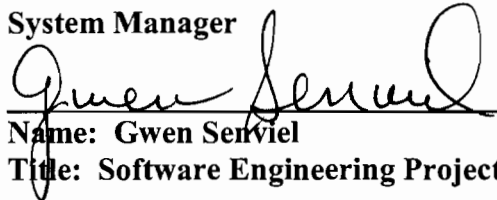
The data is used to determine the level of an employee's access to sensitive or classified data. Clearance request data is used to determine if an applicant is suitable for such access.

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

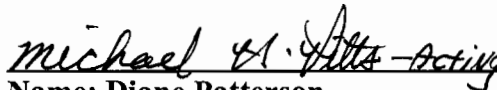
Diane Patterson, Chief,
Access Authorization Branch
U.S. Department of Energy
Oak Ridge Operations Office
200 Administration Road
Oak Ridge, TN 37830
865-576-0925

The Following Officials Have Approved this Document

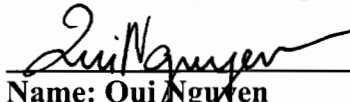
1) System Manager

 (Signature) 9/24/07 (Date)
Name: Gwen Serviel
Title: Software Engineering Project Manager


2) System Owner

 (Signature) 10-25-07 (Date)
Name: Diane Patterson
Title: Chief, Access Authorization Branch

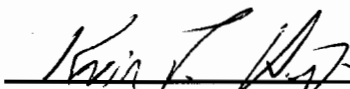
3) Cyber Security Manager

 (Signature) 10/25/07 (Date)
Name: Qui Nguyen
Title: Cyber Security Manager


4) Privacy Act Officer

 (Signature) 10/25/07 (Date)
Name: Amy Rothrock
Title: Privacy Act Officer

DOE Privacy Officer

 (Signature) 11/8/07 (Date)
Name: Kevin T. Hagerty
Title: Director, Office of Information Resources

DOE Senior Official for Privacy Policy

 (Signature) 11-8-07 (Date)
Name: Ingrid Kolb
Title: Senior Officer for Privacy Policy