U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Personnel Security Adjudication Tracking System (PSATS)

Office of Administration (ADM)

Version 1.0

9/29/2023

Template Version 2.0 (03/2023)

Document Revision History

Date	Version	PIA Name/Description	Author
9/29/2023	1.0	PSATS PIA - Initial Release.	ADM Oasis Systems, LLC
9/11/2023	DRAFT	PSATS PIA - Draft Release.	ADM Oasis Systems, LLC

Table of Contents

The agency is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below help determine any privacy risks related to the E-Government Act or later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

Name/System/Subsystem/Service Name: Personnel Security Adjudication Tracking System (PSATS).

Data Storage Location (i.e., Database Server, SharePoint, Cloud, Other Government Agency, Power Platform): Database.

Date Submitted for review/approval: September 29, 2023.

1 Description

1.1 Provide the description of the system/subsystem, technology (i.e., Microsoft Products), program, or other data collections (hereinafter referred to as "project"). Explain the reason the project is being created.

The PSATS subsystem of the Office of Administration's (ADM) Moderate ADM Support Systems (MASS) supports the personnel and facilities security functions for the ADM Division of Facilities and Security (ADM/DFS). PSATS is used by the NRC to automate the tracking of personnel security related activities, serving as a mechanism to track the status of security checks (i.e., security clearances, security investigations, access authorizations). This also includes tracking foreign travel declarations as required by the Security Executive Agent Directive 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position." The system monitors the status of personnel security clearance checks for applicants, current NRC employees, contractors, consultants, student interns, licensees, and anyone who requires access to NRC facilities, classified information, sensitive NRC information and equipment, nuclear power facilities, and special nuclear material.

In December 2021, the Security Executive Agent Directive 3 (SEAD3) portal was added to the MASS boundary as a module of PSATS. SEAD3 is a web portal used to report, record, and track foreign travel of personnel who hold a security clearance. This portal was developed in response to the Federal Government requirement to track employee, contractor, and licensee personal travel to foreign countries in the interest of national security. Please refer to the separate SEAD3 PIA for additional information.

Please mark appropriate response below if your project/system will involve the following:

☐ PowerApps	☐ Public Website
☐ Dashboard	☒ Internal Website
☐ SharePoint	☐ None
☐ Other:	

1.2 Does this privacy impact assessment (PIA) support a proposed new project, proposed modification to an existing project, or other situation? Select options that best apply in table below.

Mark appropriate response.

Status Options	
☐	New system/project
☒	Modification to an existing system/project. *If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.* Annual update, migration to new PIA template for PSATS, and no longer tracking foreign assignees in the system. ADAMS ML: ML20288A500
☐	Annual Review *If making minor edits to an existing system/project, briefly describe the changes below.*
☐	Other (explain)

1.3 Points of Contact:

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
Name	Christoph Heilig	Jennifer Golder	Zia Anderson	N/A	Lisa Nichols-Streck	N/A
Office /Division /Branch	ADM/ DFS/PSB	ADM	ADM/ DRMA/BITT	N/A	ADM/ DFS/PSB	N/A
Telephone	301-415-7731	301-287-0741	301-415-3483	N/A	301-415-5834	N/A

2 Authorities and Other Requirements

2.1 What specific legal authorities and/or agreements permit the collection of information for the project?

Provide all statutory and regulatory authorities for operating the project, including the authority to collect the information; NRC internal policy is not a legal authority. Please mark appropriate response in table below.

Mark with an "X" on all that apply.	**Authority**	**Citation/Reference**
☒	**Statute**	42 United States Code (U.S.C.) 2011 et seq., 2165, 2201(i), 2201a, 2284, and 5801 et seq.
☒	**Executive Order**	Executive Order (E.O.) 9397, as amended by E.O. 13478; 10450, 10865, 12968, 13467, 13488, 13526, and 13587.
☒	**Federal Regulation**	5 Code of Federal Regulation (CFR) parts 731 and 732; 10 CFR parts 10, 11, 14, 25, 50, 73, and 95; and OMB Circular No. A-130, Revised.
☐	**Memorandum of Understanding/Agreement**	
☐	**Other (summarize and provide a copy of relevant portion)**	

2.2 Explain how the information will be used under the authority listed above (*i.e., enroll employees in a subsidies program to provide subsidy payment*).

Information in PSATS is used to track and manage the official agency records on investigations, clearances, drug testing, and credentialing that are maintained as part of the NRC personnel and facilities security programs. PSATS information relates to the personnel security (security clearances, investigations, 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 is used to enable reciprocal acceptance of personal identity verification (PIV) credential determinations across agencies. Classified visit data is used to validate an individual's clearance level and show access approval for the specific visit.

If the project collects Social Security Numbers (SSNs), state why this is necessary and how it will be used.

SSNs are needed to identify personnel security records unique to the individual.

3 Characterization of the Information

In the table below, mark the categories of individuals for whom information is collected.

Category of individual	
☒	Federal employees
☒	Contractors
☒	Members of the Public (any individual other than a federal employee, consultant, or contractor)
☒	Licensees
☒	**Other:** Consultants, employment applicants, student interns, and applicable visitors.

In the table below, is a list of the most common types of PII collected. Mark all PII that is collected and stored by the project/system. If there is additional PII not defined in the table below, a comprehensive listing of PII is provided for further reference in ADAMS at the following link: PII Reference Table 2023.

Categories of Information			
☒	Name	☒	Resume or curriculum vitae
☒	Date of Birth	□	Driver's License Number
☒	Country of Birth	□	License Plate Number
☒	Citizenship	☒	Passport Number
□	Nationality	☒	Relatives Information
□	Race	□	Taxpayer Identification Number
☒	Home Address	□	Credit/Debit Card Number
☒	Social Security Number (Truncated or Partial)	☒	Medical/health information
□	Gender	☒	Alien Registration Number
□	Ethnicity	☒	Professional/personal references
☒	Spouse Information	☒	Criminal History
☒	Personal e-mail address	☒	Biometric identifiers (e.g., facial images, fingerprints, iris scans)
□	Personal Bank Account Number	□	Emergency contact (e.g., a third party to contact in case of an emergency)
☒	Personal Mobile Number	□	Accommodation/disabilities information
☒	Marital Status	☒	**Other:** Education history, financial history, employment history, military history, foreign activities/contacts/financial interests, foreign countries visited, police records, drug activity, alcohol use, investigations information, clearance information, financial information, civil court actions, copies of personnel security
☒	Children Information		
☒	Mother's Maiden Name		

Categories of Information			
			investigative reports from other Federal agencies, date of marriage, place of marriage, other names used by employee/applicant, and other names used by spouse/cohabitant, foreign travel information, and drug test dates/results.

3.1 Describe how the data is collected for the project. (i.e., NRC Form, survey, questionnaire, existing NRC files/databases, response to a background check).

PSATS acts as a repository of unclassified personnel data to record adjudications. Information in PSATS consists of personnel security files collected from directly from the subject individual via applicable forms and third parties, containing: demographic data, personal identification, and security clearance/access approval information, to include but not limited to: full name, SSN, 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), employee and contractor foreign travel information, and classified visit data (name of visitor, agency/organization, level of clearance, dates of visit).

Prior to initiating an investigation for an applicant, NRC personnel security check the Defense Counterintelligence and Security Agency (DCSA) Central Verification System (CVS) to determine if there is an existing adjudication/investigation that meets the NRC needs and can be leveraged. If an investigation is needed, the DCSA e-App system is used by NRC employees/applicants to complete all personnel investigative forms, including the Standard Form SF-85 ("Questionnaire for Non-Sensitive Positions") and SF-86 ("Questionnaire for National Security Positions"). The collections process for e-App is documented in the separate e-App PIA.

For fingerprinting, NRC employees/applicants can get their fingerprints taken at an NRC site (NRC HQ, Regional Offices, Technical Training Center (TTC)), at a General Services Administration (GSA) USAccess shared site, or at an authorized law enforcement location (i.e., local police department). For individuals fingerprinted at NRC or GSA sites, data (fingerprints and badging information) is collected directly from the subject individual through USAccess. USAccess transmits the electronic fingerprint images to DCSA for processing. For individuals fingerprinted at authorized non-NRC/GSA sites, hard card fingerprints are mailed to NRC HQ. The fingerprint card is scanned by NRC personnel security and electronically submitted from PSATS to DCSA.

Copies of the e-App submissions (SF-85 and SF-86) are manually uploaded to PSATS into the individual's record. Investigative files from DCSA (i.e., law enforcement and financial/credit information) are electronically sent to PSATS from the DCSA eDelivery system to track and manage the official agency records on investigations and for clearance tracking purposes. Additionally, for completed investigations, NRC personnel security will upload applicable clearance information (SSN, last name, active clearance level, date, and place of birth) to DCSA's CVS through the portal.

NRC personnel security use the Federal Bureau of Investigation's (FBI) Enterprise Vetting Center / Law Enforcement Enterprise Portal (EVC/LEEP), which provides name checks for the spouses/cohabitants of NRC employees/applicants holding or requiring a security clearance. For the EVC/LEEP, NRC employees/applicants are required to complete the NRC Form 354 ("Data Report on Spouse"). After use of the information for EVC/LEEP, the form is retained in PSATS as part of the employee/applicant's case file. The collections process for EVC/LEEP is documented in the separate EVC/LEEP PIA.

As mentioned above in section 1.1, the SEAD3 portal is used by NRC to collect information on and approve unofficial (personal) foreign travel of individuals who possess an NRC security clearance. For NRC employees and contractors, information collected from the "NRC Personal International Travel Form" completed in the SEAD3 portal becomes part of the individual's case file in PSATS. For licensees and other individuals who possess an NRC security clearance, unofficial foreign travel requests are submitted to NRC through the UnofficialTravel.Resource@nrc.gov email address. The collections process for SEAD3 is documented in the separate SEAD3 PIA.

In addition to the data provided by DCSA, NRC personnel security manually enter information directly into PSATS as part of an individual's case file. The NRC Form 277 ("Request for Visit") is used to request authorization to attend classified meetings at NRC facilities for federal employees/contractors from external agencies. The form is submitted to NRC personnel security in order for the individual's clearance status to be verified and approved. The following information is provided on the form: requesting NRC office name/business telephone number, NRC office requestor job title and signature, name of the NRC facility/facilities to be visited, visit start/end date(s), purpose of the visit/need-to-know, visit point of contact (POC) name/telephone number/fax number, security POC name/telephone number/fax number, level of clearance/access required for visit, individual(s) investigative information (full legal name, SSN, citizenship status, date of birth, place of birth, clearance type/date, investigation type/date), name and title of NRC security official, and any applicable remarks. After the data is entered into the system by personnel security, a copy of the form is uploaded to PSATS, where it is retained as part of the subject individual's case file.

The NRC Form 850 ("Request for Contractor Assignment(s)") is used by Contracting Office Representatives (CORs), submitted to NRC personnel security for processing a new NRC contractor, processing an NRC contractor requiring an access/clearance upgrade, or adding an additional contract to an existing NRC contractor. The following information is provided on the form: contractor information (full legal name, SSN, date of birth, place of birth, current address, phone number, email address, and citizenship), contract information (reason for submission, contract expiration, contract company name, contract number, COR name(s), type of access needed, drug testing requirement indicator, type of badge needed), and, if applicable, task order information. After the data is entered into the system by personnel security, a copy of the form is uploaded to PSATS, where it is retained as part of the contractor's case file.

The NRC Form 977 ("Applicant Clearance Status Checklist") is used by the Office of the Chief Human Capital Officer (OCHCO), submitted to NRC personnel security as a request to create a new personnel security file for a prospective NRC federal employee. The following information is provided on the form: OCHCO requestor name/email address, NRC contractor status, current clearance status/level, granting Agency/Branch, applicant information (full name, home telephone number, mobile telephone number, home address, email address, NRC position title/organization/duty station, clearance level required, project information, and drug testing requirement indicator. Additionally, the applicant's resume, Office of Personnel Management (OPM) Optional Form (OF) 306 ("Declaration for Federal Employment"), and a Suitability Memo, if applicable, are provided as attachments. After the data is entered into the system by personnel security, a copy of the email correspondence regarding the submission of the NRC Form 977 is retained in PSATS, not the form itself.

The NRC Form 176 ("Security Acknowledgement") is completed by licensee applicants as part of the clearance application and security debriefing process. Information collected on the form includes licensee name, last four of the SSN, name of employer, and witness name (for security debriefings). NRC personnel security indicate in PSATS the date the form was received, after which a copy of the form is uploaded to PSATS, where it is retained as part of the licensee's case file.

For NRC federal employees, all pre-employment drug testing dates and results are entered into PSATS by NRC personnel security adjudicators. In the event that a random drug test contains a positive result, the individual's drug test date and result are also recorded in PSATS by NRC personnel security adjudicators.

3.2 If using a form to collect the information, provide the form number, title, and/or a link.

The following NRC forms are used for PSATS purposes:

- NRC Form 176, "Security Acknowledgement"
- NRC Form 277, "Request for Visit"
- NRC Form 850, "Request for Contractor Assignment(s)"
- NRC Form 977, "Applicant Clearance Status Checklist"
- NRC Form 354, "Data Report on Spouse" (used to support EVC/LEEP)
- NRC Personal International Travel Form (from SEAD3: https://sead3portal.nrc.gov/sead3portal/landing)

Additionally, the following forms owned by external agencies are used for PSATS purposes:

- OPM OF 306, "Declaration for Federal Employment"
- SF-85, "Questionnaire for Non-Sensitive Positions" (from e-App)
- SF-86, "Questionnaire for National Security Positions" (from e-App)

3.3 Who provides the information? Is it provided directly from the individual or a third party.

Information is provided from both the subject individual and third parties. Refer above to section 3.1 for details.

3.4 Explain how the accuracy of the data collection is validated. If the project does not check for accuracy, please explain why.

PSATS does not perform data validation, the system is primarily a repository of personnel and facilities security data. However, personnel security staff verify information on NRC Forms received prior to entry into PSATS. The NRC Form 277 is cross-checked using government-wide databases; and NRC Form 850, NRC Form 977, NRC Form 176, and OF 306 are validated using the individual's SF-85/SF-86. For checking an individual's investigative history in DCSA's CVS, name and SSN are used to verify the records belong to the individual. For validation of information collected for e-App, EVC/LEEP, DTTS, and SEAD3 refer to the respective PIAs.

3.5 Will PII data be used in a test environment? If so, explain the rationale.

Yes, data containing PII is used in the PSATS test environment in order to support personnel security training.

3.6 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

NRC personnel security manually review forms/files received and case file information, check information across records in the system, and will coordinate any corrective actions to records, as applicable.

4 Data Security

4.1 Describe who has access to the data in the project (i.e., internal NRC, system administrators, external agencies, contractors, public).

All access to data in PSATS is restricted to personnel with a need-to-know, based on roles and responsibilities. The PSATS users include system administrators, personnel security/adjudicators, facilities security/NRC guards, a limited number of ADM/DFS Security Management and Operations Branch (SMOB) personnel, a limited number of Office of Inspector General (OIG) personnel, and a limited number of Office of Nuclear Security and Incident Response (NSIR) personnel.

4.2 If the project/system shares information with any other NRC systems, identify the system, what information is being shared, and the method of sharing.

Information is manually entered, scanned, and/or uploaded from the official agency records on investigations, clearances, drug testing, and credentialing maintained on paper as part of the personnel and facility security program.

Additionally, the Federal Personnel Payroll System (FPPS) and Enterprise Identity System (EIH) share data with PSATS. OCHCO's FPPS provides home address updates for NRC personnel, and Office of the Chief Information Officer (OCIO) EIH provides identity credential information (PSATS ID, name, DOB, and UPN). PSATS also publishes limited information (only PSATS ID, day/month of birth, and submission status) through an enterprise portal (https://check.nrc.gov/ADMCheck) created by OCIO for PSATS submission status checks.

Refer above to section 3.1 for additional discussion of information sharing with other NRC systems.

4.3 If the project/system connects, receives, or shares information with any external non-NRC partners or systems, identify what is being shared.

Refer above to section 3.1.

Identify what agreements are in place with the external non-NRC partner or system in the table below.

Agreement Type	
□	Contract Provide Contract Number:
□	License Provide License Information:
☒	Memorandum of Understanding Provide ADAMS ML number for MOU: DCSA NBIS (CVS): ML19326A925
☒	Other Interconnection Security Agreement Provide ADAMS ML number for ISA: *Please note, updated agreement for use of DCSA eDelivery and fingerprinting are in the process of being updated and approved.*
□	None

4.4 Describe how the data is accessed and describe the access control mechanisms that prevent misuse.

PSATS resides behind the NRC network firewall, authorized users must first gain access to the NRC network using valid authentication credentials. PSATS user accounts are integrated with the Information Technology Infrastructure (ITI) Identity, Credential, and Access Management (ICAM) for Single Sign-On (SSO) access.

An individual's PSATS access is further restricted by the user's assigned role in the system. Access to PSATS is restricted to personnel with a need-to-know, based on roles and responsibilities, limiting permissions to view/modify information to only that which is required for their job function. An audit log tracks modification to applicable data fields within PSATS. The date and time of user logins are also captured.

4.5 Explain how the data is transmitted and how confidentiality is protected (i.e., encrypting the communication or by encrypting the information before it is transmitted).

PSATS is accessible to staff over the NRC network; data transfers are encrypted. For information uploaded electronically to DCSA CVS, personnel security accessing the portal use secure web-browser connections. For fingerprint transmissions to DCSA, this occurs over secure Virtual Private Network (VPN) connection from NRC to DCSA. For receiving file transmissions from DCSA eDelivery, communications are encrypted to the DMZ server using SFTP for file transfers.

4.6 Describe where the data is being stored (i.e., NRC, Cloud, Contractor Site).

PSATS data is stored at NRC HQ, on physical servers.

4.7 Explain if the project can be accessed or operated at more than one location.

PSATS is a web-based system that operates from the NRC HQ Data Center. User access is through authorized NRC network connectivity. Login requirements and access levels remain the same no matter from what location an approved user attempts to access the system.

4.8 Can the project be accessed by a contractor? If so, do they possess an NRC badge?

Yes, all NRC contractors accessing and supporting PSATS possess an HSPD-12 PIV card issued by the NRC.

4.9 Explain the auditing measures and technical safeguards in place to prevent misuse of data.

PSATS user actions (varying by assigned role) and data transaction/import events are captured in audit logs, which include the date and time of the action. Audit logs are reviewed by PSATS administrators to monitor activities and report any anomalies within the system.

4.10 Describe if the project has the capability to identify, locate, and monitor (i.e., trace/track/observe) individuals.

N/A.

4.11 Define which FISMA boundary this project is part of.

PSATS is included as a subsystem of the Moderate ADM Support System (MASS) FISMA boundary.

4.12 Is there an Authority to Operate (ATO) associated with this project/system?

Authorization Status	
☐	Unknown
☐	No *If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Organization (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track***.**
☐	In Progress provide the estimated date to receive an ATO. Estimated date:
☒	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO) Confidentiality – Moderate Integrity – Moderate Availability – Moderate

4.13 Provide the NRC system Enterprise Architecture (EA)/Inventory number. If unknown, contact EA Service Desk to get the EA/Inventory number.

EA Number: 20110002.

5 Privacy Act Determination

5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
☒	**Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)**
☒	**List the identifiers that will be used to retrieve the information on the individual.** For personnel security/adjudicators, information about an individual in PSATS is retrievable by name, SSN, and/or PSATS ID. Information can also be retrieved via the reporting tool for standard reports and queries. For NRC guards checking-in visitors attending sensitive meetings, records are retrieved in PSATS via full name, SSN, and date of birth for clearance level and access authorization verification.
☐	**No, the PII is not retrieved by a personal identifier.** **If no, explain how the data is retrieved from the project.**

5.2 For all collections where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a System of Record Notice (SORN) in the Federal Register. *As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other personal identifier assigned to the individual."*

Mark the appropriate response in the table below.

Response	
☒	***Yes, this system is covered by an existing SORN. (See existing SORNs: https://www.nrc.gov/reading-rm/foia/privacy-systems.html)*** ***Provide the SORN name, number, (List all SORNs that apply):*** NRC-35 – "Drug Testing Program Records" NRC-39 – "Personnel Security Files and Associated Records"
☐	**SORN is in progress**
☐	**SORN needs to be created**
☐	**Unaware of an existing SORN**
☐	**No, this system is not a system of records and a SORN is not applicable.**

5.3 When an individual is asked to provide personal data (i.e., form, webpage, survey), is a Privacy Act Statement (PAS) provided? *A Privacy Act Statement is a disclosure statement required to appear on documents used by agencies when an individual is asked to provide personal data. It is required for any forms, surveys, or other documents, including electronic forms, used to solicit personal information from individuals that will be maintained in a system of records.*

Mark the appropriate response.

Options	
☒	**Privacy Act Statement:** The following NRC forms are used for PSATS purposes and contain Privacy Act Statements: • NRC Form 176, "Security Acknowledgement" • NRC Form 277, "Request for Visit" • NRC Form 850, "Request for Contractor Assignment(s)" For the NRC Form 977, because this form is completed by OCHCO on behalf of the subject individual, this form does not require a Privacy Act Statement. For NRC Form 354 Privacy Act Statements, refer to the EVC/LEEP PIA. For the "NRC Personal International Travel Form", refer to the SEAD3 PIA.
☐	**Not Applicable**
☒	**Unknown** For SF-85 and SF-86 Privacy Act Statements, e-App is owned by a non-NRC agency (DCSA), refer to the e-App PIA. For OF 306 Privacy Act Statements, this is N/A as this form is owned by a non-NRC agency (OPM).

5.4 Is providing the PII mandatory or voluntary? What is the effect on the individual by not providing the information?

PII is needed to uniquely identify the employee/applicant to support their initial or continuing eligibility for a security clearance and/or NRC access authorization. Therefore, PII disclosure is mandatory to ensure the information used by PSATS matches the information collected from external sources and forms for adjudicative determinations.

6 Records and Information Management-Retention and Disposal

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are **Temporary** (eligible at some point for destruction/deletion because they no longer have business value) or **Permanent** (eligible at some point to be transferred to the National Archives because of historical or evidential significance). Records/data and information with historical value, identified as having a "permanent" disposition, are transferred to the National Archives of the United States at the end of their retention period. All other records identified as having a "temporary" disposition are destroyed at the end of their retention period in accordance with the NARA Records Schedule or the General Records Schedule.

These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR, agencies are required to establish procedures for addressing Records and Information

Management (RIM) requirements. This includes strategies for establishing and managing recordkeeping requirements and disposition instructions before approving new electronic information systems or enhancements to existing systems.

The following questions are intended to determine whether the records/data and information in the system have approved records retention schedules and disposition instructions, whether the system incorporates RIM strategies including support for NARA's Universal Electronic Records Management (ERM) requirements, and if a mitigation strategy is needed to ensure compliance.

If the project/system:

- Does not have an approved records retention schedule and/or
- Does not have an *automated* RIM functionality,
- Involves a cloud solution,
- And/or if there are additional questions regarding Records and Information Management - Retention and Disposal, please contact the NRC Records staff at **ITIMPolicy.Resource@nrc.gov** for further guidance.

If the project/system has a record retention schedule or an automated RIM functionality, please complete the questions below.

6.1 Does this project map to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules?

☐	NUREG-0910, "NRC Comprehensive Records Disposition Schedule"
☒	NARA's General Records Schedules
☐	Unscheduled

6.2 If so, cite the schedule number, approved disposition, and describe how this is accomplished.

System Name (include sub-systems, platforms, or other locations where the same data resides)	PSATS
Records Retention Schedule Number(s)	GRS 2.7 Item 130 – "Employee drug test results. Positive results." GRS 2.7 Item 131 – "Employee drug test results. Negative results." GRS 3.2 Item 030 – "System access records. Systems not requiring special accountability for access." GRS 3.2 Item 031 – "System access records. Systems requiring special accountability for access." GRS 4.2 Item 030 – "Information access and protection operational records. Records tracking and controlling access to protected

	information." GRS 5.6 Item 010 – "Security management administrative records." GRS 5.6 Item 110 – "Visitor processing records. Areas requiring highest level security awareness." GRS 5.6 Item 111 – "Visitor processing records. All other facility security areas." GRS 5.6 Item 120 – "Personal identification credentials and cards. Application and activation records." GRS 5.6 Item 170 – "Personnel security investigative reports. Personnel suitability and eligibility investigative reports." GRS 5.6 Item 171 – "Personnel security investigative reports. Reports and records created by agencies conducting investigations under delegated investigative authority." GRS 5.6 Item 181 – "Personnel security and access clearance records. Records of people issued clearances." GRS 5.6 Item 190 – "Index to the personnel security case files."
Approved Disposition Instructions	GRS 2.7 Item 130: **Temporary**. Destroy when employee leaves the agency or when 3 years old, whichever is later. GRS 2.7 Item 131: **Temporary**. Destroy when 3 years old. GRS 3.2 Item 030: **Temporary**. Destroy when business use ceases. GRS 3.2 Item 031: **Temporary**. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. GRS 4.2 Item 030: **Temporary**. Destroy 2 years after last form entry, reply, or submission; or when associated

	documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use. GRS 5.6 Item 010: **Temporary**. Destroy when 3 years old, but longer retention is authorized if required for business use. GRS 5.6 Item 110: **Temporary**. Destroy when 5 years old, but longer retention is authorized if required for business use. GRS 5.6 Item 111: **Temporary**. Destroy when 2 years old, but longer retention is authorized if required for business use. GRS 5.6 Item 120: **Temporary**. Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use. GRS 5.6 Item 170: **Temporary**. Destroy in accordance with the investigating agency instructions. GRS 5.6 Item 171: **Temporary**. Destroy in accordance with delegated authority agreement or memorandum of understanding. GRS 5.6 Item 181: **Temporary.** Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use. GRS 5.6 Item 190: **Temporary**. Destroy when superseded or obsolete.
Is there a current automated functionality or a manual process to support RIM requirements? This includes the ability to apply records retention and disposition policies in the system(s) to support records	PSATS employs manual processes to support RIM requirements.

accessibility, reliability, integrity, and disposition.	
Disposition of Temporary Records Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	Active personnel security records are retained in PSATS for the duration of employment. Inactive personnel security records in PSATS are archived. Upon deletion of a PSATS user account, all reports generated by the user are deleted.
Disposition of Permanent Records Will the records be exported to an approved format and transferred to the National Archives based on approved retention and disposition instructions? If so, what formats will be used? **NRC Transfer Guidance (Information and Records Management Guideline - IRMG)**	N/A.

7 Paperwork Reduction Act

The Paperwork Reduction Act (PRA) of 1995 requires that agencies obtain an Office of Management and Budget (OMB) approval in the form of a "control number" — before promulgating a paper form, website, surveys, questionnaires, or electronic submission from 10 or more members of the public. If the data collection is from federal employees regarding work-related duties, then a PRA clearance is not necessary.

7.1 Will the project be collecting any information from 10 or more persons who are not Federal employees?

The information collection does not have OMB approval directly by PSATS. Information maintained in PSATS is collected by a variety of tools/sources. The following NRC forms are used for PSATS purposes:

- NRC Form 176 (“Security Acknowledgement”) – OMB No. 3150-0239
- NRC Form 277 (“Request for Visit”) – OMB No. 3150-0051
- NRC Form 850 (“Request for Contractor Assignment(s)”) – OMB No. 3150-0218
- NRC Form 977 (“Applicant Clearance Status Checklist”) – N/A
- NRC Form 354 (“Data Report on Spouse”, used for FBI EVC/LEEP) – OMB No. 3150-0026
- “NRC Personal International Travel Form” (used for SEAD3):
  - For NRC employees and contractors with a security clearance, the SEAD3 portal is used to complete the “NRC Personal International Travel Form” (https://sead3portal.nrc.gov/sead3portal/landing) prior to, or immediately after returning from unofficial foreign travel.

- For licensees and other individuals who possess an NRC security clearance, unofficial foreign travel requests are submitted to NRC via the UnofficialTravel.Resource@nrc.gov email address. An external portal for non-NRC personnel use is planned to be developed within the next year to replace the current email process.

Additionally, the following forms owned by external agencies are used for/retained by PSATS:

- OPM OF 306 ("Declaration for Federal Employment") – OMB No. 3206-0182
- SF-85 ("Questionnaire for Non-Sensitive Positions", used for DCSA e-App) – OMB No. 3206-0261
- SF-86 ("Questionnaire for National Security Positions", used for DCSA e-App) – OMB No. 3206-0005

7.2 Is there any collection of information addressed to all or a substantial majority of an industry (i.e., Fuel Fabrication Facilities or Fuel Cycle Facilities)?

No.

7.3 Is the collection of information required by a rule of general applicability?

No.

Note: For information collection (OMB clearances) questions: contact the NRC's Clearance Officer. Additional guidance can be found on the NRC's internal Information Collections Web page at: https://intranet.nrc.gov/ocio/33456.

8 Privacy Act Determination

Project/System Name: Personnel Security Adjudication Tracking System (PSATS).

Submitting Office: Office of Administration (ADM).

Privacy Officer Review

Review Results		Action Items
☐	This project/system **does not contain PII.**	**No further action** is necessary for Privacy.
☐	This project/system **does contain PII**; the Privacy Act does **NOT** apply, since information is NOT retrieved by a personal identifier.	**Must be protected with restricted access** to those with a valid need-to-know.
☒	This project/system **does contain PII**; the **Privacy Act does apply**.	**SORN is required-** Information is **retrieved** by a personal identifier**.**

Comments:

Covered by NRC-35 – Drug Testing Program Records and NRC-39 – Personnel Security Files and Associated Records.

Reviewer's Name	Title
Sally A. Hardy Signed by Hardy, Sally on 12/29/23	Privacy Officer

9 OMB Clearance Determination

NRC Clearance Officer Review

Review Results	
□	No OMB clearance is needed.
□	OMB clearance is needed.
☒	Currently has OMB Clearance. Clearance No. See the list in Section 7.2

Comments:

Reviewer's Name	Title
Signed by Cullison, David on 12/27/23	Agency Clearance Officer

10 Records Retention and Disposal Schedule Determination

Records Information Management Review

Review Results	
□	No record schedule required.
□	Additional information is needed to complete assessment.
□	Needs to be scheduled.
☒	Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
Marna B. Dove Signed by Dove, Marna on 12/18/23	Sr. Program Analyst, Electronic Records Manager

11 Branch Chief Review and Concurrence

Review Results	
☐	This project/system **does not** collect, maintain, or disseminate information in identifiable form.
☒	This project/system **does** collect, maintain, or disseminate information in identifiable form.
☒	I concur with the Privacy Act, Information Collections, and Records Management reviews.

Signed by Feibus, Jonathan
on 01/02/24

Chief Information Security Officer
Chief Information Security Division
Office of the Chief Information Officer

ADDITIONAL ACTION ITEMS/CONCERNS

Name of Project/System: Personnel Security Adjudication Tracking System (PSATS)	
Date CISD received PIA for review: December 7, 2023	**Date CISD completed PIA review:** December 29, 2023
Action Items/Concerns:	
Copies of this PIA will be provided to: *Caroline Carusone* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Garo Nalabandian* *Deputy Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	