

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: <u>https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx</u>

 System Name: Environmental Protection Agency - Insider Threat Inquiry Management (E-ITIM)

 Preparer: Ken Collins
 Office: Office of the Administrator - Office of Homeland Security

 Date: March 5, 2021
 Phone: 202-564-1676

 Reason for Submittal: Revised PIA
 Environmental Protection Agency - Insider Threat Inquiry Management (E-ITIM)

This system is in the following life cycle stage(s): IMPLEMENTATION

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 developed an Insider Threat Program (ITP) to manage insider threat matters within EPA. The ITP is mandated by Executive Order 13587, "*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,*" issued October 7, 2011, which requires Federal agencies to establish an insider threat detection and prevention program. The purpose of this system is to detect, deter, and mitigate insider threats. EPA will use the system to facilitate management of insider threat inquiries; identify and track potential insider threats to EPA; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and generate statistical reports and meet other insider threat reporting requirements.

EPA's ITP utilizes information obtained from software that monitors EPA users' activity on U.S. Government assigned computer equipment and network information supplied by individuals to the agency or by the individual's employer; information provided to the agency to gain access to EPA facilities, information, equipment, networks, or systems; publicly available information obtained from open-source platforms; any agency records for which the ITP has been given authorized access; and any federal, state, tribal, local government, or private sector records for which the ITP has been given authorized access. The ITP receives tips and leads by other means, such as email or telephone. Tips and leads may also be provided by members of the public.

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 such as the Federal Bureau of Investigation (FBI) or the Intelligence Community (IC), or offices within EPA such as the Security Management Division (SMD), the Office of Human Resources (OHR), 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 because 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.

The PIA is being revised because the storage of the data is being moved to the agency's MS365 as a SaaS. The retrieval mechanism has changed to using PII to retrieve information the system.

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: 32 CFR Parts 2001 and 2003 (Classified National Security Information), Executive Order 13526 (Classified National Security Information), Executive Order 13587 (Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information), Intelligence Community Directive 404 (Executive Branch Intelligence Customers).

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 the unclassified network. Homeland Secure Data Network (HSDN) and Joint Worldwide Intelligence Communication System (JWICS) will be housed on the respective systems with unclassified information referencing the inquiry will be maintained in E-ITIM. The aforementioned classified systems are 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 Authorizations-to-

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?

Yes. It will be stored in a secured, access-controlled SharePoint folder within the agency's system housed on the Microsoft 365 Government Cloud platform (MS 365). MS 365 is currently FedRamp approved and CSP will provide PaaS services. Classified ITP inquiry information will be housed on the appropriate system (HSDN for Secret and JWICS for Top Secret).

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, as well as external to, EPA. Such records and information may include or be derived from: individual's name and alias(es); date and place of birth; Social Security number; addresses; open-source information accessed through EPA controlled equipment or managed networks; personal and official email addresses; citizenship; personal and official phone numbers; driver license number(s); Vehicle Identification Numbers (VINs); license plate number(s); demographic information; current employment and performance information; work history; education history; contract information; passport number(s); EPA-held travel records; gender; hair and eye color; biometric data; other physical or distinguishing attributes of an individual; medical information in relation to the inquiry; access control pass, credential number, or other identifying number(s); media obtained through authorized procedures, such as Closed Caption Television (CCTV) footage; and any other information provided to obtain access to EPA facilities or information systems. Completed standard form questionnaires issued by the Office of Personnel Management (OPM); background investigative reports and supporting documentation, including criminal background, medical, and financial data; current and former clearance status; other information related to an individual's eligibility for access to classified information; criminal history records; polygraph examination results; logs of computer activities on all EPA Information Technology (IT) systems or any EPA controlled IT systems accessed by EPA personnel; non-disclosure agreements (NDAs); document control registries; courier authorization requests; derivative

classification unique identifiers; requests for access to sensitive compartmented information (SCI); records reflecting personal and official foreign travel; facility access records; records of contacts with foreign persons; briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations. Reports of investigations or inquiries regarding security violations or misconduct, including: individuals' statements or affidavits and correspondence; incident reports; drug test results; investigative records of a criminal, civil, or administrative nature; letters, emails, memoranda, and reports; exhibits, evidence, statements, and affidavits; inquiries relating to suspected security violations; recommended remedial actions for possible security violations; and personnel files containing information about misconduct and adverse actions. Documentation pertaining to fact-finding or analytical efforts by ITP personnel to identify insider threats to EPA resources, personnel, property, facilities, or information; records of information technology events and other information that could reveal potential insider threat activities; intelligence reports and database query results relating to individuals covered by this system; information obtained from the Intelligence Community (IC), law enforcement partners, and from other agencies or organizations about individuals and/or organizations known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat; information provided by subjects and individual members of the public; and information provided by individuals who report known or suspected insider threats. 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?

Records are obtained from software that monitors EPA users' activity on U.S. Government computer equipment and managed networks; information supplied by individuals to the agency or by the individual's employer; information provided to the agency from the agency security office to gain access to EPA facilities, information, equipment, networks, or systems; publicly available information obtained from open-source platforms if accessed through the use of government furnished equipment; any agency records for which the ITP has been given access; and any federal, state, tribal, local government, or private sector records for which the ITP has been given authorized access.

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

The system does not use commercial sources or publicly available data exclusively. It may however utilize information containing publicly available data contained within other applications, such as email services, chats, etc., gathered using EPA networks.

2.4 Discuss how accuracy of the data is ensured.

Accuracy will be ensured through the use of monthly self-inspections of produced and stored data using known baseline thresholds compared against identified deviations.

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:

There is a risk that ITP data will become inaccurate or outdated because it is obtained from external sources instead of collecting from the individuals.

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. Prior to any external disclosure of information, the ITP will review all referrals to minimize the amount of information sent to the recipient to perform their official responsibilities.

Privacy Risk:

Data transmitted/transferred from external sources may be lost, corrupted, or intercepted in transit.

Mitigation:

All data being transferred via means of electronic methods will be, at a minimum, data-atrest encrypted requiring authentication from both the sender and the receiver.

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 SharePoint through EPA's government cloud platform with Microsoft 365. Access to these folders will be strictly controlled by the ITP 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 authorizations or permissions will have access to the ITP information. In addition, System Administrator (SA) duties have been limited and those with a need for access will be administered Non-

Disclosure Agreements (NDAs) emphasizing the criticality of keeping Insider Threat related material confidential. Restriction will be accomplished and monitored through SharePoint's inherent permission and role-based access structure. Personal Identity Verification (PIV) card certificates will permit or restrict access as applicable. The number of ITP personnel is limited to prevent widespread access to the sensitive information available to the ITP. All ITP personnel are required to sign a Non-Disclosure Agreement. The ITP maintains electronic access records showing personnel who have accessed or attempted to gain access to the stored information when relevant to the inquiry. ITP management revokes a user's access when no longer needed or permitted.

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

Access control levels are documented in the JWICS and HSDN Memorandum of Understanding (MOU) between EPA and the Intelligence Community respectively. Access procedures to E-ITIM will be listed within the EPA ITP Standard Operating Procedure (SOP).

Access to folders/data within MS O365 is governed by the Information Security – Access Control Procedure (<u>https://www.epa.gov/sites/production/files/2015-09/documents/cio-2150-p-01.2.pdf</u>)

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

Yes, the inquiry management database will be housed on an Office of Environmental Information Management (OEIM) platform. As such, tasks such as updates, maintenance, patching, Security Technical Implementation Guides (STIGs), etc. will need to be routinely performed through OEIM. As such, a minimal number of System Administrators will need to be granted access. These individuals will be identified, sign NDAs, and receive additional training on Insider Threat Records Management and Security provided through the Center for Development of Security Excellence (CDSE).

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 government employees assigned full-time to the ITP will have access to the data and or information only when it is determined necessary by the ITP Manager. EPA's Office of General Counsel (OGC) and Office of the Inspector General (OIG) will also be granted READ-ONLY access as part of the program's agency oversight efforts. These representatives will be identified and will be administered NDAs. In the case where an NDA is limiting in responsibility to safeguard information, such as with the OIG, the OIG policies will control over the ITP NDA requirement. At this time, no contractors have access to the system. Should contractors need to access the system the future, the ITP Program Manager will ensure that the

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:

There is a risk that records could be retained longer than needed. Users could store the data in an unsecure fashion (i.e. unencrypted, personal hard drive, etc.) which may result in the inadvertent (or willful) disclosure of information to unauthorized persons. Backup copies of O365 data could be stolen resulting in potential exposure of archived data to unauthorized persons. Additionally, backup copies of O365 data could be corrupted resulting in loss of archived data.

Mitigation:

The ITP will follow the appropriate Records Control Schedule. The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed. The Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy. The ITP Manager (or their delegee) will review all log entries for suspicious activity monthly. All backup copies are stored in an encrypted format. Further, the backup schema at the EPA results in differential backups and full backups performed on a schedule. This ensures that a minimal amount of data would be lost due to a corrupted backup file

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.

Under certain circumstances, 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. FBI 811 Referral Process provides additional information regarding the referral process to the FBI.

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

The purpose of this system is to detect, deter, and mitigate insider threats. This goal is achieved through monitoring user activity and referring potential or actual insider threats to the appropriate investigative agency at the federal, state, or local level. EO 13587 established policy regarding the creation, storage, and dissemination of insider threat related indications.

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 utilizes 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 and outside EPA. Data retained within the system will be categorized by assigning a systematic inquiry identification number based on the calendar year, example (YYYY) succeeded by a four-digit sequential number, beginning with 0001. All information requests, MOUs, new uses of information, and new access to ITP data by organizations both within EPA and outside EPA will be reviewed by the ITP Program Manager in consultation with EPA's OGC. This review will occur upon initial implementation and annually thereafter unless the need for out-of-cycle reviews arise due to policy change. Upon completion of review, existing agreements will be replaced with the newest version and previous versions will be maintained for historical purposes.

4.4 Does the agreement place limitations on re-dissemination?

Recipients of information from the EPA ITP are provided information consistent with EPA insider threat policies and records handling procedures in addition to the receiving agency's authority to act on the information contained within the referral. As a condition of accessing ITP information, individuals are required to sign EPA's ITP NDA which places limitations on re-dissemination. The NDAs will be approved by EPA's OGC and administered by the ITP Program Manager. Only individuals with a "need-to-know" and authorization to access the information can gain access to EPA 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 ITP users have access to sensitive information, including personally identifiable information (PII), as a routine part of their official duties. These users may make intentional or inadvertent disclosures of this information to unauthorized persons. Data transmitted/transferred to external sources may be lost, corrupted, or intercepted in transit. This includes traditional methods of transfers such as postal/courier/delivery services or via electronic transfers.

Mitigation:

All government assigned ITP personnel are required to complete initial and annual Insider Threat Awareness Training as well as annual Information Security and Privacy training. These trainings address proper handling of ITP system information, including appropriate uses and disclosures. The use of E-ITIM and the access to additional EPA ITP information is monitored through access control logs administered through OEIM and reviewed by EPA ITP personnel. Should EPA ITP personnel inappropriately disclose EPA ITP information, they may lose access to the system and could face disciplinary action which may include employment termination. Additionally, all EPA ITP personnel are required to sign NDA's, which contain specific provisions regarding the non-disclosure of EPA ITP information without the appropriate permissions and approvals. Furthermore, The ITP Manager (or their delegate) will review all log entries for suspicious activity monthly to identify inappropriate activity like unauthorized copying/storing of data.

IAW Directive No.: 2151-P-10.0, when data is transferred by traditional methods, such as postal/courier/delivery service, the recipient will be required to provide the Agency with a signed receipt indicating that the data was successfully received. Data transferred by traditional methods can include hardcopy documents, compact discs, external USB drives, etc. Data transmitted through electronic methods will be encrypted or at a minimum password protected. MOU/ISA/sharing documents will include language for external users addressing the proper handling of PII IAW the aforementioned directive.

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 ITP is subject to audits from EPA's OIG and reviews by the Office of the Director of National Intelligence's Insider Threat Task Force (NITTF). The purpose of these audits and reviews is to help ensure that the information is used for its intended purpose, consistent with EPA policy. Additionally, an OGC advisor will have complete access to the system and will conduct periodic compliance reviews . EPA Information Security and Privacy

Awareness training is required annually for all users of this system. All ITP personnel will go through annual, mandatory privacy training, conducted by EPA, related to their responsibilities in the ITP and the handling of sensitive information.

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

Various privacy training courses are mandated annually through EPA's Fed Talent training portal (*Information Security and Privacy Awareness Training, Records Management Training, FOIA Training, Controlled Unclassified Information Awareness Training*) in addition to several other optional training opportunities. FedTalent tracks the completion status of all EPA employees.

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 ITP records to manage and mitigate 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? 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 either by insider threat indicator trigger or through PII such as name, date of birth, address, email address, telephone number, or other identifying information belonging to the subject of the inquiry. Additionally, non-discriminate identifiers, such as EPA assigned inquiry number or EPA assigned employee ID number, may be used.

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?

EPA's ITP Program Manager, in conjunction with EPA's OGC and EPA's Privacy Office, has evaluated the potential or probable effect on individuals' privacy. Administrative, physical, and technical controls limiting access have been instituted to aid in access control, only allowing people with a "need-to-know" access to the information for the performance of their official duties.

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 could result in adverse action against the offending individual.

Mitigation:

Monitoring by ITP personnel through existing agency resources will be conducted using system access logs and system alerts for unauthorized, attempted access. Triggers will be set to notify ITP personnel when access or an attempt to access has occurred and will populate within the ITP systems log dashboard. All ITP members will be mandated to sign the required NDA and participate in mandatory initial and 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 Nationwide Suspicious Activity Reporting Initiative (NSI) Program Handbook.

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.

An Information Technology Acceptable User Agreement Policy (UAP) is administered through the agency prior to access being granted to utilize EPA computer systems and requires the user to accept the provisions prior to usage. Contained within the acceptable user agreement notice is the collection of user identifiable information for purposes of attribution when appropriate.

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 requires system users to acknowledge consent for monitoring prior to use of an EPA computer systems. Lack of consent to the banner language and user agreements will result in declination of access and use.

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 no risk of inadequate notice as the use of banners notifying EPA network users of activity monitoring is required to be acknowledged through the use of a log-on acknowledgement selection (button) prior to prompting the user to enter their password or PIN.

Mitigation:

The notice provided by the EPA User Agreement allows system users to agree to the notice and accept or decline the terms prior to gaining access to EPA's Information Technology system. This agreement and notice are required by the NITTF, 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 their 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 C.F.R. part 16. Any individual requesting information regarding E-ITIM records pertaining to him or herself should make a written request to; Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov. Freedom of Information Act (FOIA) requests can be submitted through use of the U.S. governments FOIAOnline system https://foiaonline.gov/foiaonline/action/public/home or https://www.epa.gov/foia/forms/contact-us-about-freedom-information-act-and-foia-requests#101. Written request should be addressed to:

National FOIA Office U.S. Environmental Protection Agency 1200 Pennsylvania Avenue, NW (2310A) Washington, DC 20460

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

Individuals seeking to correct inaccurate or erroneous information about themselves may submit a written request to the EPA Privacy Act Officer pursuant to 40 CFR part 16. 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.

EPA is exempting records maintained within the system from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(1), (2), (4), (5), (6), (7). In addition, exempt records received from other systems of records in the course of EPA ITP record checks may, in turn, become part of the case records in this system. When records are exempt from disclosure in systems of records for record sources accessed by this system, EPA also claims the same exemptions for any copies of such records received by and stored in this system.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 310. For additional information contact the system manager.