Department of the Interior
Privacy Impact Assessment

May 2, 2011

Name of Project: Electronic Access Control and Surveillance System (EACSS)

Bureau: Bureau of Reclamation
Project's Unique ID: DOI_BOR_81

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

Bureau/office IT Security Manager

Bureau/office Privacy Act Officer

DOI OCIO IT Portfolio Division

DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Casey Snyder
Privacy Act Officer
Bureau of Reclamation
Denver Federal Center, Building 67, 12th Floor
Denver, CO 80225
Phone: 303-445-2048
Email: csnyder@usbr.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. The EACSS deployments are supported by commercial off-the-shelf software products. The applications contain information about individuals issued access to facilities specific to each deployment. Each individual is assigned a profile containing the following information about each individual:

- First and Last name
- Badge number and the PIN associated with the badge
- Photograph of the individual

Some deployments also include additional information such as:

- Office/location
- Position description/job title
- Home Address
- Phone Numbers
- Emergency Contact Information

a. **Is this information identifiable to the individual[1]?** (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F can be marked not applicable).

Yes. The information is identifiable to the individual.

b. **Is the information about individual members of the public?** (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

No. The information pertains to Federal employees and contractors authorized to work on site at dams and facilities within Reclamation. Therefore, this PIA is included as part of the DOI IT Security C&A process and does not need to be submitted with the OMB Exhibit 300.

c. **Is the information about employees?** (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes. The information in the EACSS deployments is about employees and contractors of the Federal Government. Therefore, this PIA is included as part of the DOI IT Security C&A process.

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

EACSS are physical protection systems consisting of technical capabilities designed to provide an integrated method of detection and response to alarms, threats, and other adverse activities. EACSS technical capabilities include electronic access control (key cards), alarm sensors, and video surveillance. All EACSS components within a single deployment are deployed on an isolated, dedicated network system. Each EACSS deployment does not interconnect with any other information system.

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

The following authorities require and support the establishment of security requirements for the Bureau of Reclamation to the benefit of reliable and secure water and power production and delivery to the American public:

- Reclamation Act of June 17, 1902 (32 Stat. 388; 43 U.S.C. 391) and acts amendatory thereof and supplementary thereto
- Consolidated Natural Resources Act of 2008, Section 513, Bureau of Reclamation Site Security
- Critical Infrastructure Protection Act of 2001 (Public Law 107-56; 115 Stat. 272, 42 USC 5195c)
- Homeland Security Act of 2002 (Public Law 107-296; 116 Stat. 2135, 6 USC 101); Executive Orders 10450, 10577, 12958 as amended, and 12968
- Homeland Security Presidential Directives; Federal Information Processing Standard 201 (FIPS-201); and Departmental Manual Parts 441 through 44

[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 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 descriptors).

C. DATA IN THE SYSTEM:

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

Individuals covered by the EACSS system are Federal employees and contractors.

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

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information is obtained from the individual or from personnel records.

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

Information is obtained directly from the individual or from information obtained by the Bureau of Reclamation.

c. What Tribal, State and local agencies are providing data for use in the system?

N/A

d. From what other third party sources will data be collected?

N/A

e. What information will be collected from the employee and the public?

Information will only be collected from employees and contractors. Collected information includes only the employee's first name and last name. Where physical access within a facility requires both the keycard and a PIN, the employee will input a PIN that will be associated with their access card. As noted in B1 above, some deployments may also collect additional information such as:

- Office/location
- Position description/job title
- Home Address
- Phone Numbers
- Emergency Contact Information

3) Accuracy, Timeliness, and Reliability

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

The individual verifies information about themselves.

b. How will data be checked for completeness?

The individual verifies information about themselves.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes, the data is current. Individuals are responsible for notifying officials when information has changed and should be updated.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data elements are described in detail and documented in the site-specific system.

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?

The use of the data is necessary in order to issue electronic key cards.

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?

Data is not being consolidated.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Processes are not being consolidated. Each deployment resides on a physically isolated network. Access to the information requires both physical and logical access to the system. Strong password requirements, including account lockout features are in place to protect access to the system. Application roles are in place to protect access to the personnel profile information.

8) How will the 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 can be retrieved by name or by unique card number associated with the data record.

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 systems are capable of producing reports that can include attributes associated with individual profiles. These types of reports are run only when requested by management and would be used during a review process whose purpose is to verify the information is accurate.

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.)

Individuals consent to providing the information prior to being granted an electronic access card. Individuals agree to provide the information.

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?

Each system is operated at a specific site. All EACSS deployments are subject to consistent program directives, policies, and standard operating procedures.

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

Personal data associated with an individual is retained in the system throughout the individual's employment period. Handling of data for employee and contractor after their employment ceases is determined at a specific site,.

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?

N/A

4) Is the system using technologies in ways that the DOI 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? If yes, explain.

No. The system will provide a history of locations that the individual has accessed within the sites of the specific deployment but does not track the location of individuals.

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 systems of records notice does the system operate? Provide number and name.

The Privacy Act system of records notices that cover this system are:

- OPM/GOVT-1 (government-wide system for general personnel records maintained by the Office of Personnel Management)
- Interior Personnel Records – Interior, DOI-79 [for Department of the Interior records]
- HSPD 12: Identity Management System and Personnel Security Files – Interior, DOI—45 [for Department of the Interior records]

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

No. The system of records notice already identifies EACSS as a Privacy system.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Only authorized management personnel, EACSS administrators and EACSS personnel with responsibility for issuing keycards will have access to personnel information.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

User access to the data is determined by the requirements associated with their professional responsibilities. Access to the data is based upon the concept of least privilege and is allowed only in keeping with professional responsibilities. Criteria, procedures, controls, and responsibilities regarding access are documented in the deployment-specific EACSS System Security Plans.

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

Users will not have access to all data on the system. User access to data will be restricted by role.

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

The software is configured with application roles that allow only those with appropriate permission assignments to access personnel information. Further, access to the application requires individuals to be issued Microsoft Windows credentials and assigned access to the application. Because all EACSS deployments operate autonomously with no connection to any other information system, individuals must be granted physical access to the locations where EACSS systems are deployed.

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 will be involved with the maintenance of the system. FAR Privacy Act clauses are included in all contracts.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No. Each EACSS deployment is an isolated system and does not connect with, or share information with any other system.

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

Ultimately the Privacy Officer and the local Information System Security Officer (ISSO) are responsible for protecting the privacy rights of those affected.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

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?**

The EACSS System Manager, Information System Security Officer (ISSO), and users of the system are responsible for assuring proper use of the data. All users of the system sign accountability forms prior to being granted access to the system and the information it processes.