

## 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:** October 20, 2017

#### **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:**

<b>Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Tom Marenchin	OE/EB	301-287-9518
<b>Business Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Tom Marenchin	OE/EB	301-287-9518
<b>Technical Project Manager</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Tom Marenchin	OE/EB	301-287-9518
<b>Executive Sponsor</b>	<b>Office/Division/Branch</b>	<b>Telephone</b>
Anne Boland	Director, OE	301-287-9527

**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  Other (Explain)

PIA supports a system that has been in existence for several decades.

- b. **If modifying an existing system, has a PIA been prepared before?**

Yes

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

March 13, 2008, ML080650740

- (2) **If yes, provide a summary of modifications to the existing system.**

This PIA update is being performed in accordance with Agency-wide instructions, dated September 14, 2007, from the Deputy Chief Information Officer. Updates to the March 13, 2008 version have been incorporated.

**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).**

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)?**

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 a sworn testimony during an Office of Investigations (OI) investigation.

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

Yes

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

No

**(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**

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?**

No

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

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

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? (Be specific.)**

By individual's name or unique tracking number

**7. 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?**

**8. 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?**

N/A

**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 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 are required under 36 CFR 1234.10. The following questions are intended to determine whether the records in the system have an approved records retention schedule or if one will be needed.*

1. Can you map this system to an applicable retention schedule in [NUREG-0910](#), or the [General Records Schedules](#) at <http://www.archives.gov/records-mgmt/grs>?

Yes

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished. For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to a file for transfer based on their approved disposition?

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 the answer to question E.1 is yes, skip to F.1. If the response is no, complete question E.2 through question E.7.

2. If the records cannot be mapped to an approved records retention schedule, how long do you need the records? Please explain.

3. Would these records be of value to another organization or entity at some point in time? Please explain.

4. **How are actions taken on the records? For example, is new data added or updated by replacing older data on a daily, weekly, or monthly basis?**
  
5. **What is the event or action that will serve as the trigger for updating, deleting, removing, or replacing information in the system? For example, does the information reside in the system for three years after it is created and then is it deleted?**
  
6. **Is any part of the record an output, such as a report, or other data placed in ADAMS or stored in any other location, such as a shared drive or MS SharePoint?**
  
7. **Does this system allow for the deletion or removal of records no longer needed and how will that be accomplished?**

**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 LAD 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

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

None

**9. Are 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?**

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

**System Name:** Individual Action Tracking System (IATS)

**Submitting Office:** Office of Enforcement

**A. PRIVACY ACT APPLICABILITY REVIEW**

Privacy Act is not applicable.

Privacy Act is applicable.

**Comments:**

Maintained as part of NRC-3, Enforcement Actions against Individuals.

Reviewer's Name	Title	Date
Sally A. Hardy	Privacy Officer	11/27/17

**B. INFORMATION COLLECTION APPLICABILITY DETERMINATION**

No OMB clearance is needed.

OMB clearance is needed.

Currently has OMB Clearance. Clearance No. \_\_\_\_\_

**Comments:**

Reviewer's Name	Title	Date
David Cullison	Agency Clearance Officer	11/27/17

**C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION**

- 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	Date
Marna B. Dove	Sr. Program Analyst, Electronic Records Manager	11/30/17

**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.
- 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 December 1, 2017  
Anna T. McGowan, Chief  
Information Services Branch  
Governance & Enterprise Management  
Services Division  
Office of the Chief Information Officer

**TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/  
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS**

TO: <b>Anne Boland, Director, Office of Enforcement</b>	
Name of System: <b>Individual Action Tracking System (IATS)</b>	
Date ISB received PIA for review: <b>November 2, 2017</b>	Date ISB completed PIA review: <b>November 30, 2017</b>
<p><b>Noted Issues:</b></p> <p>NRC-3, Enforcement Actions against Individuals.</p>	
Anna T. McGowan, Chief Information Services Branch Governance & Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date:  <b>/RA/ December 1, 2017</b>
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Tom Rich, Director IT Services Development &amp; Operation Division Office of the Chief Information Officer</i></p> <p><i>Jonathan Feibus Chief Information Security Officer (CISO) Governance &amp; Enterprise Management Services Division Office of the Chief Information Officer</i></p>	