

---

# U.S. Nuclear Regulatory Commission

---



## **Privacy Impact Assessment Insider Threat Program Office of Administration**

**Version 02  
12/01/2023**

**Instruction Notes:**

*Please do not enter the PIA document into ADAMS. An ADAMS accession number will be assigned through the e-Concurrence system which will be handled by the Privacy Team*

**Template Version 2.0 (08/2023)**

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## Document Revision History

Date	Version	PIA Name/Description	Author
12/01/2023	1.1	Convert to new template	Denis Brady
09/10/2020	1.0	Insider Threat Program Initial Release	Denis Brady

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## Table of Contents

1	Description	1
2	Authorities and Other Requirements	2
3	Characterization of the Information	3
4	Data Security	4
5	Privacy Act Determination	7
6	Records and Information Management-Retention and Disposal	8
7	Paperwork Reduction Act	10
8	Privacy Act Determination	11
9	OMB Clearance Determination	12
10	Records Retention and Disposal Schedule Determination	13
11	Branch Chief Review and Concurrence	14

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

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:** Insider Threat Program.

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

**Date Submitted for review/approval:** December 1, 2023.

*Note: When completing this PIA do not include any information that would raise security concerns or prevent this document from being made publicly available.*

# 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 program uses Microsoft Products, as employed by the agency, to document and maintain program documents.

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

<input type="checkbox"/> PowerApps	<input type="checkbox"/> Public Website
<input type="checkbox"/> Dashboard	<input type="checkbox"/> Internal Website
<input checked="" type="checkbox"/> SharePoint	<input type="checkbox"/> None
<input type="checkbox"/> 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	
<input type="checkbox"/>	New system/project
<input checked="" type="checkbox"/>	Modification to an existing system/project. <i>If modifying or making other updates to an existing system/project, provide the ADAMS ML of the existing PIA and describe the modification.</i> ADAMS Main Library (ML) ML16089A240.
<input checked="" type="checkbox"/>	Annual Review <i>If making minor edits to an existing system/project, briefly describe the changes</i>

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

	<i>below.</i>
<input type="checkbox"/>	Other (explain)

**1.3 Points of Contact:** (Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary.)

	Project Manager	System Owner/Data Owner/Steward	ISSO	Business Project Manager	Technical Project Manager	Executive Sponsor
<b>Name</b>	Denis Brady	Denis Brady	Tamar Katz		Michael England	Jennifer Golder
<b>Office /Division /Branch</b>	ADM/DFS/S/FSB	ADM/DFS/SM OB	ADM/DRMA /BITT		ADM/DFS/SM OB/SOT	ADM
<b>Telephone</b>	301-415-5768	301-415-5768	301-415-2500		301-415-0178	301-287-0741

## 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
<input type="checkbox"/>	Statute	
<input checked="" type="checkbox"/>	Executive Order	13587
<input type="checkbox"/>	Federal Regulation	
<input type="checkbox"/>	Memorandum of Understanding/Agreement	
<input type="checkbox"/>	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).**

Purpose of the system is to house individual's personal data related to a reported insider threat concern or anomalous activity on a classified and/or safeguards information system. As well as, the review and analysis of the concern and any disposition of the concern.

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

Data to be collected is the concern, individual's name, biographical information, and personnel security file information, user activity monitoring on classified and safeguards information systems, and disposition of the concern.

**If the project collects Social Security numbers, state why this is necessary and how it will be used.**

N/A.

### 3 Characterization of the Information

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

Category of individual	
<input checked="" type="checkbox"/>	Federal employees
<input checked="" type="checkbox"/>	Contractors
<input type="checkbox"/>	Members of the Public (any individual other than a federal employee, consultant, or contractor)
<input checked="" type="checkbox"/>	Licensees
<input type="checkbox"/>	<b>Other</b>

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			
<input checked="" type="checkbox"/>	Name	<input type="checkbox"/>	Resume or curriculum vitae
<input checked="" type="checkbox"/>	Date of Birth	<input type="checkbox"/>	Driver's License Number
<input type="checkbox"/>	Country of Birth	<input type="checkbox"/>	License Plate Number
<input checked="" type="checkbox"/>	Citizenship	<input type="checkbox"/>	Passport number
<input checked="" type="checkbox"/>	Nationality	<input type="checkbox"/>	Relatives Information
<input checked="" type="checkbox"/>	Race	<input type="checkbox"/>	Taxpayer Identification Number
<input type="checkbox"/>	Home Address	<input type="checkbox"/>	Credit/Debit Card Number
<input type="checkbox"/>	Social Security number (Truncated or Partial)	<input type="checkbox"/>	Medical/health information
<input checked="" type="checkbox"/>	Gender	<input type="checkbox"/>	Alien Registration Number
<input checked="" type="checkbox"/>	Ethnicity	<input type="checkbox"/>	Professional/personal references
<input type="checkbox"/>	Spouse Information	<input type="checkbox"/>	Criminal History
<input type="checkbox"/>	Personal e-mail address	<input checked="" type="checkbox"/>	Biometric identifiers (facial images, fingerprints, iris scans)
<input type="checkbox"/>	Personal Bank Account Number	<input type="checkbox"/>	Emergency contact e.g., a third party to

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

Categories of Information			
			contact in case of an emergency
<input type="checkbox"/>	Personal Mobile Number	<input type="checkbox"/>	Accommodation/disabilities information
<input type="checkbox"/>	Marital Status	<input type="checkbox"/>	<b>Other</b>
<input type="checkbox"/>	Children Information		
<input type="checkbox"/>	Mother's Maiden Name		

**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).**

The data that will be reviewed and summarized is collected from other System of Records that may collect the information directly from the individual.

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

N/A.

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

No, the information is not being directly collected from the individual. The data that will be reviewed and summarized and will be from other System of Records that may collect the information directly from the individual. We will not be re-collecting already provided information like access records for their badge access.

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

The collected data will be corroborated with other data.

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

N/A.

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

Inaccurate and erroneous information corrections can be made in the other Systems of Record used by this program.

## **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).**

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

The Insider Threat Program Manager, Coordinator, Technical Project Manager, and Senior Agency Official.

**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.**

- NRC-2 – Biographical Information
- NRC-3 – Enforcement actions against individuals
- NRC-4 – Conflict of Interest
- NRC-8 – Employee disciplinary actions, appeals, grievances, and complaints
- NRC-11 – General Personnel (Official Personnel File and related)
- NRC-18 – Office of the Inspector General (with prior OIG approval)
- NRC-19 – Official personnel training
- NRC-20 – Official travel
- NRC-21 – Payroll
- NRC-22 – Personnel performance appraisals
- NRC-23 – Office of Investigations indices, files, & associated records (with prior OI coordination)
- NRC-32 – Office of the Chief Financial Officer financial transactions & debt collection
- NRC-36 – Employee locator records
- NRC-39 – Personnel security files & associated records
- NRC-40 – Facility security access control records
- NRC-45 – Digital certificates for personal identity verification

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

N/A.

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

Agreement Type	
<input type="checkbox"/>	Contract Provide Contract Number:
<input type="checkbox"/>	License Provide License Information:
<input type="checkbox"/>	Memorandum of Understanding Provide ADAMS ML number for MOU:
<input type="checkbox"/>	Other
<input checked="" type="checkbox"/>	None

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

Hard copy information is stored in a GSA approved container. The safe combination for which the safe is secured is only provided to three individuals which limits the access.



Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

**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).**

The data will be transmitted and disclosed in hardcopy format only due to the classification of the information.

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

Hard copy information is stored in a GSA approved container. The safe combination for which the safe is secured is only provided to three individuals which limits the access.

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

No.

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

No.

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

The GSA container will have a SF-702 form attached.

**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.**

Information Technology Infrastructure (ITI)

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

Authorization Status	
<input type="checkbox"/>	Unknown
<input checked="" type="checkbox"/>	No <i>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.</i>
<input type="checkbox"/>	In Progress provide the estimated date to receive an ATO. Estimated date:
<input checked="" type="checkbox"/>	Yes Indicate the data impact levels (Low, Moderate, High, Undefined) approved by the Chief Information Security Officer (CISO)

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

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.**

20090005.

## 5 Privacy Act Determination

### 5.1 Is the data collected retrieved by a personal identifier?

Mark the appropriate response.

Response	
<input checked="" type="checkbox"/>	<b>Yes, the PII is retrieved by a personal identifier (i.e., individual's name, address, SSN, etc.)</b>
<input type="checkbox"/>	<b>List the identifiers that will be used to retrieve the information on the individual.</b>
<input type="checkbox"/>	<b>No, the PII is not retrieved by a personal identifier. If no, explain how the data is retrieved from the project.</b>

**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	
<input checked="" type="checkbox"/>	<b>Yes, this system is covered by an existing SORN. (See existing SORNs: <a href="https://www.nrc.gov/reading-rm/foia/privacy-systems.html">https://www.nrc.gov/reading-rm/foia/privacy-systems.html</a> ) Provide the SORN name, number, (List all SORNs that apply): NRC 39, NRC 40, NRC 3</b>
<input type="checkbox"/>	<b>SORN is in progress</b>
<input type="checkbox"/>	<b>SORN needs to be created</b>
<input type="checkbox"/>	<b>Unaware of an existing SORN</b>
<input type="checkbox"/>	<b>No, this system is not a system of records and a SORN is not applicable.</b>

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

**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	
<input type="checkbox"/>	Privacy Act Statement
<input checked="" type="checkbox"/>	Not Applicable
<input type="checkbox"/>	Unknown

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

Neither. Information is derived from other Systems of Record.

## 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:**

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

- 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](mailto: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?**

<input type="checkbox"/>	<a href="#">NUREG-0910, “NRC Comprehensive Records Disposition Schedule</a>
<input checked="" type="checkbox"/>	<a href="#">NARA’s General Records Schedules</a>
<input type="checkbox"/>	Unscheduled

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

<b>System Name (include sub-systems, platforms, or other locations where the same data resides)</b>	Insider Threat Program
<b>Records Retention Schedule Number(s)</b>	See schedules/dispositions below.
<b>Approved Disposition Instructions</b>	See schedules/dispositions below.
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 accessibility, reliability, integrity, and disposition.	TBD
<b>Disposition of Temporary Records</b>  Will the records/data or a composite be automatically or manually deleted once they reach their approved retention?	<a href="#">GRS 5.6, item 210, item 220, item 230, and item 240.</a>  See table below.
<b>Disposition of Permanent Records</b>  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?  <a href="#">NRC Transfer Guidance (Information and Records Management Guideline - IRMG)</a>	TBD

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

Schedule Number	Schedule Title	Disposition Instructions
<a href="#">GRS 5.6 item 210</a>	Insider threat administrative and operations records	Temporary. Destroy when 7 years old, but longer retention is authorized if required for business use.
<a href="#">GRS 5.6 item 220</a>	Insider threat inquiry records	Temporary. Destroy 25 years after close of inquiry, but longer retention is authorized if required for business use.
<a href="#">GRS 5.6 item 230</a>	Insider threat information	Temporary. Destroy when 25 years old, but longer retention is authorized if required for business use.
<a href="#">GRS 5.6 item 240</a>	Insider threat user activity monitoring (UAM) data	Temporary. Destroy no sooner than 5 years after inquiry has been opened, but longer retention is authorized if required for business use.

**Note:** Information in *Section 6, Records and Information Management-Retention and Disposal*, does not need to be fully resolved for final approval of the privacy impact assessment.

## 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?

Yes.

### 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?

N/A.

*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>.*

**STOP HERE - The remaining pages will be completed by the Privacy Officer, Records Management, and Information Collections Team.**

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## 8 Privacy Act Determination

**Project/System Name:** Insider Threat Program (ITP).

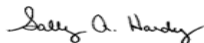
**Submitting Office:** Office of Administration.

### Privacy Officer Review

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

**Comments:**

The information is collected from NRC systems that are covered by existing SORNs.

Reviewer's Name	Title
 Signed by Hardy, Sally on 12/27/23	Privacy Officer


## 9 OMB Clearance Determination

### NRC Clearance Officer Review

Review Results	
<input checked="" type="checkbox"/>	No OMB clearance is needed.
<input type="checkbox"/>	OMB clearance is needed.
<input type="checkbox"/>	Currently has OMB Clearance. Clearance No. _____

**Comments:**

The Insider Threat Program maintains information about Federal employees, Federal contractors, and NRC licensees. The information is collected from NRC systems that are covered by existing OMB clearances.

Reviewer's Name	Title
 Signed by Cullison, David on 12/11/23	Agency Clearance Officer


Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## 10 Records Retention and Disposal Schedule Determination

### Records Information Management Review

Review Results	
<input type="checkbox"/>	No record schedule required.
<input type="checkbox"/>	Additional information is needed to complete assessment.
<input type="checkbox"/>	Needs to be scheduled.
<input checked="" type="checkbox"/>	Existing records retention and disposition schedule covers the system - no modifications needed.

**Comments:**

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



Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## 11 Branch Chief Review and Concurrence

Review Results	
<input type="checkbox"/>	This project/system <b>does not</b> collect, maintain, or disseminate information in identifiable form.
<input checked="" type="checkbox"/>	This project/system <b>does</b> 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

Insider Threat Program	Version 02
Privacy Impact Assessment	12/01/2023

## ADDITIONAL ACTION ITEMS/CONCERNS

<b>Name of Project/System:</b> Insider Threat Program (ITP)	
<b>Date CISD received PIA for review:</b> December 1, 2023	<b>Date CISD completed PIA review:</b> December 21, 2023
<b>Action Items/Concerns:</b>          	
<p><i>Copies of this PIA will be provided to:</i></p> <p><i>Caroline Carusone</i>  <i>Director</i>  <i>IT Services Development and Operations Division</i>  <i>Office of the Chief Information Officer</i></p> <p><i>Garo Nalabandian</i>  <i>Deputy Chief Information Security Officer (CISO)</i>  <i>Office of the Chief Information Officer</i></p>	