

**Department of Energy**  
**Privacy Impact Assessment (PIA)**

**Name of Project:** Oak Ridge Office (ORO) ARMING Database (Firearm Credentials Disposition Tracking)

**Bureau:** Department of Energy (DOE)

**Project's Unique ID:** 019-60-02-00-01-5000-04

**Date:** September 15, 2007

**A. CONTACT INFORMATION:**

**1) Who is the person completing this document?**

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

**2) Who is the system owner?**

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

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

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

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

Qui Nguyen  
U.S. Department of Energy

Materials Control and Accountability  
and Information Security Team  
200 Administration Road  
Oak Ridge, TN 37830  
865-576-1600

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

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

Abel Lopez  
U.S. Department of Energy  
FOIA and Privacy Act Group  
1000 Independence Avenue, SW  
Washington, DC 20585  
202-586-5958

**B. SYSTEM APPLICATION/GENERAL INFORMATION:**

**1) Does this system contain any information about individuals?**

Yes.

**a. Is this information identifiable to the individual?<sup>1</sup>**

Yes.

**b. Is the information about individual members of the public?**

No.

**c. Is the information about DOE or contractor employees?**

Yes.

---

<sup>1</sup> "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).

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

The data is collected directly for use as a tracking database concerning the issuance of the federal arming credential. The system is used by the DOE ORO Access Authorization Branch of the Office of Assistant Manager for Security and Emergency Management to log the Protective Force employees who have approved credentials to carry firearms in the performance of their regular duties. The system also identifies the specific site at which an individual is authorized to carry arms. The Oak Ridge Protective Force is made up of contractor employees only.

**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 *et seq.* and Section 161 of the Atomic Energy Act of 1954.

**C. DATA IN THE SYSTEM:**

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

The categories of individuals are DOE ORO contractor employees who are required to carry firearms in the performance of their job duties.

**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 originally obtained from the individual. A "Request from Arming Credential Issuance" Form is completed and provided by the ORO Protective Force contractor to DOE ORO Security and Emergency Management for arming authorization approval.

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

None. The records are ORO documents only.

**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?**

The information, including Social Security Number and name, is collected from the individual by the ORO Protective Force contractor and sent to DOE ORO Security and Emergency Management for arming authorization approval.

**3) Accuracy, Timeliness, and Reliability**

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

The data in the system is collected by the ORO Protective Force contractor and submitted to DOE ORO Security and Emergency Management for arming authorization approval. Therefore, it is determined the data is accurate at the time it is submitted to DOE ORO and entered into the system..

**b. How will data be checked for completeness?**

The ORO Protective Force contractor submits a request to DOE ORO to authorize/rescind authorization/change the credential to carry a firearm. The DOE ORO Safeguards & Security Division will confirm the completeness of the information before updating the system. Therefore, it is determined the data is complete at the time it is entered/modified in the system.

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

Yes. ORO Protective Force contractor submits a request to DOE ORO to authorize/rescind authorization/change the credential to carry a firearm. The DOE ORO Safeguards & Security Division will confirm the request and update the system as required.

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

The data elements are described and documented 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.

- 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?**

No, the system cannot make determinations about the individual.

- 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.**

The social security number and the name of the individual are used interchangeably to retrieve the data.

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

The reports consist of listings of individuals who were issued federal arming authorization cards. The reports can be run by authorized Security and Emergency Management personnel. The responsibility for report distribution is the responsibility of the system owner.

- 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 information is provided 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 ORO General Support System (GSS) boundaries. All system users are ORO GSS users.

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

The Records retention periods are in accordance with applicable National Archives Records Administration (NARA) and DOE record schedules 6: Accountable Officers Accounts Records, dated 6/17/02. (see <http://cio.doe.gov/RBManagement/Records/PDF/RS-DOEADM06.PDF> )

- 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 the NARA and with DOE Administrative Records Schedule 6: Accountable Officers Accounts Records, dated 6/17/02. (see <http://cio.doe.gov/RBManagement/Records/PDF/RS-DOEADM06.PDF> )

- 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?**

The system is subject to the functional and administrative controls for the Information Resources 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 ID. No user is permitted access to the documents for monitoring purposes without ORO and IRMD management direction.

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

DOE-31 "Firearms Qualifications Records."

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

No, the system is not being modified.

**F. ACCESS TO DATA:**

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

ORO Security and Emergency Management personnel assigned to Weapons Authorization Credential Tracking and systems administrators.

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

Access is determined by ORO Domain User ID and application access controls.

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

Yes, users have access to all data on the system.

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

The database is an MS Access database stored in a protected file share in the moderate enclave. The share is protected by an Access Control List (ACL).

**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?**

Contractors are involved in the design, development, and maintenance of the system. Personal information from systems maintained by the Information Technology Support Services Contractor may be disclosed as a routine use to these contractors and their officers and employees in performance of their contracts. Those individuals provided information under this routine use are subject to the same limitations 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 to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE. The contractor shall ensure that all DOE 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.**

The arming data is not shared with other systems.

**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 data is shared with other agencies.

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

N/A

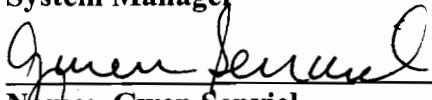


**10) Who is responsible for assuring proper use of the data?**

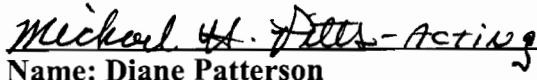
N/A

**The Following Officials Have Approved this Document**

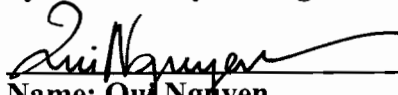
1) System Manager

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

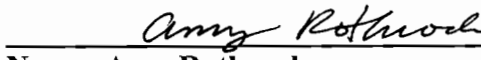
2) Systems Owner

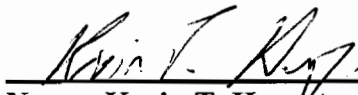
 (Signature) 10-25-07 (Date)  
Name: Diane Patterson  
Title: Chief, Access Authorization Branch

3) Cyber Security Manager

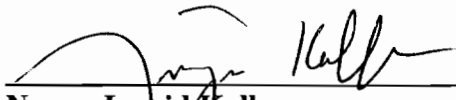
 (Signature) 10/25/07 (Date)  
Name: Qui Nguyen  
Title: Cyber Security Manager

4) Privacy Act Officer

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

 (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: Director, Office of Management