United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Marlyn Aguilar, at aguilar.marlyn@epa.gov or (202) 566-0012.

System Name: e-Manifest	
Preparer: Thomas Reaves	**Office: OLEM/ORCR**
Date: October 3, 2017	**Phone: 703-308-7281**
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: 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 Hazardous Waste Electronic Manifest Establishment Act, signed into law by President Obama on October 5, 2012, authorizes EPA to implement a national electronic manifest system. Commonly referred to as "e-Manifest," this national system will provide a means for waste handlers to process electronic manifests.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the system in question?

Per the e-Manifest Final Rule[1], the information is being collected to facilitate implementation of certain provisions of the Hazardous Waste Electronic Manifest Establishment Act, Public Law 112–195[2] (the e-Manifest Act), which directs EPA to establish a national electronic manifest system.

1. Federal Register/Vol. 79, No. 26/Friday, February 7, 2014/Rules and Regulations, (p. 7544).
2. https://www.congress.gov/112/plaws/publ195/PLAW-112publ195.pdf.

1.2 Has a system security plan been completed for the information system(s) supporting the system?

No. The system is under development and the system security plan is incomplete.

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.

OMB No. 2050-0039, EPA Form 8700-22, EPA Form 8700-22A

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 electronic Uniform Hazardous Waste Manifests (EPA Form 8700-22)[3], and (if necessary) the associated Continuation Sheet (EPA Form 8700-22A)[4]. 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. All other manifest data that is stored is directly related to waste handler entities and waste stream processing.

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

The data sources for manifests are the individuals and/or information systems who work for companies involved in the generation, transport and treatment, storage, and/or disposal of waste streams.

There are two methods for electronically collecting manifest data:

a) Users will be able to log into the e-Manifest system to process hazardous waste manifests. Generators, Brokers (acting on-behalf of Generators), Transporters, and TSDF personnel will be able to enter manifest data directly into the system via a web browser.
b) TSDFs will have the ability to process manifest data via secure Application Programming Interfaces (APIs) (system to system connections) with the e-Manifest back-end. As with the first method, TSDF access will be limited to only those manifests to which they are a party.

3. https://www.epa.gov/sites/production/files/2015-06/documents/newform.pdf
4. https://www.epa.gov/sites/production/files/2015-06/documents/con-sheet.pdf

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 process hazardous waste manifests. States monitoring hazardous waste shipments can/do publish manifest data on various state sites today. Per the e-Manifest Final Rule, "after the 90-day period of restricted access has passed, the Agency intends to provide full direct, on-line access by the public to all manifest data in the system". [5]

2.4 Discuss how accuracy of the data is ensured.

Prior to making manifests publically available, the 90-day period for corrections and verifications serves as an opportunity for users to ensure accuracy. Manifests serve as historical records for hazardous waste handling. As such, the information contained in the manifest is deemed sufficiently accurate, relevant, timely and complete until legal disposal. Electronic manifest processing involves logging of any/every action performed against a manifest 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 publically available through generic search engines (i.e. Google, Bing, etc.), it could potentially 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 will be 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 will be 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.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the system uses the information.

There are two methods for collecting manifest data:

5. Federal Register/Vol. 79, No. 26/Friday, February 7, 2014/Rules and Regulations, (p. 7544)

a) Users will be able to log into the e-Manifest system to process hazardous waste manifests. Generators, Brokers (acting on-behalf of Generators), Transporters, and TSDF personnel will be able to enter manifest data directly into the system.

b) TSDFs will have the ability to process manifest data via secure Application Programming Interfaces (APIs) (system to system connections) with the e-Manifest back-end. As with the first method, TSDF access will be limited to only those manifests to which they are a party.

The system uses the information to comply with the Hazardous Waste Electronic Manifest Establishment Act, Public Law 112–1955 (the e-Manifest Act)[6], which directs EPA to establish a national electronic manifest system.

3.2 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 EPA ID Number, Facility name, or by state.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

Information is not retrieved by personal identifier.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Per the 2017 Privacy Threshold Analysis results, no SORN applies to this system.

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No.

3.6 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 publically 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 will be 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 will be 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.

Section 4.0 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.

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

Users are provided with educational resources prior to login by reading and acknowledging the System Warning notice on the home screen. Users may also obtain additional privacy information by reviewing the Privacy and Security Notice which is available via the link on the home screen. [6]

4.2 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?

Per the e-Manifest Final Rule, waste handlers will still be able to use the paper Uniform Hazardous Waste Manifest (8700-22), and Continuation sheet (8700-22A). An individual and/or entity using paper manifests will not be required to enter information into e-Manifest, but instead will fill out the paper versions of the Uniform Hazardous Waste Manifest. Per Federal regulations, applicable hazardous waste cannot be shipped without a proper manifest.

4.3 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

6. https://www.congress.gov/112/plaws/publ195/PLAW-112publ195.pdf

information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

The e-Manifest Act requires that all hazardous waste manifests be submitted to the system. Users are notified of the ability to continue to use paper manifests. No risk has been identified related to notice.

Mitigation:

Users will be encouraged to review the system help to address privacy related questions.

Section 5.0 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.

5.1 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 uses roles and associated permission levels to ensure that prior to public release, manifest data is protected. All applicable NIST 800-53 rev.4 Security and Privacy controls will be implemented to ensure protection commensurate with the system categorization. Also, each user account permission is granted based on a need to know basis.

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

No.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

Internally, members of the e-Manifest team/administrators (government and contract employees) will have access to the data/information in the system. During manifest processing, EPA regional employees, external users from the impacted states, and external registered handling parties will have access to the data/information related to manifests to which they are a party. After the initial 90-day period for corrections, per the Final Rule, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system".

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). FAR 24.104 is the prescription that indicates when to include the clauses, and is therefore not included in contracts or solicitations.

5.4 What procedures are in place to determine which users may access the information and how does the system determine who has access?

The system uses roles and associated permission levels to ensure that prior to public release, manifest data is protected. Each account submission is reviewed and verified by a Site Manager to validate that the users request corresponds to the level of permission required to perform the requested action. Access is either approved/granted or denied. Per the e-Manifest Final Rule, after the 90-day period for corrections and verification, the information is made available to the public. A flag marking the 90 days determines when the data is released.

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

Manifests serve as historical records for hazardous waste handling. As such, the information contained in the manifest is deemed sufficiently accurate, relevant, timely and complete until legal disposal. The applicable record schedule is 0257.

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes.

5.7 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 with the stated purpose and mission of the system.

Privacy Risk:

The data in the system is released to the public after the 90-day corrections and verification period. Privacy risks related to retention are relieved once the data is released to the public.

Mitigation:

System data is transferred to NARA on an annual basis. However, data is publically releasable after 90 days.

Section 6.0 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.

6.1 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. Initially the impacted states and registered handling parties will have access to the data/information related to manifests to which they are a party. As indicated in the Final Rule, after a 90-day period to allow for correction and verification of waste shipment information, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system". After the initial 90-day period for corrections, per the Final Rule, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system". There is no need for an agreement to access public data.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A – No SORN applicability.

6.3 Does the agreement place limitations on re-dissemination?

No. As indicated in the Final Rule, after a 90-day period to allow for correction and verification of waste shipment information, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system".

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

As indicated in the Final Rule, after a 90-day period to allow for correction and verification of waste shipment information, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system". This will be logged as information is published for public accessibility.

6.5 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?

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

6.6 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 information contained within the system is to become publically available after 90 days. The Privacy risk associated with information sharing before/after public release is minimal and commensurate with other public government data.

Mitigation:

All applicable NIST 800-53 rev.4 Security and Privacy controls will be 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 e-Manifest system will be 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 (to include other systems) of the system are given a unique user identification (ID) with system identifiers, and all interactions between the e-Manifest system and all connecting systems are logged.

Section 7.0 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.

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

Individuals can log into the system to view manifests associated with their user account. Individuals will also be able to view/access all manifests which have been made available to the public.

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

During the initial 90-day period after submissions, manifests are withheld from public purview to allow for corrections and verification. This period allows for users to correct inaccurate or erroneous information.

7.3 How does the system notify individuals about the procedures for correcting their information?

Aside from the published e-Manifest Final Rule, the system Help contains information on the simplistic procedures for correcting information.

7.4 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:

As a system which provides a 90-day period for corrections and verification prior to public release, e-Manifest provides no additional redress program.

Mitigation:

Users are afforded a 90-day period for corrections and verification prior to public release of the information.

Section 8.0 Auditing and Accountability

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

8.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

The single privacy element stored in the e-Manifest system is the users name. Data validation limits the types of information that may be entered into the system. Roles and permissions limit the quantity and context of the information that may be retrieved from the system prior to public release.

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

All EPA employees are required to take Annual Records Management Training which includes privacy elements. Given the public releasable nature of the data within the system, external elements must manage their privacy implementations.

8.3 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:

Electronic manifest processing involves logging of any/every action performed against a manifest. 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. Activity logs ensure any alterations are properly and sufficiently accounted for. Audit logs are protected against unauthorized access.