Department of the Interior
Privacy Impact Assessment (PIA)
Updated February 2011

Name of Project: Electronic Time and Attendance System (E-TAS)
Bureau: Bureau of Reclamation
Project's Unique ID: DOI_BOR_5

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, Information Management Division, 303-445-2048

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

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, the remainder of the Privacy Impact Assessment does not have to be completed).

Yes – The application displays legal names. Also, social security numbers (SSNs) are stored in one table in the database, and are not directly associated with the individual. A link to the SSN table

[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).

is provided by a randomly assigned employee number. The system only maintains SSNs to create the payroll file which is a requirement of the Federal Payroll and Personnel System (FPPS). SSNs are not used or displayed anywhere in the system.

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

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

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

Collect and transmit time and attendance data for Reclamation payroll, as described in the E-TAS IT Security Plan.

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

In March 2000, GAO issued a checklist, Human Resources and Payroll Systems Requirements (GAO AIMD-00-21.2.3), based on the PFMIP requirements document.

C. <u>DATA in the SYSTEM:</u>

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

Federal employees

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?**

- Employees' personnel and payroll data comes from the Federal Personnel and Payroll System (FPPS).

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

- Department of Interior (DOI) National Business Center (NBC)
- 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?**

None

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

- Employee – daily time/ flextime log (hours worked, hours of leave, per day)
- Public – None

3) Accuracy, Timeliness, and Reliability

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

N/A

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

The data comes from the NBC. When the file is sent back to the NBC for processing, if the data is incomplete the NBC will notify the E-TAS organization that there is an error.

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).

- FPPS data are downloaded daily to the Reclamation Transformation and Integration Database (TIDB) in the Corporate Data Warehouse (CDW). All changed records are date stamped. Personnel responsible for the downloads (both hardware and software) are alerted via E-mail if any part of the process fails.
- All records in the E-TAS database are date stamped and have the individual's account name that entered/modified the data.

This practice is standard practice for developing Reclamation data models.

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

Yes, FPPS data elements are described in the FPPS Combined File document maintained by the National Business Center. Data elements unique to E-TAS are documented in a data model maintained in 84-21120, Corporate Information Services Group.

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 system only contains data required for time and attendance processing and that data is being used for the purpose it was designed for.

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. E-TAS maintains data downloaded from FPPS and data entered by individuals in its original form in an Oracle database. The system does, however, aggregate the data collected and attaches the individual's SSN in a payroll file that is transmitted to the FPPS.

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?**

N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Time and Attendance data are consolidated into a payroll file. The payroll files are kept on a server in a secure location (Denver Data Center) that has restricted and limited access.

Although the actual payroll file is not stored encrypted, the files are encrypted when they are transmitted to the National Business Center (NBC) for payroll processing.

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

N/A

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.

An individual must have a unique account to logon to the E-TAS. The account user ID is associated with the employee's own FPPS data.

The employee's FPPS data in turn has a unique key to retrieve the employee's E-TAS data.

Individuals are also placed in a Timekeeper Group and Signatory Group. E-TAS users who have additional privileges to the system (E-TAS Controls, Timekeepers, Signatories, etc.) must be authorized to access data for specific groups of individuals by their manager/supervisor. A limited number of users with additional privileges are assigned access to these groups.

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

Official Time and Attendance Report
Current Pay Period Time and Attendance Report
Employee Leave Report

Reports are accessible to E-TAS users by a need-to-know basis based on an individual's role. In addition, E-TAS users with specific roles can only run reports on individuals they are authorized to access.

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.)**

N/A – Employee must have a flexitime record in order to get paid.

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?**

N/A - The system operates in only the Denver Data Center.

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

6 calendar years

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 following media are disposed in accordance with Directives and Standards IRM 08-13, "Reclamation Information Technology (IT) Security Program (ITSP): IT Asset Disposal":

- Hard-copy Flexitime logs are shredded after 6 years.
- On-line data are deleted after 6 years
- CDs are destroyed after 6 years
- Backup tapes are degaussed or wiped after 6 years

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.**

Yes, systems logs can only identify the individual logged on based on the user ID and locate the user based on IP address. Other audit logs and audit tables monitor user activity.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

All E-TAS transactions are associated with user IDs and timestamps

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

The E-TAS is an Intranet application so the Reclamation firewall prevents unauthorized external access to the system. All monitoring performed by IT is authorized and complies with security directives and standards. Any attempts by individuals to monitor other individuals are covered by the General Rules of Behavior.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

   Interior/DOI-85 64 FR 26997, 5/18/99, Payroll, Attendance, Retirement, and Leave Records

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

   No, E-TAS is covered by the aforementioned System of Records.

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)

   E-TAS Administrators, E-TAS Controls, Reclamation employees, timekeepers, signatories, Finance personnel, developers, database administrators, and user support personnel have limited access based on their roles.

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

   All access to data is based on successful authentication, activation in E-TAS and for advanced privileges, membership in one or more groups and granted access to specific data.

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

   Every E-TAS user is granted only those privileges necessary for he/she to perform their official duties.

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 E-TAS application and database limits access based on roles and authorization. All E-TAS users having requiring one or more specific E-TAS roles must have a signed E-TAS User Access Form indicating approval by his/her manager/supervisor. In addition, treatment of Privacy Act information is included in the required IT Security Awareness Training.

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. The following Privacy Act Clauses are in the basic ITOP contract for contractors involved with E-TAS:

FAR 52.224.01 Privacy Act Notification
FAR 52.224.02

In addition, contractors are only given access on a need to know basis.

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

Yes, as described in the E-TAS IT System Security Plan, Reclamation's work management systems, CARMA, MAXIMO, and TSCMIS/ESAM, have interfaces with E-TAS.

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

The system security manager(s) and functional system manager(s), identified in each IT System Security Plan, are responsible for protecting the Privacy Act data in the interconnected systems.

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 Maintenance Services Division, as well as manager and supervisors at Reclamation facilities are responsible for assuring proper use of the data.

Due to the sensitive nature of the data within the E-TAS system the security controls such as “access controls” have been implemented to protect the data. Access controls as defined by NIST SP 800-53 is a mechanism put in place to restrict access to data based on the required authentication and need to know. Essentially users are able to access only the data for which they are authorized based on their login credentials. The ETAS application utilizes the general support system (GSS) implementation of active directory (AD) to enforce the access controls.

E-TAS further protects data through active account management, enforcement of assigned authorizations, separation of duties, utilizing the concept of least privilege/functionality, limiting failed access attempts, and prohibiting remote access, among other things. Additionally, included in Reclamation continuous monitoring program the above mentioned controls are evaluated regularly by the ETAS ISSO.