United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

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

If you need further assistance contact Brooks Patricia @ Brooks.patricia@epa.gov or (202) 566-0012.

System Name: Engines and Vehicles – Compliance Information System (EV-CIS)	
Preparer: Holly Pugliese	**Office: OAR-OTAQ-CD**
Date: April 10, 2019	**Phone: 734-214-4288**
Reason for Submittal: New PIA____ Revised PIA__X__ 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:

EV-CIS is a comprehensive data management system that allows vehicle and engine manufacturers to securely submit the required emissions data and other compliance information to EPA. EV-CIS also contains a subsystem, the Engine and Vehicle Exemption System (EV-ES), which collects basic contact information (name, address, e-mail, Vehicle Identification Number (VIN) and phone number) from individuals seeking to temporarily import nonconforming vehicles or engines in to the U.S. It is the information that is collected in the EV-ES subsystem that is covered by the PIA.

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?

Title II of the Clean Air Act, (42 U.S.C. 7521 et seq.)

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, the system has an ATO. The current ATO expires on July 29, 2019 and the renewal process is already underway.

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 2060-0717, EPA Control Number 2583.01

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, the data is not stored in a Cloud.

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 PII collected consists of basic contact information (name, address, e-mail and phone number, and Vehicle Identification Number (VIN)).

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

The PII information is collected from individuals who are seeking an exemption from the Clean Air Act requirements for importing vehicles or engines. Individuals seeking an exemption submit a written request in a letter to EPA requesting the exemption. EPA staff and contractors with the appropriate roles enter the information into EV-ES. The system generates approval or denial letters that are sent back to the requestor via the email or mailing address provided in their request letter.

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 information originates from the requesters themselves, so it is to their benefit to provide accurate information and keep it updated by notifying EPA of any changes. To the extent that EPA is made aware of any inaccuracies, the data is updated accordingly.

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:

1. Interception of U.S. mail
2. Interception of envelopes before delivered to EPA Contractor staff.
3. Accidental disclosure of the information once the envelopes are opened.
4. Storage of hard copies after envelopes are opened.
5. Shoulder surfing while entering or viewing information on screen.
6. The system stores the requestors name, address, phone number, Vehicle Information Number (VIN), or email address which is considered Personally Identifiable Information (PII).

Mitigation:

Nothing can be done about interception of U.S. mail while in transit. But after the mail reaches the facility, it is only handled by designated EPA staff. Mail is sorted and delivered to division mail boxes, for distribution to applicable groups/people. To avoid disclosure of PII information, envelopes addressed to the Imports staff are delivered to a designated internal mail box and are kept sealed until they are ready to be processed by Contractor staff.

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?

The system employs role-based authorization so users are only granted access to the information that is relevant to the roles that have been assigned to their account.

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

The system employs role-based authorization, so users are only granted access to the information that is relevant to the roles that have been assigned to their account. When a user requests access to the system, the system owner approves all role requests specific to what the user needs to do. Minimal access approach is always used. Users who do not have the role for the part of system that contains PII cannot view or take any action on this data.

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

Yes

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 Staff and contractors who process exemption requests will have access to the information in order to perform their duties of evaluating the requests. Also, EPA Staff and contractors who support the EV-ES System may have access to the data. There are 4 contracts in place where contractors have access to the EV-ES information. Two of the contracts have the FAR clauses included. The third contract that oversees the imports exemptions application process for EV-ES is in the process of being awarded. The new contract does contain the Federal Acquisition Regulations (FAR) clauses. The fourth contract is used to do development work on the system. The Statement of Work (SOW) for this contract includes the FAR clauses**.**

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 are retained for 7 years per EPA Records Schedule 485. The information is retained in case the need arises to contact requestors.

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:

Because the information is now stored electronically, it is effectively kept for longer than 7 years.

Mitigation:

Only users authorized to have access to information can see it.

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.

General routine uses A, F, H, and K apply to this system.

Exemptions numbers generated for requestors that have submitted their PII is shared with a system at the Customs and Border Patrol (CBP). An employee of the CBP can then log into their system and see whether or not the Exemption number presented to them by an individual has indeed been approved.

No PII information is shared with CBP.

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

The external sharing noted in section 4.1 is compatible with the original purposes of collection of PII information, because exemption numbers cannot be issued unless the requestor provides their information. CBP only requires validation of the exemption number from the EV-CIS, and not the PII associated with it.

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?

Exemption number information is only shared with CBP. New uses of the information or new access is not granted to other organizations.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable.

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:

None. Information is not shared externally. Only exemption numbers from the system are shared.

Mitigation:

None.

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 in accordance with stated practices in this PIA?

The system uses the name, address, and VIN provided by the requestor of the exemption only to generate an approval or denial letter that is then emailed to the email address provided by the requestor. This information is not used for any other purpose other than to generate the letter needed by requestor.

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

As stated above, anyone with access to the system must read and sign the EV-CIS Rules of Behavior document and must successfully complete EPA's annual security awareness training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

1. PII information could be used for purposes not intended.

Mitigation:

EPA has enlisted only designated EPA Contractors to perform the work needed by the system. All contractors are properly trained and asked to review and sign EV-CIS Rules of Behavior, which state that the information is not to be used for purposes not intended. Any user who is determined to have misused the information contained in the system will have their access revoked and their user accounts terminated.

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.

The PII information is being collected in order to correspond with an exemption requester and to identify the individual to which the exemption was issued. If the applicable criteria for receiving an exemption is met, EPA issues an approval letter which is sent to the requester at the email or mailing address they provide to us. This letter is then presented to Customs and Border Patrol (CBP) by the requester when the product arrives at the port to facilitate entry into the United States. If the applicable criteria for an exemption have not been met, a denial letter will be sent to the requestor outlining the reasons for denial.

The PII information may be used in the following ways: (a) to correspond with the individual who requested the exemption and (b) in the case an exemption is issued, to identify the individual to which the exemption was issued.

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.*)

The system retrieves information by the requestors name, Vehicle Identification Number (VIN), and email address

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

EPA-65

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:

1. PII information being seen by those not authorized.
2. Letter intercepted by internal EPA staff.
3. Letter intercepted in transit via U.S. Mail

Mitigation:

Only users with the appropriate roles are granted access to the information according to the roles that have been assigned to their account. Users are also required to take EPA's annual security awareness training and sign a Rules of Behavior document. In addition, approval letters are only printed when the Contractor is actively working on the exemption at hand; any printouts are immediately picked up from the printer. On screen access to the PII information is protected by having only those authorized to see the information being able to access the information in the system (special roles are needed to access information). As far as letters being intercepted by internal EPA staff, all internal staff that work onsite are considered trusted and knows not to disclose information unless they have explicitly permission to do so. There is nothing that can be done about possible interception of letter in U.S. mail.

*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.

Individuals do not submit information directly into the system. Rather, individuals who need the exemption provide the necessary information to EPA in the form of a letter to request the exemption and EPA staff and contractors with the appropriate roles enter the information in to the system.

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 cannot process their requests for exemptions without providing this information. If they choose not to provide it, we cannot process the exemption request and they will not be able to import their vehicle.

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:

1. As stated above, individuals need to supply their name, mailing address, phone number, Vehicle Identification Number (VIN) and email in order for EPA to process their request.
2. People beside the person requesting the exemption have access to their information (they don't enter their information in the system themselves).
3. People can't update the information themselves.

Mitigation:

Due to the simplicity of the information being collected, EPA decided to create an internal EPA system to store this information, which in itself reducing exposure to outside world. It was then decided that internal EPA contractors would enter the information into the system, on behalf of each person requesting the exemption, so only trusted partners have been assigned this task. These contractors are only authorized to work onsite, and do not perform this work offsite, or remotely (i.e. home). To get around user's not being able to update information themselves, we have enlisted contractors to maintain all information in the system, so when they receive updates from customer's, they update the information accordingly.

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?

Request for access must be made in accordance with the procedures described in EPA's Privacy Act regulations at 40 CFR part 16. Requesters will be required to provide adequate identification, such as a driver's license, employee identification card, or other identifying document. Additional identification procedures may be required in some instances.

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

Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA Agency Privacy Officer, MC2831T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

8.4 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:

None.

Mitigation:

None