

Department of Energy
Privacy Impact Assessment (PIA)

Name of Project: DEPARTMENTAL INTEGRATED STANDARDIZE CORE ACCOUNTING SYSTEM (DISCAS) DATA WAREHOUSE (DDW)

Bureau: Department of Energy (DOE)

Project's Unique ID: None

Date: March 15, 2007

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Tammy D. McDuffie, Chief, Financial Systems and Reporting Branch, FM-712, U.S. Department of Energy 200 Administration Road, Oak Ridge, TN, 37830, (865) 576-0880

2) Who is the system owner?

Nancy J. Fitchpatrick, Director, Oak Ridge Financial Service Center, FM-71, U.S. Department of Energy 200 Administration Road, Oak Ridge, TN 37830, (865) 576-0770

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

Roy Settle, Science Applications International Corporation (SAIC), 200 Administration Road, Oak Ridge, TN 37830 (865) 576-2126

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

Qui Nguyen 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 Bureau/Office Privacy Act Officer who reviewed this document?

Abel Lopez, Director, Freedom of Information Act and Privacy Act Group, MA-74, 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 individual¹?

Yes

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

Yes, the system contains information about DOE vendors.

c. Is the information about employees?

Yes

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

The DISCAS Data Warehouse (DDW) database is a non production and historical read only ORACLE database accessible over the DOE business network. DDW was converted from the old DISCAS (precursor to STARS).

C. DATA IN THE SYSTEM:

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

Vendors and DOE employees of these DOE sites:

- Environmental Management Consolidated Business Center (CBC) (including Rocky Flats Field Office);
- Richland Operations Office;
- Strategic Petroleum Reserve Office;
- National Energy Technology Laboratory (NETL);
- The Office of Scientific and Technical Information;
- Savannah River Operations Office; and
- Oak Ridge Operations including regional offices

2) What are the sources of information in the system?

Converted from old DISCAS database.

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).

a. Is the source of the information from the individual or is it taken from another source?

Other – source is old DISCAS database.

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

None.

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?

None.

3) Accuracy, Timeliness, and Reliability.

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

The data is fixed. It is historical data.

b. How will data be checked for completeness?

The data is fixed. It is historical data.

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

Yes. It is historical data.

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

DDW Personally Identifiable Information (PII) data include the individual's Taxpayer Identification Number (TIN), the Social Security Number (SSN), bank account numbers, routing numbers, the name and address of the individual.

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?

No.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No.

5) How will the new data be verified for relevance and accuracy?

The data is fixed. The data is historical.

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 data is retrieved by using non PII data. PII is not used in the retrieval of 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?

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.)

DDW is the only system that contains historical DISCAS data.

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?

DDW is only operated at one site.

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

The DDW database is a non production and historical read only ORACLE database accessible over the DOE business network. DDW was converted from the old DISCAS (precursor to STARS). Since this is historical data, information is archived and kept indefinitely.

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?

The DDW database is a non production and historical read only ORACLE database accessible over the DOE business network. DDW was converted from the old DISCAS (precursor to STARS). Since this is historical data, information is archived and kept indefinitely.

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?

N/A.

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?

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 will be limited to the DOE Financial Staff from the following offices:

- Environmental Management Consolidated Business Center (CBC) (including Rocky Flats Field Office);
- Richland Operations Office;
- Strategic Petroleum Reserve Office;
- National Energy Technology Laboratory (NETL);
- The Office of Scientific and Technical Information;
- Savannah River Operations Office; and
- Oak Ridge Operations including regional offices

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

DOE Finance will request user-id password via <http://finweb.oro.doe.gov/>. Their CHRIS-ID is then verified against DOEINFO.

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

All data.

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. 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 nondisclosure agreements and system 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?

Contractors are involved in the design, development and maintenance of the system. Personal information from STARS and VIAS 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.

VIPERS interfaces with STARS. Information is retrieved from STARS based on the vendor's TIN. Payment information is displayed back to the vendor for verification.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Director, Oak Ridge Financial Service Center.

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?

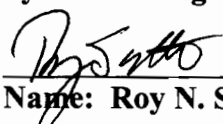
N/A

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

N/A

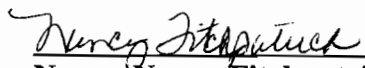
The Following Officials Have Approved this Document

1) System Manager

 (Signature) 3-15-07 (Date)
Name: Roy N. Settle

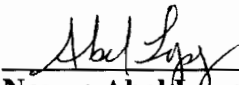
Title: System Administrator

2) System Owner

 (Signature) 3-15-07 (Date)
Name: Nancy Fitchpatrick

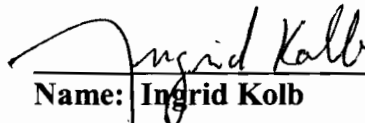
Title: Director, Oak Ridge Financial Service Center

3) Privacy Act Officer

 (Signature) 3/21/07 (Date)
Name: Abel Lopez

Title: Privacy Act Officer

4) Senior Official for Privacy Policy

 (Signature) 3-26-07 (Date)
Name: Ingrid Kolb

Title: Senior Official for Privacy Policy