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: Waste Import Export Tracking System (WIETS)	**System Owner:** Carolyn Hoskinson, ORCR Director
Preparer: Thomas Reaves	**Office: OLEM/ORCR**
Date: April 27, 2021	**Phone: 703-308-7281**
Reason for Submittal: New PIA____ Revised PIA____ Annual Review__X__ 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:

The Waste Import and Export Tracking System, also known as WIETS, is an EPA major information system (MIS). WIETS was developed in 2009 and 2010 and has been operational since May 2010.

WIETS is a web-based application that provides simultaneous multiple user access for data entry/edit and/or read-only capabilities for interactive real-time data retrieval. WIETS is used for tracking the prior informed consent process for imports to and exports from the US.

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?

42 U.S. Code § 6938 [1] provides the basis for the regulations found in Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal, [2] and through ratification by the US Senate of the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, with Annexes, done at Basel on March 22, 1989.[3]

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?

A System Security Plan has been completed. An ATO has been issued. ATO expires 7/22/2023.

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 system collects data associated with processing transboundary shipments of hazardous wastes. Privacy data stored in the system consists of the name of the waste Generator, name of the waste Transporter(s), and name of the waste Treatment, Storage, and Disposal Facility (TSDF or Designated Facility) receiving party.

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

The data sources are the individuals and/or information systems who work for companies involved in the transboundary movement of hazardous waste for recovery or disposal. The information is manually entered and/or uploaded into WIETS.

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

Yes. The system exists to allow commercial entities to import and/or export hazardous waste. The information is used to meet the statutory requirements associated with this process (Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal).

2.4 Discuss how accuracy of the data is ensured.

System users are responsible for providing the information in WIETS system. The information contained in the system is deemed sufficiently accurate, relevant, timely and complete until legal disposal. WIETS processing involves logging of any/every action performed which ensures any alterations are properly and sufficiently accounted for.

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:

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could potentially be used to tie an individual to a specific employer, state, and/or nation.

Mitigation:

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. EPA has minimized the risk of unauthorized access to the system by establishing a secure environment for exchanging electronic information. The system is housed within a EPA data center, which is a secured facility. Additionally, multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records within the system. All users of the system are given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged.

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 system applies the applicable controls of the Low baseline of NIST 800-53 rev.4 Access Control (AC) family and all associated and applicable Agency prescribed Privacy controls. Controls to prevent access to role-restricted information is via system implemented Role Based Access Controls. Individual users request a role within the system. Permissions associated with the role are applied when the Role Request is approved/denied by a system manager. The applicable permission levels are Create, Read, Update, Delete (CRUD) and are applied based on user roles.

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

NIST 800-53 rev.4 as prescribed in the EPA Information Security and Privacy Control Guide Rev 4-FY21.

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

No.

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?

Internally, members of the WIETS team/administrators (government and contract employees) will have access to the data/information in the system. During Notice processing, EPA employees, external users from the impacted states and/or nations, and external registered handling parties will have access to the data/information related to transboundary waste movements to which they are a party.

FAR Clauses 52.224-1 and 52.224-2 are both included by reference in the base contracts (and are therefore applicable to any resultant task orders).

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.

Transboundary shipping documents serve as historical records for hazardous waste handling. The applicable record schedule is 0257. Records in the system under this schedule are Permanent (NARA Disposal Authority: N1-412-04-8c, NARA Disposal Authority: N1-412-04-8d).

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:

The privacy risk is the potential of keeping records longer than their actual retention timeframe. Transboundary shipping information is documented on manifests, which may be publicly available through generic search engines (i.e. Google, Bing, etc.), during the pre-release period (90 days). This means that the information could potentially be used to tie an individual to a specific employer and/or state. By Congressional mandate, the manifest documented data in the system is released to the public after a 90-day corrections and verification period. Privacy risks related to retention are relieved once the data is released to the public domain.

Mitigation:

System data is transferred to NARA on an annual basis. However, data is publicly releasable after 90 days. Also, all applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. The system has minimized the risk associated with access and data retention by establishing a secure environment for storing current system information within the FedRAMP Moderate AWS US East facilities.

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. the impacted transboundary shipping parties will have access to the data/information related to imports/exports to which they are a party. On the system, information is accessed via logging into WIETS using system credentials to manage/monitor transboundary waste shipments. There is no need for an agreement to access public data.

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

WIETS exists to allow external entities to participate in transboundary waste shipping.

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?

Existing agreements are reviewed as a part of the annual system security review. Inquiries

for new uses/access by internal (EPA) organizations will follow the Agency established procedures for system interconnections and/or information sharing.

4.4 Does the agreement place limitations on re-dissemination?

No. For transboundary data, the external waste handling entities initiate data entry and retain visibility to their information. Only those external parties to transboundary transactions may view data associated with their own transactions. In other words, an external entity can view their own information, but not another (non-party) handler's 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:

The Privacy risk associated with information sharing before/after public release is minimal and commensurate with other public government data. The privacy information in the system consists of first and last name. The risk is that during the pre-release period (90 days), it could be used to tie an individual to a specific employer and/or state. This risk is relieved once the Congressionally mandated information is released into the public domain.

Mitigation:

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. The system has minimized the risk associated with information sharing by establishing a secure environment for exchanging electronic information with other systems. The WIETS system is housed within a controlled entry area, within a secured facility (the RTP NCC). Additionally, multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users (to include other systems) of the system are given a unique user identification (ID) with system identifiers (via CDX), and all interactions with the WIETS system are logged.

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 single privacy element stored in the WIETS is the users name. The system exists to singularly provide a mechanism for processing transboundary shipments of hazardous waste. NIST 800-53 rev 4 AC, Access Control (AC), Identification and Authentication (IA) family controls, and all associated and applicable Privacy controls address use in accordance with Section 6.1. Additionally, data validation limits the types of information that may be entered

into the system, while roles and permissions limit the quantity and context of the information that may be retrieved from the system.

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

All EPA employees are required to take the Annual Security and Privacy Awareness Training which includes privacy elements. Given that data initiation/input relies on external commercial waste handler organizations, external elements must manage their privacy implementations.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

If system auditing and accountability measures are not implemented, data could potentially be at risk of alteration and/or repudiation.

Mitigation:

WIETS data processing involves logging of any/every action performed on the system. All users of the system are given a unique user identification (ID) with personal identifiers (via CDX), and all interactions between the system and the authorized individual users are logged. Activity logs ensure any alterations are properly and sufficiently accounted for. Audit logs are protected against unauthorized 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.

Users log into the system to process hazardous waste transboundary shipments. The shipments can be either in the form of imported wastes (from entities located outside of the US), or in the form of exported wastes (to entities located outside of the US).

The system uses the information to comply with Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X_. 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.)

Information is retrieved by the user by entering a EPA ID Number, facility name, state, or country.

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

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could be used to tie an individual to a specific employer and/or state. The waste handler name is required under the governing documentation listed in Section 1.1. Only registered users can access the non-publicly released data, an individual must be a party to a transaction to view information associated with that transaction, and all NIST applicable 800-53 rev4 and applicable EPA Privacy controls have been implemented and are assessed in accordance with OISP policies/procedures.

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:

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could be used to tie an individual to a specific employer and/or state.

Mitigation:

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. EPA has minimized the risk of unauthorized access to the system by establishing a secure environment for exchanging electronic information. The system is housed within a controlled entry area, within a secured facility. Additionally, multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users of the system are given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged.

***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?

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:

Mitigation:

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 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:

Mitigation: