ADAMS ML11066A005

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

(*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)*

Personnel Security Adjudication Tracking System (PSATS)

Date: 03/01/11

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   The Personnel Security Adjudication Tracking System (PSATS) tracks and manages the personnel security data (security clearances, investigative and access authorizations data) and data associated with the issuance of permanent and temporary badges; drug program data associated with applicant drug testing and employee random drug testing; and incoming and outgoing classified visit data.

2. What agency function does it support?

   PSATS supports Personnel and Facilities Security functions for the Office of Administration (ADM), Division of Facilities and Security (ADM/DFS).

3. Describe any modules or subsystems, where relevant, and their functions.

   Not applicable.

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
Karen Cudd	ADM/PMDA/ITT	301-492-3691
Business Project Manager	Office/Division/Branch	Telephone
Valerie Kerben	ADM/DFS/PSB	301-492-3527
Technical Project Manager	Office/Division/Branch	Telephone
Karen Cudd	ADM/PMDA/ITT	301-492-3691

Marjorie Dimig	OIS/BPIAD	301-415-5781
Rick Ellsbury	ADM/PMDA	301-492-3479
Executive Sponsor	Office/Division/Branch	Telephone
Kathryn Greene	ADM/OD	301-492-3500

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. __X__ New System ___ Modify Existing System ____ Other (Explain)

This supports the replacement of a current system (Integrated Personnel Security System (IPSS)) with a new system (PSATS). The PIA for IPSS can be located in ADAMS at ML091660040, approved 06/15/2009.

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes.

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

Federal employees; Federal contractors; Licensees; Consultants; Foreign Assignees; and employment applicants.

b. What information is being maintained in the system about individuals (describe in detail)?

Demographic data, personal identification, and security clearance/access approval information, to include but not limited to: name, social security number, date and place of birth, identity verification information, credential/badge number, a subset of drug testing records (testing date, date of results, applicant test result, random test result if positive), and classified visit data (name of visitor, agency/organization; level of clearance, dates of visit).

c. Is information being collected from the subject individuals?

Yes, but not directly by PSATS. It is being collected from the subject individuals through the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) system and/or the completion of standard government forms used for personnel security.

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

Yes, but not directly by PSATS. Information that will be maintained in PSATS is collected by a variety of tools. OMB Clearances already exist for those tools. Therefore no additional OMB Clearance is required.

e. Is the information being collected from internal files, databases, or systems?

Yes.

(1) If yes, identify the files/databases/systems and the information being collected.

Information will be manually entered and/or scanned from the official agency records on investigations, clearances, drug testing, and credentialing maintained in paper as part of the Personnel, Facility Security, and Drug Testing Programs.

f. Is the information being collected from an external source(s)?

Yes.

(1) If yes, what is the source(s) and what type of information is being collected?

OPM is the Investigative Service Provider. They provide completed investigation products such as fingerprints results and clearance information.

g. How will this information be verified as current, accurate, and complete?

The e-QIP signature page acts as the certification from the individual that the information they submit as part of their investigation is current, accurate, and complete. OPM and/or NRC then conduct a thorough review to ensure completeness and accuracy.

h. How will the information be collected (e.g. form, data transfer)?

Information is manually entered and/or scanned into PSATS, and electronically sent from OPM through e-Delivery (.pdf documents).

i. What legal authority authorizes the collection of this information?

Executive Order 10450, as amended, "Security Requirements for Government Employment."

j. What is the purpose for collecting this information?

To track and manage the official agency records on investigations, clearances, drug testing, and credentialing that are maintained in paper in as part of its Personnel and Facilities Security Programs.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. What type of information will be maintained in this system (describe in detail)? If not applicable, move to question C.1.

Not applicable.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

c. What is the purpose for collecting this information?

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

PSATS tracks and manages the personnel security (security clearances, investigative and access authorizations), drug program data associated with applicant drug testing and employee random drug testing, and incoming and outgoing classified visit data. The information is used for reporting, statistics, forecasting, history tracking, validation, etc. Credentialing data will be used to enable reciprocal acceptance of personal identity verification (PIV) credential determinations across agencies. Classified visit data will be used to validate an individual's clearance level and show access approval for the specific visit.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the information?

ADM/DFS authorized staff ensures proper use of the information.

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

   Yes.

   a. If yes, what is the name of the document that contains this information and where is it located?

      The PSATS Data Dictionary and User's Guide contains this information and is located in Rational ClearCase.

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

   No.

6. How will the information be *retrieved* from the system (be specific)?

   Information about an individual will be retrievable by name or social security number. Information can also be retrieved via the PSATS reporting tool (standard reports and queries).

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

   No.

8. Describe the report(s) that will be produced from this system.

   There are over 75 specific reports and an ad hoc capability available from the PSATS reporting tool. Reports are run on an as needed basis.

   a. What are the reports used for?

      Reports will be used for security information, budgetary purposes, resource planning, and quality control purposes.

   b. Who has access to these reports?

      Staff from the Personnel Security and Facilities Security Branches, the System Administrator, and ADM IT Coordinator will have need-to-know access based on a roles and responsibilities.

D. RECORDS RETENTION AND DISPOSAL

*(This question is intended to establish whether the information, data, or records contained in this system has an approved records retention schedule. (*Reference NUREG-0910*, NRC Comprehensive Records Disposition Schedule.)*

1. Has a retention schedule (either under the General Records Schedule or NRC-specific) for this system been approved by the National Archives and Records Administration?

   Yes.

   a. If yes, list the schedule number and approved disposition.

      GRS 1, Item 36, Federal Workplace Drug Testing Program Files; GRS 1, Item 10, Temporary Individual Employee Records; GRS 18, Item 17, Visitor Control Files; GRS 18, Item 22, Personnel Clearance Files; and GRS 24, Item 6, User Identification, Profiles, Authorizations, and Password Files (excluding records relating to electronic signatures).

2. If you answered "No" to question D.1, complete the following section.

   a. Does the information in the system:

Have historical value?	YES	NO
Document NRC business decisions?	YES	NO
Contain data used to make a judgment or conclusion?	YES	NO
Provide statute or required regulatory information?	YES	NO

   b. What is the value of the information to your organization and the Agency?

      (1) When will it no longer be needed?

   c. How will information, no longer required for current business operations, be maintained?

      (1) Will it be separated from currently active information?

   d. Does this electronic information system replace an existing paper-based or electric information file system?

      (1) If so, which files?

E. ACCESS TO DATA

1. INTERNAL ACCESS

   a. What organizations (offices) will have access to the information in the system?

ADM/DFS and ADM/Program Management, Policy Development and Analysis/Information Technology approved staff will have access to the information in the system. There may be a few potential positions (Office of the Inspector General, Office of Human Resources) on a need-to-know basis (limited access with view-only) that will have access to PSATS. The Office Director of ADM determines who is allowed read-only access.

(1) For what purpose?

For reporting, validation, statistics, forecasting, history tracking, etc.

(2) Will access be limited?

Yes, limited by need-to-know based on roles and responsibilities.

b. Will other systems share or have access to information in the system?

No other NRC systems will have direct access (connection) to PSATS. However, there will be imports of current data from other NRC systems, such as Human Resources Management System, Employee Drug Testing Tracking System, and Access Control and Computer Enhanced Security System.

c. How will information be transmitted or disclosed?

Information will be transmitted via secure file transfer.

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

Authorized users of PSATS have at least a 145b or an IT-II access authorization. PSATS has an audit trail to track modifications to the data. PSATS requires a user ID and password to access the role-based system and the roles are set by least-privilege. Before an individual can gain access to the system, the ADM/DFS Personnel Security Branch Chief must approve the access and then an integrity statement is signed. The system will be personal identity verification (PIV) enabled using an individual's badge.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes.

(1) If yes, where?

PSATS User's Guide is located in Rational ClearCase.

2. EXTERNAL ACCESS

a. Will external agencies/organizations/public share or have access to the information in this system?

No external agencies will have direct access to the information in PSATS. However, a flat file (batch loading of data in a specific layout for agency reporting) is produced monthly to verify security clearances with OPM's Clearance Verification System (CVS).

b. What information will be shared/disclosed and for what purpose?

The information uploaded into the secure portal at OPM's CVS includes the social security number, last name, active clearance level, and date and city and state/country of birth. Since OPM already has the information about an individual, NRC is just communicating the clearance information.

c. How will this information be transmitted/disclosed?

This information is uploaded electronically to the secure portal within OPM. The transmission is secured with 128-bit encryption.

F. TECHNICAL ACCESS AND SECURITY

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

PSATS uses a user id and encrypted password to access the system. The password must be reset every 90 days. PSATS automatically locks a user's access after 3 unsuccessful tries and the user is also logged out of the system after 15 minutes of inactivity. The system will be PIV enabled using an individual's badge and PIN for access.

2. Will the system be accessed or operated at more than one location (site)?

PSATS will be a web based system that will operate from the NRC Headquarters Data Center. User access is through authorized network connectivity.

a. If yes, how will consistent use be maintained at all sites?

Log in requirements and access levels remain the same no matter from what location an approved user attempts to access the system.

3. Which user group (e.g., system administrators, project manager, etc.) has access to the system?

PSATS Administrator
Security Manager
Senior Adjudicator
Adjudicator
Processor
Facilities Security Specialist
Station Guard
Drug Manager
Drug Tester
View Only

4. Will a record of their access to the system be captured?

   Yes.

   a. If yes, what will be collected?

      The date and time of the last login is captured. Certain fields are also captured in an audit log as the data is modified.

5. Will contractors have access to the system?

   Yes.

   a. If yes, for what purpose?

      The Processor role is handled by an ADM/DFS/PSB contractor and they have limited rights. The NRC Guards will have access with limited rights.

      The Processor role processes the Standard Forms as well as updating investigation and clearance information. The Station Guard role has viewing capability as well as the issuance of temporary badges.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

   An audit log tracks modifications to certain data fields within PSATS. All access to data in PSATS is restricted to a need-to-know based on roles and responsibilities.

7. Are the data secured in accordance with FISMA requirements?

   PSATS is currently going through the Certification and Accreditation process.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD Staff)

System Name: Personnel Security Adjudication Tracking System (PSATS)

Submitting Office: Office of Administration

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:

PSATS will maintain personally identifiable information. There will be an indexing or retrieval capability using identifying particulars built into the system and the NRC, in fact, will retrieve records about individuals by use of an individual's name or personal identifier…..therefore, PSATS meets the criteria for a system of records. PSATS will be covered by the following currently published NRC Privacy Act systems of records – no modification to notices required.

- NRC-39, Personnel Security Files and Associated Records
- NRC-40, Facility Security Access Control Records

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Act Program Analyst	March 16, 2011

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

___ No OMB clearance is needed.

___ OMB clearance is needed.

__X__ Currently has OMB Clearance.

Comments:

The data maintained in PSATS will be collected by various tools that already have approved OMB clearances. These tools will collect information from 10 or more individuals who are not Federal employees. No additional OMB Clearance is required for PSATS.

Reviewer's Name	Title	Date
Tremaine Donnell	Information Collections Team Leader	March 16, 2011

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

____ Additional information is needed to complete assessment.

____ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

____ Records retention and disposition schedule must be modified to reflect the following:

Comments:

GRS 1, Item 36, Federal Workplace Drug Testing Program Files; GRS 1, Item 10, Temporary Individual Employee Records; GRS 18, Item 17, Visitor Control Files; GRS 18, Item 22, Personnel Clearance Files; and GRS 24, Item 6, User Identification, Profiles, Authorizations, and Password Files (excluding records relating to electronic signatures). The retention periods for the above records series vary. Conversations with the program officer indicated that the system is capable of managing the varied dispositions and can separate the active from the inactive records. The implementation of these retentions are mandatory under 44 U.S.C 3303 a(d); therefore, retention functionality or a manual process must be incorporated to meet this requirement.

Reviewer's Name	Title	Date
Mary L. Haynes	Records Management Analyst	Mar 16, 2011

D. BRANCH CHIEF REVIEW AND CONCURRENCE

___ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

__X__ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RAN/ ***03/24/2011***

_____ Date _____

Russell A. Nichols, Chief
Information Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Kathryn O. Greene, Director, Office of Administration**	
Name of System: **Personnel Security Adjudication Tracking System (PSATS)**	
Date IRSD received PIA for review: **March 3, 2011**	Date IRSD completed PIA review: **March 24, 2011**

Noted Issues:

PSATS will be maintained as part of NRC Privacy Act Systems of Records NRC-39, Personnel Security Files and Associated Records, and NRC-40, Facility Security Access Control Records.

Federal Acquisition Regulation clauses *52.224-1 Privacy Act Notification* and *52.224-2 Privacy Act* must be referenced in any contract/acquisition where a contractor has access to a Privacy Act system of records, to ensure that the wording of the contract/acquisition make the provisions of the Privacy Act binding on the contractor and his or her employees.

No information collection issues.

Existing records retention and disposition schedules cover the records in the system - no modifications needed.

Russell A. Nichols, Chief Information Services Branch Information and Records Services Division Office of Information Services	Signature/Date: ***/RAN/ 03/24/2011***

Copies of this PIA will be provided to:

James C. Corbett, Director
Business Process Improvement and Applications Division
Office of Information Services

Paul Ricketts
Senior IT Security Officer (SITSO)
FISMA Compliance and Oversight Team
Computer Security Office