United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 12/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Fleet Access (FA)	
Preparer: Jackie Brown	**Office:** Office of Mission Support (OMS)
Date: February 4, 2020	**Phone:** (202) 564-0313
Reason for Submittal: New PIA__X__ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).	
The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).	

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

Fleet Access (FA) is a contractor owned and operated system used by EPA to store and maintain vehicle asset data. It has been selected to comply with the General Services Administration (GSA) FMR B-15 requirement that each federal agency store and maintain vehicle asset data collected in a Fleet Management Information System (FMIS). As a contractor owned system, the FA technical and operational security measures will be implemented and managed by the contractor. The FA system serves two primary purposes:

1. Stores vehicle level data such as license plate, VIN, make, model, acquisition value/lease rates, designations regarding alternative fuel, energy and sustainability mandates. Which is used to produce the Federal Automotive Statistical Tool Report (FAST Report) as an end of year report. This end of year report is submitted jointly to the Department of Energy (DOE), the GSA, and the Idaho National

Lab (INL). The FAST report summarizes each vehicle's annual data with respect to fuel, mileage, maintenance, acquisition, and disposal.

2. Used by EPA's Fleet program management, regional, local staff and support contractors as a standardized vehicle reservation system to reserve and utilize fleet vehicles for official agency business.

   New users "sign-up" using first and last name, work phone number, work email address, and driver's license expiration date. The user's profile is reviewed by the applicable fleet manager to ensure the user has a valid driver's license. The driver's license is for verification purposes but, with the exception of the driver's license expiration date, is NOT collected, stored or maintained on the FA system. Once the user is verified by the fleet manager and profile marked as "Enabled", the user can then make a vehicle reservation. Alternatively, a user can visit a local fleet manager in person and provide information verbally or written. The designated local fleet manager physically verifies driving credentials and enables the individual's profile.

   FA does not have any external partners. The system is vendor-hosted, and data can be accessed, downloaded and backed up at any time using a vendor-provided dashboard. Data is encrypted and protected both in transit and at rest using both the SSL certificate and Database Encryption Key (DEK) in the vendor's secure hosting environment with real-time monitoring. FA administrators use the first and last name and email address to register vehicle users. Currently, (but will change approximately 2/28/2020) a User last name can be searched in FA via the reservation module in order to make a reservation for another user.

   FA is about to be awarded a sole sourced contract with the same vendor (Agile), expected to close on February 28, 2020.

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?

- 40 USC 175 – Federal Motor Vehicle Expenditure Control
- Sections 15301 and 15302 of the Consolidated Omnibus Budget Reconciliation Act of 1986 (Pub. L. No. 99-272) (40 U.S.C. Sec. 17502 and 17503); and
- General Services Administration (GSA) FMR B-15.

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?

An ATO has not been granted. To facilitate ATO, a draft SSP, in addition to the supporting documentation, is in progress. However, this is a contractor-owned system and all information required for ATO package development must be provided by the vendor and is currently under evaluation/review.

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. FA isn't a cloud-based system.

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).

- Last Name,
- First Name,
- Work Phone Number
- Work Email Address
- Driver's License Expiration Date
- Profile Picture (not required for EPA purposes. Comes standard as part of the COTS product)

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

Information (first name, last name, work phone number, work email address, driver's license expiration date, and profile picture (optional)) is collected directly from the individual using an online portal (link provided below).
https://epa.agilefleet.com/_UserRegistration.asp

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. FA doesn't use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

FA Administrators or Local Fleet Managers ensure the accuracy of data by verifying a

physical copy of the driver's license. Users verify, certify and acknowledge that the information they provided in the system is accurate.

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 information provided by the user might be more than required for account maintenance (i.e. cell / home phone).

Mitigation:

Account information maintained, is limited by the fields available and the account registration form directs the user to provide business information. In addition, EPA users are required to attend annual Information Security and Privacy Awareness (ISPAT) training. All contractor employees with access to data are required annually to provide a signed "End User Computing Agreement" which describes company policies relative to Personal, Private, and Sensitive Information (PPSI).

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?

Role-Based and least privilege account access controls have been implemented for the FA system.

Available accounts have been provided below:

- Enterprise Administrator
- Enterprise Admin
- Enterprise Dispatchers.
- Enterprise Maintenance
- Enterprise Driver
- Enterprise Requestor
- Site Administrator
- Site Admin
- Site Dispatchers
- Site Maintenance
- Site Driver
- Site Requestor

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

The authorized accesses have been documented in the vendor provided administrator manual (uploaded to Xacta – Filename: Fleet Commander System Admin Manual_20190510.docx. Date: 1/6/2020.).

- Local Fleet Managers determine who requires access to the system and the roles assigned.
- FA has established conditions for each user role.
- Each access request must be authorized by the fleet manager, has a defined role, and the account is audited upon activation.
- Account verification is provided by the fleet manager prior to account activation.
- Account creation, access, modification, etc. is made in accordance with EPA standards.
- The use of accounts used to access the FA system is monitored.
- Review of user accounts are audited. Inactive accounts are disabled.

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

No, EPA personnel and the contractor are the only users.

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?

The following FAR clauses will be included in future contracting guidance:

- 52.224-1
- 52.224-2
- 52.224-3

If it is determined that these clauses need to be included in the original contract, a contract modification will be submitted and unilaterally included and accepted.

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.

- EPA Records Schedule 0090-Administrative Support Databases
  Personnel information is retained for as long as the user or administrator determines necessary. Generally, as long as the individual is employed by the EPA and requires vehicle reservation access. Vehicle data (no PII) is stored for a minimum of 3 years. All user profile data retained is required to facilitate vehicle reservations only. If a user no longer needs to reserve a vehicle for agency business their user information can be deleted permanently, no user information is ever shared or reported outside of EPA.

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:

Any unauthorized deletion of records outside of the EPA Retention Schedule poses a serious risk to EPA and its mission.

Mitigation:

Removal events are audited on a weekly basis by reports generated from the Fleet Commander system. All deletions from the system are audited. The addition of records to the system is audited through weekly transaction reports and daily records transmission reports. The reports are maintained by the EPA FA Program Management Office.

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.

No information is shared outside EPA.

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

Not applicable. This is a contractor-owned system, which is used by EPA personnel. There is no information shared with any other organization.

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?

Not applicable. This is a contractor-owned system, which is used by EPA personnel. There is no information shared with any other organization.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable. This is a contractor-owned system, which is used by EPA personnel. There is no information shared with any other organization.

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. There is no information sharing.

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 (Section 6.1)?

All transactions are tracked within the fleet dashboard through auditable events. There are numerous controls in place to ensure data integrity and to prevent unauthorized access. Access is controlled by User Roles, each role assigned gives access only to a user on a need-to-know basis to perform their job.

FA offers several measures to secure access to data, such as access control rules and password authentication. Non-authorized users are prevented from gaining access to FA and mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information.

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

All EPA users are required to take annual Information Security and Privacy Awareness (ISPAT) training. All contractor employees with access to data are required annually to provide a signed "End User Computing Agreement" which describes company policies relative to Personal, Private, and Sensitive Information (PPSI).

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Improper or infrequent audit log reviews may not detect the exfiltration or misuse of PII

Mitigation:

System audit logs are maintained and reviewed. Data is encrypted while in transit and at rest.

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 information collected is for account creation purposes and to reserve vehicles. Information is collected using the fleet registration portal (web-based registration). Link to the web portal is provided below.

https://epa.agilefleet.com/_UserRegistration.asp

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.)

FA is currently designed to retrieve data using User ID and Last Name.

The UserID is set at the user's discretion and may or may not contain first / last name. This cannot currently be locked down by technical means, however procedures may be put into place to help reduce the likelihood of this occurring.

In a future version (v.5.05 – release 2/2020), Agile will reduce the lookup capability for the standard user. Once this has been implemented, the last name lookup field will be hidden for the standard user but will still available to administrative personnel.

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

The requirement for SORN documentation has just been identified. A SORN request is pending submission to the LPO.

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:

There is a risk of unauthorized disclosure or modification to information collected.

Mitigation:

FA administrators ensure that information is protected by employing appropriate controls (i.e. account access and audit accountability) to prevent unauthorized access or disclosure. All EPA users are required to attend annual Information Security and Privacy Awareness (ISPAT) training. All contractor employees with access to data are required annually to provide a signed "End User Computing Agreement" which describes company policies relative to Personal, Private, and Sensitive Information (PPSI).

*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.

FA allows only authorized EPA personnel to request a user account. Prior to submitting the information required for automated account generation, the user should acknowledge the following system-specific privacy warning notice:

Government Warning
You are about to access a U.S. Government computer information system. Access to this system is restricted to authorized users only. Fleet Access user accounts are provided solely for the use of the individual for whom they were created. Anyone who accesses this system without authorization, or exceeds authorized access could be subject to a fine, imprisonment, or both, under public law 98-473.

EPA federal employees and contractors do not have a right, nor should they have an expectation, of privacy while using any government office equipment at any time, including remote dial-in, business and personal Internet usage. By accessing this system, you consent to having your activities and/or access recorded by system software and periodically monitored. If this record reveals any unauthorized use, this record may be provided to supervisory personnel and law enforcement officials as evidence.

Privacy Notice
Federal executive agencies are required by Sections 15301 and 15302 of the Consolidated Omnibus Budget Reconciliation Act of 1986 (Pub. L. No. 99-272) (40 U.S.C. Sec. 17502 and 17503) to have a centralized system to identify, collect, and analyze motor vehicle data with respect to all costs incurred for the operation, maintenance, acquisition, and

disposition of motor vehicles. Furnishing the information on this form is voluntary, but failure to do so may result in disapproval of your request to access the Fleet Access system. EPA will use the personal identifying information you provide for the expressed purpose of registration to Fleet Access. The Agency will not make this information available for other purposes unless required by law. EPA does not sell or otherwise transfer personal information to any outside party.

Individuals who wants to know whether this system of record contains a record about them, who wants access to their record, or who wants to contest the contents of a record, should make a written request to the EPA Privacy Office, Attn: Privacy Officer, MC 2831 T, 1200 Pennsylvania Avenue NW., Washington, DC 20460. Requests for correction or amendment must identify the record to be changed and the corrective action sought. Requests must be submitted to the Agency contact indicated on the initial document for which the related contested record was submitted. Complete EPA Privacy Act procedures are set out in 40 C.F.R. part 16.

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?

Individuals consent to provide their information during the self-registration process. They can decline or opt out of sharing their personal information by not creating the FA account. FA accounts are not mandatory, however due to the limited information collected, similar to that available in the EPA locator, users don't opt out of providing 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:

FA users may not know that the request for personal information is not mandatory and may feel obligated to provide their information. Or, FA users may not realize that they are providing PII.

Mitigation:

There is a consent confirmation field prior to submitting the self-registration form. It states: "The use of Fleet Access for vehicle reservations is not required. If you do not want to have your last name and username searchable, you can choose not to use the system and can make reservations manually via phone, email, or in person at your local fleet location. If consent to collect the above information is authorized, please type your full name in the box below. Consent to collect also acknowledges acceptance of the FA privacy notice provided at the top of the page."

Potential users can simply cancel the self-registration process and close the page if they choose not to accept the Privacy & Security Policy.

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?

All users can access and view their own respective user data at any time by accessing a web-based profile page within the FA system.

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

All users can access and view their own respective information at any time. Utilizing a web-based profile page within the FA system, users can modify work phone and email at any time. In the event a change must be made to name, the user may request assistance from the local fleet manager.

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

The FA profile page provides information for users that need assistance. They can also contact the local EPA Fleet Manager to request assistance with updating the information.

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, FA allows users to correct their own information within the system using their profile page. In addition, they are also able to contact the local account managers for assistance.

Mitigation:

None