ADAMS ML20182A130

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 collection requirements, and records management requirements.

Individual Action Tracking System (IATS)

Date: June 14, 2020

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system:

The Individual Action Tracking System (IATS) tracks cases of individuals involved in NRC-licensed activities who have been subject to NRC enforcement actions.

2. What agency function does it support?

IATS supports the Office of Enforcement (OE) in their ability to track and trend enforcement actions taken against individuals.

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

N/A

4. What legal authority authorizes the purchase or development of this system?

Atomic Energy Act of 1954. Also 42 U.S.C 2113, 2114, 2231; 42 U.S.C. 2167, as amended; 42 U.S.C. 2201(I), as amended; and 42 U.S.C. 2282, as amended; 10 CFR 30.10, 40.10, 50.5, 60.11, 61.9b, 70.10, 72.12, and 110.7b.

5. What is the purpose of the system and the data to be collected?

To allow the Office to manage case work, and track and trend actions against individuals.

6. Points of Contact:

Project Manager	**Office/Division/Branch**	**Telephone**
Bob Fretz	OE/EB	301-287-9235
Business Project Manager	**Office/Division/Branch**	**Telephone**
Bob Fretz	OE/EB	301-287-9235
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Bob Fretz	OE/EB	301-287-9235
Executive Sponsor	**Office/Division/Branch**	**Telephone**
George Wilson	Director, OE	301-287-9527
ISSO	**Office/Division/Branch**	**Telephone**
Patty Nibert	Mgmt Analyst, OE	301-287-9522
System Owner/User	**Office/Division/Branch**	**Telephone**
Bob Fretz	OE/EB	301-287-9235

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ____ New System

____ Modify Existing System

__X__ Other

b. **If modifying or making other updates to an existing system, has a PIA been prepared before?**

Yes

(1) If yes, provide the date approved and ADAMS accession number.

October 20, 2017, ML17306A603

(2) If yes, provide a summary of modifications or other changes to the existing system.

A.6-New Points of Contact, C.7-8 New questions for this Update.

8. Do you have an NRC system Enterprise Architecture (EA)/Inventory number?

Yes

a. If yes, please provide Enterprise Architecture (EA)/Inventory number.

3633

b. If, no, please contact EA Service Desk to get Enterprise Architecture (EA)/Inventory number.

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, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

General Public—who work at, or for, an NRC licensee, vendors, certificate holders, and/or applicants; including contractors.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (be specific – e.g. SSN, Place of Birth, Name, Address)?

The individual's first and last name.

c. Is information being collected from the subject individual?

Yes

(1) If yes, what information is being collected?

Individual's name is taken as sworn testimony during an Office of Investigations (OI) investigation.

d. Will the information be collected from individuals who are not Federal employees?

Yes

(1) If yes, does the information collection have OMB approval?

No, the collection of information needed to identify a respondent is exempt from the requirements of the Paperwork Reduction Act (5 CFR 1320.3(h)(1))

(a) If yes, indicate the OMB approval number:

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

Internal files

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

OI investigation report and enforcement action.

f. Is the information being collected from external sources (any source outside of the NRC)?

No

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

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Information is taken as sworn testimony by the individual during an OI investigation. Individual's name is entered into the system manually by an enforcement specialist.

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

Information collected by OI recording of testimony and field notes. Data provided to OE through issuance of the OI investigation report.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

N/A

(1) If yes, identify the type of information (be specific).

N/A

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

N/A

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 data in this system.

To allow the office to manage case work, and track sanctions taken against individuals, and trend individual enforcement actions.

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

Yes

3. Who will ensure the proper use of the data in this system?

OE management

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

IATS system is comprised of a SharePoint list hosted on the NRC's SharePoint site (https://usnrc.sharepoint.com/teams/OE-Enforcement-Program/). Data elements are generally limited to (1) a person's first and last name, (2) name of employer and location (e.g., plant), (3) name of responsible enforcement specialist, (4) action taken (if applicable), date issued and ADAMS Accession No., and (5) the individual action case number ("IA Number"). Additional information about IATS is documented in OE's internal Office Instruction OE-ENF-108.

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

OE's internal Office Instruction OE-ENF-108

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

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).
No

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

Yes

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

By individual's name or unique tracking number

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes

a. If "Yes," provide name of SORN and location in the Federal Register.

Federal Register, Vol. 84, No. 248, December 27, 2019,
pgs. 71539-71541

8. If the information system is being modified, will the SORN(s) require amendment or revision?

No

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

No

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

10. List the report(s) that will be produced from this system.

- Current restricted individual list.
- Banned individual list.
- Types of violations/orders issued.
- Licensed vs. non-licensed individual list
- Actions taken since a specific period in time.

a. What are the reports used for?

Identify if individual previously committed a violation, and trending.

b. Who has access to these reports?

OE specialists and regional and program office enforcement specialists who have a need to use the system.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

OE and regional and program office enforcement specialists who have a need to use the system.

(1) For what purpose?

Identify if an individual had previously committed a violation of NRC requirements.

(2) Will access be limited?

Yes

2. Will other NRC systems share data with or have access to the data in the system?

No

(1) If yes, identify the system(s).

(2) How will the data be transmitted or disclosed?

3. Will external agencies/organizations/public have access to the data in the system?

No external access to the database; however, the sanction against the individual is made public on the NRC external website at the time the violation is issued to the individual. If a violation is committed by the individual, the individuals' name, identifier (IA number) and the sanction are listed on the NRC public website for a period of time to inform licensees and the general public of actions taken against individuals (e.g., banning from working at NRC licensed facilities).

(1) If yes, who?

(2) Will access be limited?

(3) What data will be accessible and for what purpose/use?

(4) How will the data be transmitted or disclosed?

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - 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). These determinations are made through records retention schedules and NARA statutes (44 U.S.C., 36 CFR). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management (RIM) and NARA's Universal Electronic Records Management (ERM) requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule(NUREG-0910), or NARA's General Records Schedules?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

Case files are permanent records and are transferred to NARA with related indexes when 20 years old in accordance with NARA approved schedule N1-431-00-05, Item 3a(1) and 3.a(4); found in NRC's Comprehensive Records Schedule, NUREG-0910, Revision 4 in Schedule 2, Part 10, item 2.a(1) and 2.a(4).

All other enforcement actions and violations are destroyed 10 years after the actions are cut off, in accordance with NARA approved schedule N1-431-00-05, Item 3.b(1) and 3.b.(4); also found in NUREG 0910, Revision 4, Schedule 2, Part 10, item 2.b(1) and 2.b(4).

b. If no, please contact the Records and Information Management (RIM) staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

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

IATS resides on the NRC LAN as a SharePoint List under the Office of Enforcement/Enforcement Program sub-folder. Access to the database is restricted to current OE, regional and program office enforcement specialists who have a need to use the system. Security is provided by establishing unique SharePoint permissions (i.e., IATS does not inherit the SharePoint site's parent permissions) through membership in either the "IATS Owners" or "IATS Users" groups. As a result, the IATS SharePoint platform controls and prevents misuse by ensuring that users are properly logged on to the LAN (password protected) and verifying that the LAN ID has permission to view, edit or otherwise change the list. Membership in IATS user groups is periodically reviewed by the system's owners.

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

IATS system data is limited to (1) a person's first and last name, (2) name of employer and location (e.g., plant), (3) name of responsible enforcement specialist, (4) action taken (if applicable), date issued and ADAMS Accession No., and (5) "IA Number." As such, the potential misuse of data is inherently narrow, and would be limited to releasing the name of a person who had been involved in a case where there was potential wrongdoing and where no action was taken (typically non-public information). Access to this information is controlled by granting system permissions to NRC employees with a current need to access IATS. System owners review access to IATS on a periodic basis.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes

(1) If yes, where?

OE Office Instruction OE-ENF-108, "Use of the Individual Actions Tracking System."

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

Yes

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

See answer to Question F.1 above.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

See answer to Question F.1 above.

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

No

a. If yes, what will be collected?

7. Will contractors be involved with the design, development, or maintenance of the system?

No

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or PII contract clauses are inserted in their contracts.

- *FAR clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*
- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

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

Access to IATS is restricted to enforcement specialists through the use of unique SharePoint permissions associated with the list (i.e., the SharePoint list does not inherit permissions). The unique permissions are periodically reviewed by OE to add or remove names from the list of authorized users.

9. Is the data secured in accordance with FISMA requirements?

The security of IATS data relies on the protections provided by the NRC's SharePoint system. OCIO ensures that SharePoint information is secured in accordance with the appropriate FISMA requirements.

a. If yes, when was Certification and Accreditation last completed?

SharePoint is authorized under the Information Technology Infrastructure (ITI) Authority to Operate which has been continuously authorized since September 22, 2017.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMS/CSB Staff)

System Name: Individual Action Tracking System (IATS)

Submitting Office: Office of Enforcement (OE)

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
Covered by Systems of Records Notice - NRC-3, Enforcement Actions against Individuals.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	07/10/2020

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:
The collection of information needed to identify a respondent is exempt from the requirements of the Paperwork Reduction Act (5 CFR 1320.3(h)(1))

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	7/2/2020

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.

Comments:

Reviewer's Name	Title	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	7/10/2020

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:

/RA/ Date August 28, 2020

Clarissa L. Evans Brown, Chief
Computer Security Branch
Governance & Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **George Wilson, Director, Office of Enforcement**	
Name of System: **Individual Action Tracking System (IATS)**	
Date CSB received PIA for review: **June 15, 2020**	Date CSB completed PIA review: **July 10, 2020**
Noted Issues:	
Clarissa L. Evans Brown, Chief Computer Security Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: **/RA/ August 28, 2020**
Copies of this PIA will be provided to: *Tom Ashley, Director* *IT Services Development & Operation Division* *Office of the Chief Information Officer* *Jonathan Feibus* *Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	