Department of Energy
Privacy Impact Assessment (PIA) for Personal Identity Verification (PIV) System

**Name of Project: PIV System**
**Bureau: Department of Energy**
**Project's Unique ID: 019-60-01-17-01-8062-04-404-140**
**Date: October 21, 2005**

## A. CONTACT INFORMATION:

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

Frederick Catoe, U.S. Department of Energy, IM-31, 1000 Independence Avenue, S.W., Washington, DC 20585, (202) 586-3768, frederick.catoe@hq.doe.gov

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

Rosita Parkes
DOE Chief Information Officer
Email: rose.parkes@hq.doe.gov
Phone: (202) 586-0166

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

Frederick Catoe, U.S. Department of Energy, IM-31, 1000 Independence Avenue, S.W., Washington, DC 20585, (202) 586-3768, frederick.catoe@hq.doe.gov

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

Paul Aaron, U.S. Department of Energy, IM-31, 1000 Independence Avenue, S.W., Washington, DC 20585, (202) 586-0847, paul.aaron@hq.doe.gov

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

Abel Lopez, U.S. Department of Energy, Director, Freedom of Information Act and Privacy Act Group, MA-74, 1000 Independence Avenue, S.W., 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, the system contains information about DOE employees, contractor employees, and individuals requiring long term access to DOE facilities.

**c. Is the information about employees?**

Yes.

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

The purpose of the system is to establish a standards-based authentication and authorization infrastructure. In order to comply with the authentication requirements of **Federal Information Processing Standards Publication 201** (FIPS 201), the identity of an individual must be established before issuing that individual a **Personal Identity Verification** (PIV) Card.

## C. DATA in the SYSTEM:

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

DOE employees, contractor employees, and other individuals seeking long-term access to DOE owned or leased facilities.

[1] "Identifiable Form" – According to the OMB Memo M-03-22, 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 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 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?**

Information is obtained from the individual.

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

The Office of Personnel Management (OPM).

**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 name, address, date and place of birth, photograph, fingerprints, and tracking information from the identity source documents will be collected from the individual. Additional information will be collected as part of the submission of the appropriate background investigation forms[2].

3) Accuracy, Timeliness, and Reliability

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

The Applicant completes and submits appropriate background investigation forms to the Registrar. The Applicant then provides two identity source documents listed in Form I-9 (Employment Eligibility Verification) to the Registrar. One of these forms will be a State or Federal Government-issued picture identification. The Registrar will verify the validity of the documents and compare the picture on the identity source document with the Applicant to confirm the identity of the Applicant. The Registrar will then record the document title,

[2] Usually SF 85, SF 85P, or SF 86 (other OPM designated checks may be acceptable).

document issuing authority, document number, and document expiration date (if any) for both identity source documents. The Registrar also ensures the collection of fingerprints and a photograph of the individual.

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

The data will be manually or electronically reviewed for completeness.

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

The Registrar will verify the two forms of identification for timeliness, relevance, and accuracy.

**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?**

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 may be retrieved by name and/or a unique file identification.

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

N/A

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

An individual may decline to provide the information necessary for identity proofing; however, such a refusal may prevent issuance of a PIV Card.

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?**

Consistent use of this system across the DOE complex will be maintained by applicable DOE policy (including DOE M 4704.2-2, *Physical Protection*, and DOE M 205.10, *Cyber Security for Risk Management*) and Federal law (including *Privacy Act*, 5 U.S.C. 552a, and *E-Government Act of 2002*, 44 U.S.C. 36 (2002)). Each person granted access to the system must be authorized in accordance with DOE policy and Federal law.

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

Information will be retained according to DOE Administrative Records Schedule 11: Space and Administrative Records dated 12/22/00. (http://cio.doe.gov/RBManagement/Records/PDF/RS-DOEADM11.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?**

According to DOE Administrative Records Schedule 11: Space and Administrative Records dated 12/22/00, these records will be destroyed after appropriately accounting for the PIV card.

**4) Is the system using technologies in ways that the 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?**

None.

**8) What controls will be used to prevent unauthorized monitoring?**

N/A

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

DOE-51, Employee and Visitor Access Control Records

DOE-52, Access Control Records of International Visits, Assignments, and Employment at DOE facilities and Contractor Sites

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

Yes.

F. Access to Data:

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

Designated Federal and contractor employees.

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

Access to data is determined by evaluation of personnel job responsibilities and functions.

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

Access will be restricted to job roles and responsibilities.

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

Technical and administrative controls are in place to prevent the misuse of data by individuals with access. The technical controls include restricted access via user-id and password based on user responsibility and job function.

All system team members (Federal and contractor) are required to take the DOE standard cyber security certification course as a necessary prerequisite for the system access. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system. Administrative controls include non-disclosure agreements, separation of duties so individuals only have access to pertinent pieces of personal information, and use of system audit logs to monitor access and user activity in the system.

**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 inserted in their contracts and other regulatory measures addressed?**

Yes.

A new system is not being developed; however, contractors with Privacy Act contract clauses in accordance with Section M of the Privacy Act inserted in their contracts are involved in the maintenance of the existing system.

**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?**

Director, Office of Management.

**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) _____ (Date)

Name: Frederick Catoe

Title: PIV Project Manager

2) Privacy Act Officer

Abel Lopez (Signature) 10/21/05 (Date)

Name: Abel Lopez

Title: Freedom of Information Act and Privacy Act Officer

3) Chief Information Officer

Rosita Parkes (Signature) 10/24/05 (Date)

Name: Rosita Parkes

Title: DOE Chief Information Officer