United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Environmental Protection Agency – Insider Threat Program (ITP)	
Preparer: John C. Martin	**Office: Office of the Administrator - Office of Homeland Security**
Date: April 22, 2020	**Phone: 202-564-2616**
Reason for Submittal: New PIA_X___ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☒	
Operation & Maintenance ☐ Rescindment/Decommissioned ☐ **Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).** **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**	

Provide a general description/overview and purpose of the system:

EPA is establishing an Insider Threat Program (ITP) pursuant to Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The ITP will have the capacity to gather, integrate, and centrally analyze and respond to key threat-related information and monitor employee use of classified networks. The ITP may maintain information from any EPA office, program, record, or source, including but not limited to records from Information Security, Personnel Security, and Human Resources.

EPA's ITP will be stored and maintained electronically on the Joint Worldwide Intelligence

Communications System (JWICS), which is owned and operated by the Intelligence Community (IC). EPA has an agreement with the IC to use this system for official business. These records will be stored in files associated with an individual and safeguarded in the Office of Homeland Security's Sensitive Compartmented Information Facility (SCIF). Access to the SCIF is restricted and safeguarded according to the requirements of Executive Order 13526, Classified National Security Information, and other applicable authorities.

EPA's ITP utilizes information supplied by personnel, prospective personnel, contractors, and grantees that is provided to EPA to gain access to facilities, information, equipment, networks, or systems. The ITP also uses tips and leads received by other means, such as email, telephone, or website submissions.

EPA's ITP does not directly conduct investigative or enforcement activities but does conduct preliminary inquiries. When certain thresholds are met, the ITP refers insider threat matters to appropriate entities for further investigation. These entities may include external partners like the Federal Bureau of Investigation (FBI), the IC, or internal offices like the Security Management Division, the Office of Human Resources, or the Office of Inspector General (OIG). An entity receiving a referral from the ITP uses its own existing legal authorities to conduct any required administrative or investigative activity resulting from the referral. No additional authorities are gained or implied as a result of the referral. The ITP retains records on matters referred to other entities and records on the final disposition or resolution of referred insider threat matters.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

EPA is authorized to collect this information pursuant to the following:

1. Executive Order 13587 Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
2. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
3. Executive Order 13467 Reforming Processes Related to Suitability for Government Employment Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
4. Executive Order 12968 Access to Classified Information (as amended)
5. Executive Order 13556 Controlled Unclassified Information
6. Executive Order 13526 Classified National Security Information
7. Executive Order 12333 United States Intelligence Activities (as amended)

8. 5 U.S.C. 301 Departmental Regulations
9. 5 U.S.C. 7106(a) Management Rights
10. 44 U.S.C. 2104(a) (as amended)
11. Section 811 of the Intelligence Authorization Act for 1995, Public Law Number 103-359, 50 U.S.C. 402a
12. White House Memorandum, Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies, August 23, 1996
13. Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts, August 5, 1993

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, a security system plan is in place for JWICS. The system is governed by the rules and regulations related to the handling of classified information, including Executive Order 12968 Access to Classified Information, and Executive Order 13526 Classified National Security Information. The Intelligence Community has an Authorization to Operate this system.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

The ITP requires information from various sources to performs its functions. The ITP derives information for analysis from multiple sources within EPA. Such records and information may include or be derived from:

All relevant counterintelligence and security databases and files, including personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

All relevant unclassified and classified network information generated by Information Assurance elements, including personnel names, email addresses, usernames and aliases, levels of network access, audit data, unauthorized use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

All relevant Human Resources databases and files as long as may be necessary for resolving or clarifying insider threat matters, including: personnel files, payroll and voucher files, outside work and activities requests, disciplinary files, and personal contact records..

The ITP may collect the following types of information:

Information related to EPA security investigations, including authorized physical, personnel, information systems, communication security investigations, and information systems security analysis and reporting;

Records relating to the management and operation of EPA physical, personnel, information systems and communications security program;

Reports of investigation regarding security violations or misconduct;

Any information related to the management and operations of the ITP.

2.2 What are the sources of the information and how is the information collected for the system?

Sources of the information originate from internal EPA offices such as the Security Management Division, the Office of Mission Support, and the Office of Human Resources. The ITP also receives records from outside entities such as the FBI, DHS, the IC, and other departments and agencies. The ITP collects information through requests to other EPA

components or outside entities. The ITP may also receive the information directly without an ITP request.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of EPA-owned records and other federal agency records is dependent on the original source. The Insider Threat Program Manager will be notified if an ITP Hub Member identifies inaccurate information in records. The original source of the information will be notified to correct the information.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Because the ITP receives information from other EPA components and other federal agencies, there is a risk that the information will become outdated and inaccurate.

Mitigation:

The ITP will routinely refresh information obtained from various sources so the ITP information accurately reflects any changes to the records contained in the underlying information source and the addition or deletion of those records.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, the electronic records will be stored on JWICS in shared folders. Access to these folders will be strictly controlled by the Insider Threat Program Manager. Only authorized ITP personnel who require access to the information as part of the performance of their official duties and who have the appropriate clearances or permissions will have access to the ITP information. Access is strictly controlled using Public Key Infrastructure (PKI)

Certificates that block access to those without permission granted by the ITP Program Manager. The number of ITP personnel is limited in order to prevent widespread access to the sensitive information available to the ITP. All ITP personnel are required to hold and maintain at least a SECRET level clearance and sign a Non-Disclosure Agreement. ITP operations are conducted in a restricted access SCIF in order to maximize the security of the location and effectively monitor the activities of ITP personnel. The policies and procedures that govern the operation of the SCIF are described in the National Security Information Handbook developed and maintained by the Security Management Division. The ITP maintains access records showing which ITP personnel have accessed the information. ITP management revokes a user's access when no longer needed or permitted. No personnel outside of the ITP are given access to the data until such time that the ITP refers the matter in accordance with the ITP procedures.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access control level is documented in the JWICS Memorandum of Understanding (MOU) between EPA and the Intelligence Community.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, currently the ITP Hub is comprised of representatives of OHS, OARM, OMS, OGC, and OIG. Other EPA Offices participate on an as-needed basis, as determined by the ITP Program Manager. Access to the ITP system is limited as described above. Also, information from the ITP is provided to EPA components or other federal agencies when the ITP refers a matter in accordance with ITP policies and procedures.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA employees that are part of the Insider Threat Program will have access to the data/information only when it is determined necessary by the Insider Threat Program Manager. No contractors will have access to the data/information.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records in the ITP system are subject to the National Archives and Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry" are destroyed 25 years after the close of the inquiry, but longer retention is authorized if required for business use; (b) records containing "insider threat information" are destroyed when 25 years old, but longer retention is

authorized if required for business use; (c) insider threat user activity monitoring (UAM) data is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records are destroyed when 7 years old, but longer retention is authorized if required for business use.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

Low risk that the records would be detained longer than needed.

Mitigation:

Records Control Schedule is strictly followed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes. When an insider threat is identified and it is determined classified information was disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, EPA is required by 50 U.S.C. 3381(e) to notify the FBI and provide access to any EPA records needed for investigative purposes. If other misconduct that raises law enforcement or national security concerns is uncovered by the ITP, the misconduct is referred to the appropriate investigative agency at the federal, state, or local level.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The sharing of information out of the ITP is compatible with the original purpose of the collection. Generally, information is shared for law enforcement, intelligence, or national security purposes to accomplish agency functions related to countering potential and actual insider threats.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

The ITP uses existing processes and procedures within OHS for reviewing and approving information sharing agreements, MOUs, new uses of the information, and new access to the

system by organizations within EPA and outside EPA. Requests for access to records, MOUs, new uses of information and new access to ITP data by organizations both within EPA and outside EPA, will be reviewed and approved by the ITP Program Manager in consultation with EPA's Office of General Counsel.

4.4 Does the agreement place limitations on re-dissemination?

Recipients of information from the ITP are provided the information consistent with their authorities to investigate or act on the referral. These recipients maintain the information consistent with their authorities. As a condition of accessing ITP information, individuals are required to sign Non-Disclosure Agreements (NDA) which place limits on re-dissemination. The NDAs will be approved by EPA's Office General Counsel and administered by the ITP Program Manager. Only individuals with a need to know are able to gain access to ITP information.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Authorized users are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information either intentionally or unintentionally.

Mitigation:

All ITP personnel are required to complete annual specialized privacy training, including the appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. The use of the ITP system and the access to ITP information is monitored. Should a user inappropriately disclose this information, they are subject to the loss of access and disciplinary action up to and including termination. Additionally, all ITP personnel are required to sign Non-Disclosure Agreements, which contain specific provisions regarding the non-disclosure of ITP information without the appropriate permissions and approvals.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy- based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The Insider Threat Program is subject to audits from EPA's OIG and reviews by the Office of the Director of National Intelligence's Insider Threat Task Force. These audits and reviews help ensure the information is used for their intended legal purpose, consistent with EPA policy and for the purpose stated in the Privacy Impact Assessment.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

EPA Information Security and Privacy Awareness training is required annually for all users of this system. All Insider Threat Program personnel will go thru annual, mandatory Privacy training, conducted by EPA, related to their responsibilities in the Insider Threat Program and the handling of sensitive information.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk that improper audits may lead to inaccurate information or unaccounted data.

Mitigation:

Any audits or oversight conducted by the OIG will be done so according to all policies and procedures in order to protect the information and limit the number of people with access.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

EPA maintains Insider Threat Program records to manage insider threat matters; facilitate insider threat inquiries; review and refer information and activities associated with counterintelligence complaints, inquires, and referrals; identify potential threats; refer potential insider threats to internal and external partners; provide statistical reports; and meet other insider threat reporting requirements.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

Yes. The information will be retrieved by name or social security number.

6.3 What type of evaluation has been conducted on the probable or potential effect on the privacy of individuals whose information is maintained in the system of records?

The ITP Program Manager has worked extensively with EPA's Office of General Counsel and EPA's Privacy Office to evaluate the potential or probable effect on individuals' privacy. We have built administrative, physical, and technical controls around the data to

limit the people who have access. These controls will help ensure only people with a need to know can access the information for the performance of their official duties, and the privacy of those with information in the system is protected.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Any unauthorized disclosure, access, or use of the information will result in adverse action against the offending individual.

Mitigation:

All Insider Threat Program members sign the required Non-Disclosure Agreement and participate in a mandatory annual Insider Threat training to prevent the unauthorized sharing of information. In addition, all records will be maintained and all access to records will be consistent with Executive Order 13526 and the NSI Program Handbook.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

EPA has user agreements in place, which include consent to monitor user activity on EPA computer systems. If users do not consent to the banner language and user agreements, they will not have access to the system.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

There is a low risk of inadequate notice.

Mitigation:

The notice provided by the EPA User Agreement allows system users to agree to the notice and proceed, or decline the terms and be denied access to the system. This agreement and notice is required by the Insider Threat Program and consistent with Executive Order 13587.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information in this system of records may submit a written request to the EPA Privacy Act Officer pursuant to 40 CFR part 16. Individuals seeking information about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

There is no risk, because there are appropriate procedures in place for redress.

Mitigation:

None.