



# Fleet Management System (FMS)

## *Privacy Impact Assessment (PIA)*

September 16, 2020

POINT of CONTACT

Richard Speidel

[gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov)

Chief Privacy Officer  
GSA IT  
1800 F Street NW  
Washington, DC 20405

**Instructions for GSA employees and contractors:**

This template is designed to help GSA employees and contractors comply with the E-Government Act of 2002, Section 208. GSA conducts privacy impact assessments (PIAs) for electronic information systems and collections in accordance with CIO 1878.3 Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices. The template is designed to align with GSA business processes and can cover all of the systems, applications, or projects logically necessary to conduct that business.

The document is designed to guide GSA Program Managers, System Owners, System Managers, and Developers as they assess potential privacy risks during the early stages of development and throughout the system, application, or project's life cycle.

The completed PIA shows how GSA builds privacy protections into technology from the start. Completed PIAs are available to the public at [gsa.gov/pia](https://gsa.gov/pia).

Each section of the template begins with a statement of GSA's commitment to the Fair Information Practice Principles (FIPPs), a set of eight precepts that are codified in the Privacy Act of 1974.

**Please complete all sections in italicized brackets and then delete the bracketed guidance, leaving only your response.** Please note the instructions, signatory page, and document revision history table will be removed prior to posting the final PIA to GSA's website. **Please send any completed PIAs or questions to [gsa.privacyact@gsa.gov](mailto:gsa.privacyact@gsa.gov).**

## Stakeholders


Name of Information System Security Manager (ISSM):  
Gerald Weeks


Name of Program Manager/System Owner:  
Mohamed Chaouchi

## Signature Page

Signed:

DocuSigned by:  
  
D47CB0624995477  
Information System Security Manager (ISSM)

DocuSigned by:  
  
8A735B43C9E7460...  
Program Manager/System Owner

DocuSigned by:  
  
171D5411183F40A...  
Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

## Document Revision History

Date	Description	Version of Template
01/01/2018	Initial Draft of PIA Update	1.0
04/23/2018	Added questions about third-party services and robotics process automation (RPA)	2.0
6/26/2018	New question added to Section 1 regarding Information Collection Requests	2.1
8/29/2018	Updated prompts for questions 1.3, 2.1 and 3.4.	2.2
11/5/2018	Removed Richard's email address	2.3
11/28/2018	Added stakeholders to streamline signature process and specified that completed PIAs should be sent to gsa.privacyact@gsa.gov	2.4
4/15/2019	Updated text to include collection, maintenance or dissemination of PII in accordance with e-Gov Act (44 U.S.C. § 208)	2.5
9/18/2019	Streamlined question set	3.0
2/20/2020	Removed email field from signature page	3.1

6/15/2020	Reviewed and updated the document	3.2
8/19/2020	Update FMS PIA based on feedback from Privacy Office	3.3

# Table of contents

## **SECTION 1.0 PURPOSE OF COLLECTION**

- 1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
- 1.2 Is the information searchable by a personal identifier, for example a name or Social Security number? If so, what Privacy Act System of Records Notice(s) applies to the information being collected?
- 1.3 Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers and expiration dates.
- 1.4 What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.

## **SECTION 2.0 OPENNESS AND TRANSPARENCY**

- 2.1 Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? If not, please explain.

## **SECTION 3.0 DATA MINIMIZATION**

- 3.1 Why is the collection and use of the PII necessary to the project or system?
- 3.2 Will the system create or aggregate new data about the individual? If so, how will this data be maintained and used?
- 3.3 What controls exist to protect the consolidated data and prevent unauthorized access?
- 3.4 Will the system monitor members of the public, GSA employees, or contractors?
- 3.5 What kinds of report(s) can be produced on individuals?
- 3.6 Will the data included in any report(s) be de-identified? If so, how will GSA aggregate or de-identify the data?

## **SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION**

- 4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection, maintenance, use, or dissemination?
- 4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?
- 4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?
- 4.4 Will the system, application, or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

## **SECTION 5.0 DATA QUALITY AND INTEGRITY**

- 5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

## **SECTION 6.0 SECURITY**

- 6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?
- 6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?
- 6.3 How will the system be secured from a physical, technical, and managerial perspective?
- 6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

## **SECTION 7.0 INDIVIDUAL PARTICIPATION**

- 7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.
- 7.2 What procedures allow individuals to access their information?
- 7.3 Can individuals amend information about themselves in the system? If so, how?

## **SECTION 8.0 AWARENESS AND TRAINING**

- 8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project?

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

- 9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

## Document purpose

This document contains important details about *Fleet Management System (FMS)*, *Travel and Transportation Logistics (TTL)*. To accomplish its mission *GSA IT, Office of Acquisition IT Services (IQ)* must, in the course of *Fleet Management*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information<sup>[1]</sup> that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's [privacy policy](#) and [program goals](#). The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.<sup>[2]</sup>

### A. System, Application, or Project Name:

Fleet Management System (FMS) - FMS can be found in GSA's GEAR and/or ARCHER system under ClearPath.

### B. System, application, or project includes information about:

FMS manages the GSA leased vehicle inventory and tracks the leased vehicle throughout its useful life, from initial vehicle receipt through operational use/assignment (including: management of accidents, maintenance and repair) to ultimate disposal/sale. FM supports over-\$2-billion per year Fleet vehicle leasing program for the Office of Fleet Management/GSA Fleet. FMS supports approximately 800 GSA users in eleven regions and 30,000 Federal customers. This application supports the stateside service GSA provides to agencies who lease vehicles from GSA.

The GSAFleet2Go mobile app provides timely, Fleet-relevant information from sources that would not otherwise be available to Fleet customers: Fleet Service Representatives and Fleet Maintenance Center Contact information, Fueling and Maintenance locations, Manufacturer Warranty Service Contact Information. FMS2Go allows users to load new vehicle inventory and assign vehicles to customers or terminate them from assignment using handheld devices. Remote users upload the data to a local PC which, in turn, sends the data to the FMS database during the nightly batch process. The targeted users of this application are "GSA" and "PUBLIC" (limited to GSA Leased Federal Agency Vehicle customers).



### **C. For the categories listed above, how many records are there for each?**

There are approximately 602 unique federal users (533 (US) and 69 (Europe)) and then there are approximately 6 contractors. There are no records being maintained for members of the public. There were 1000 plus downloads for the Android devices and 748 installations on the IOS devices

### **D. System, application, or project includes these data elements:**

Fleet applications manage the GSA leased vehicle inventory and track the leased vehicle throughout its useful life, from initial vehicle receipt through operational use/assignment (including: management of accidents, maintenance and repair) to ultimate disposal/sale. All information pertaining to vehicles such as VIN, Tag, Odometer reading, Vehicle equipment, Agency vehicle assigned to, repair vendors, sale information, leasing information are recorded in the Fleet application databases.

PII Data - The following PII information is collected when a user registers for any of the Fleet applications:

- First and Last Name
- Email address
- Telephone number
- IP Address

The CARS/MARS system collects PII information to track all the accidents that GSA leased vehicles are involved in in order to permit GSA to contact the individual driving the car at the time of accident and to recover the expenses for an accident/incident in which a 3rd party is at fault.

The CARS/MARS application and GSAFleet2Go mobile app collect additional personally identifiable information (“PII”) about the people who use these products and services. Data elements for accident investigation and recovery include name, gender, race (for Police report only), birth date, geo-location indicator, personal email address, home address, home phone number, health records, Driver’s License Number, and personal credit card information or as required in the SF91 form - <https://www.gsa.gov/forms-library/motor-vehicle-accident-report>.

## **Overview**

The Fleet Management System (FMS) manages the GSA leased vehicle inventory—it tracks the leased vehicle throughout its life cycle, from initial vehicle receipt through operational use/assignment (including management of accidents, maintenance and repair) to ultimate disposal/sale. FMS supports the +\$2 billion-per-year Fleet vehicle leasing program under the Federal Acquisition Service (FAS) Office of Motor Vehicle Management/GSA Fleet. FMS supports approximately 800 GSA users in eleven regions and 30,000 Federal customers. It also supports the stateside service GSA provides to agencies who lease vehicles from GSA. FMS includes the following components/subsystems below:

- Automated Remarketing Module (ARM)
- AutoAuctions
- Comprehensive Accident Reporting System (CARS) / Mechanical Accountability Reporting System (MARS)
- Drive-Thru
- Fleet Management System (FMS)
- FMS2Go (Hand Held Scanner and Mobile App)
- Federal Fleet Management System (FedFMS)
- FleetWeb (Agency Incurred Expenses (AIE), Sale and Admin Modules)
- Federal Motor Vehicle Registration System (FMVRS)
- GSAFleet2Go Mobile App
- Short Term Rental (STR)
- Acquisition Management Program/Customer Acquisition Module (AMP/CAM)
- Dispatch Reservation Module (DRM)
- Vehicle Fleet Exchange (VFE)
- Reports Portal

The FMS identifies individuals by name in conjunction with other data elements such as gender, race (for Police report only), birth date, age, geographic indicator, personal email address, home address, home phone number, health records, Driver's License Number, and personal credit card information. The FMS system collects PII information to track all the accidents that occur to GSA leased vehicles in order to permit GSA to contact the individual driving the car at the time of accident and to recover the expenses for an accident/incident in which a 3rd party is at fault.

The PII data collected in a pdf form (see link below) is securely transferred to the Enterprise Content Management System (ECMS) server. Link for form is located at:

<https://www.gsa.gov/forms-library/motor-vehicle-accident-report>

All files are encrypted during transmission to the ECMS server and at rest. Once the above document is saved in ECMS it is never removed or deleted unless specifically requested by the Business Line.

In the case of accidents/incidents where non-government 3rd parties are involved, the PII information is captured directly in CARS such as Driver's First Name, Middle Initial, Last Name, Home Address (Street Number, City, State, Zip), Home Phone Number, Name of Insurance Company, Address of Insurance Company (Street Number, City, State, Zip), Insurance Company Phone Number, Insurance Policy Number of Driver or Owner for both the driver of the 3rd party vehicle and the owner (if different from the driver). The data is transmitted to Financial Management Enterprise Service Bus (FMESB) [(Office of Chief Financial Officer (OCFO) Pegasys System] through Secured FTP to recover the expenses for an accident/incident in which a non-government 3rd party is at fault. When GSA seeks to recover expenses for an accident/incident in which a 3rd party is at fault a file of requisite CARS data is transmitted to FMESB. The PII information is transmitted for both the driver of the non-government 3rd party vehicle and the owner (if different from the driver). The data is AES-256 encrypted when transmitted to FMESB, which then decrypts the data upon receipt. Apart from CARS collecting accident information, the same information is captured using GSAFleet2Go mobile app. A new module called "Accident Reporting" is added to GSAFleet2Go which is used to collect accidents/incidents information where non-government 3rd parties are involved, the PII information (as referenced above) is captured directly in CARS. The data collected using a mobile app is transmitted to the ClearPath back end system using HTTPS RESTful web services and stored securely in the DMSII database. GSAFleet2GO Accident Reporting module is another form factor for the Fleet drivers to collect and transmit accident information to the Fleet Management System.

## **SECTION 1.0 PURPOSE OF COLLECTION**

*GSA states its purpose and legal authority before collecting PII.*

### **1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?**

Pursuant to 5 U.S.C. §552a (e) (3) GSA provides what is commonly referred to as a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records. FMR 102-34 requires all federal agencies operating a non-tactical vehicle fleet of more than 20 vehicles to have an inventory/asset management system to track and account for those vehicles. FPMR Subpart 101-39.4 - "Accidents and Claims" requires federal agencies operating a GSA-leased vehicle to notify the GSA Fleet of an accident and to provide all related documentation.

**1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?**

CARS allows GSA Fleet personnel to track progress of accident resolution, third-party payment issues, etc. It also includes a reporting tool and document upload feature to store police reports and other official documentation required for accident reporting. CARS holds the relevant data during some or all of the business process. Once an accident enters a claims collection it is then linkable to a person, therefore GSA/PPFM-7 Credit Data on Individual Debtors SORN applies in this instance.

**1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.**

Not Applicable as the Paperwork Reduction Act (PRA) does not apply to the information collected.

**1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.**

Accident Information is retained indefinitely for research and/or investigatory purposes.

Note: Disposition Authority – DAA-GRS-2016-0011-0017 is a document number.

See disposition Authority Number: DM-GRS-2016-0011-0017

[https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0011\\_sf115.pdf](https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2016-0011_sf115.pdf)

**SECTION 2.0 OPENNESS AND TRANSPARENCY**

*GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.*

**2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.**

The individual(s) involved in the accident provide this information, whether for purposes of the Motor Vehicle Accident Report (SF91), the police report, or for 3rd party

Insurance claims. The Privacy Act Notice is included on Page 3 of the SF91 report. When GSA seeks to recover expenses for an accident/incident in which a 3rd party is at fault, a file of requisite CARS data is transmitted to OCFO. The data is AES-256 encrypted with a specific key supplied by OCFO Pegasys System for every 90 days when transmitted to OCFO, who then decrypts the data on their end.

The information is collected through an online screen in CARS application by the authorized FMS users and stored in the database for retrieval and sending the data to OCFO Pegasys System.

## **SECTION 3.0 DATA MINIMIZATION**

*GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.*

### **3.1 Why is the collection and use of the PII necessary to the system, application, or project?**

Fleet applications manage the GSA leased vehicle inventory and track the leased vehicle throughout its useful life, from initial vehicle receipt through operational use/assignment (including: management of accidents, maintenance and repair) to ultimate disposal/sale. All information pertaining to vehicles such as VIN, Tag, Odometer reading, Vehicle equipment, Agency vehicle assigned to, repair vendors, sale information, leasing information are recorded in the Fleet application databases.

The CARS/MARS system collects PII information to track all the accidents that occur to GSA leased vehicles in order to permit GSA to contact the individual driving the car at the time of accident and to recover the expenses for an accident/incident in which a 3rd party is at fault.

### **3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?**

When GSA seeks to recover expenses for an accident/incident in which a 3rd party is at fault, a file of requisite CARS data is transmitted to OCFO. The following PII information is transmitted for both the driver of the 3rd party vehicle and the owner (if different from the driver), but all is submitted by the government employee:

- Driver's First Name, Middle Initial, Last Name
- Home Address (Street Number, City, State, Zip)

- Home Phone Number
- Name of Insurance Company
- Address of Insurance Company (Street Number, City, State, Zip)
- Insurance Company Point of Contact
- Insurance Company Phone Number
- Insurance Policy Number of Driver or Owner

The information is collected through an online screen in CARS application by the authorized FMS users and stored in the database for retrieval and sending the data to OCFO Pegasys System.

The GSAFleet2Go mobile app user shall be prompted to fill out the following data elements:

1. Date of Accident [optional]
2. Police called? [optional]
3. Accident City [optional]
4. Accident State [optional]
5. Type of Accident [optional]
6. No. of Vehicles Involved [optional]
7. Government Drivers First Name [optional]
8. Government Driver's Middle Initial [optional]
9. Government Driver's Last Name [optional]
10. Government Driver's Email [optional]
11. Government Driver's phone number [optional]
12. Other Driver's First Name [optional]
13. Other Driver's Middle Name [optional]
14. Other Driver's Last Name [optional]
15. Other Driver's License State [optional]
16. Other Driver's Driver's License [optional]
17. Other Driver's Address [optional]
18. Other Driver's City [optional]
19. Other Driver's State [optional]
20. Other Driver's Telephone [optional]
21. Other Driver's Insurance Company Name [optional]
22. Other Driver's Insurance Policy Number [optional]
23. Other Driver's Insurance Phone Number [optional]
24. Other Driver's Vehicle Manufacturer [optional]
25. Other Driver's Vehicle Model [optional]
26. Other Driver's Vehicle Year [optional]

27. Other Driver's Vehicle is - {Co-Owned, Rental, Leased, Privately Owned}  
[optional]
28. Other Driver's Vehicle License Plate Number [optional]
29. Other Driver's License Plate State [optional]
30. Government Vehicle towed? {Yes/No} [optional]
  - a. If towed, location and phone of business
    - i. Towing Company Name [optional]
    - ii. Towing Company Phone Number [optional]
31. Brief description of accident [optional]
32. Were the Police Called? {Yes/No} [optional]
33. Was anyone cited? {Yes/No} [optional]
34. Was there a Witness? {Yes/No} [optional]
35. Witness First Name [optional]
36. Witness Middle Initial [optional]
37. Witness Last Name [optional]
38. Witness Telephone Number [optional]
39. Witness Email [optional]

User is prompted to submit Photos of GOV

1. Front License Plate [optional]
2. Driver's Side  $\frac{3}{4}$  - Front [optional]
3. VIN Plate on Window or Door [optional]
4. Driver's Side  $\frac{3}{4}$  - Rear [optional]
5. Rear License Plate [optional]
6. Passenger's Side  $\frac{3}{4}$  - Rear [optional]
7. Passenger's Side  $\frac{3}{4}$  - Front [optional]
8. Damage Close Up [optional]
9. Accident Scene 1 [optional]
10. Accident Scene 2 [optional]

The user is prompted to submit Photos of Other Vehicle

1. Front License Plate [optional]
2. Driver's Side  $\frac{3}{4}$  - Front [optional]
3. VIN Plate on Window or Door [optional]
4. Driver's Side  $\frac{3}{4}$  - Rear [optional]
5. Rear License Plate [optional]
6. Passenger's Side  $\frac{3}{4}$  - Rear [optional]
7. Passenger's Side  $\frac{3}{4}$  - Front [optional]
8. Damage Close Up [optional]
9. Accident Scene 1 [optional]
10. Accident Scene 2 [optional]

GSAFleet2Go prompts for the following OPTIONAL device specific functionalities to collect (i.e., accessing current location and accessing the user's phone's camera to take accident photos). Before collecting the following information, users will be prompted by both the iOS and Android devices to "Allow" the app to collect the following information. The GSAFleet2GO users can always go back and change their choice at will. If the user denies the permission for the app to access those functionalities, the users will not be able to leverage those functionalities. This will not prevent the user from recording all other non-photo or location accident/incident data and submitting an accident report. Furthermore, if a user decides they no longer wish to allow the app to use their phone's photo or location functionality, they can remove the app's access to these functionalities in their phone's settings.

- 1. Location information:** As part of data collection of accidents, users are given the option to "Locate" the device to collect the City and State information so that the users can avoid typing. This data collection is a "snapshot" of the user's current location and



does not continue to collect location information after the current location of the user is populated in the form. If the user manually permits/allows the app to access the location services from the device then the City and State information will be pre populated in the corresponding text boxes. The user can choose to not allow this functionality and simply manually enter their location information.

**2. Camera:** As part of data collection of accidents, users can use the camera to capture accident scenes and upload it to the backend system. Users need to manually allow the app to access the camera functionality. If they permit then the users can capture images of the accident scene. If the user denies the app for accessing the camera then the images are not captured. When the images are captured by the app, no metadata information is collected by the app. The images are securely transmitted to the backend system using secured (TLS) api calls. The images are stored in the mainframe file system after being encrypted using FMS encryption keys. The encryption keys are securely stored as per the security specification for FMS.

**3. Media Gallery:** As part of data collection of accidents, users can use the gallery to upload accident scenes images already captured by the user and then upload it to the backend system. Users need to manually allow the app to access the gallery functionality. If they permit then the users can upload images of the accident scene from their media gallery. If the user denies the app for accessing the media gallery then the images are not uploaded (this does not prevent the user from submitting an accident report). When the images are captured by the app no metadata information is collected by the app. The images are securely transmitted to the back-end system using secured (TLS) api calls. The images are stored in the mainframe file system after being encrypted using FMS encryption keys. The encryption keys are securely stored as per the security specification for FMS.

**4. Push Notification:** As part of alerting the users for vehicle recall and preventive maintenance, push notifications are sent to users if the user decides to opt in. Both Email notification and device push notification opt ins are provided during the profile setup. If the push notifications are opted by the user during the profile setup, the device will prompt for the user to Allow the app to send notifications.

**5. Network Access:** The app will use the Internet to make API calls to the backend system. The back end RESTful API calls are made using HTTPS protocol.

### **3.3 What protections exist to protect the consolidated data and prevent unauthorized access?**

FMS defines roles and responsibilities associated with each permission given to the users. Based on that, access is only granted to required users. Annual Privacy Training provides guidelines for the use of sensitive information. The transactions reports are produced and is available for management review on a daily basis. Any discrepancy

found is corrected and informed to the users. It's FMS Regional manager's discretion to remove the permission assigned or the user id. Each user id and roles/permission is reviewed annually and certified by the managers.

### **3.4 Will the system monitor the public, GSA employees, or contractors?**

The information accessed by GSA employees only. FMS defines roles and responsibilities associated with each permission given to the users. Based on that, access is only granted to required users. Annual Privacy Training provides guidelines for the use of sensitive information. The transaction reports are produced and are available for management review on a daily basis. Any discrepancy found is corrected and informed to the users. It's FMS Regional manager's discretion to remove the permission assigned or the user id. Each user id and roles/permission are reviewed annually and certified by the managers.

### **3.5 What kinds of report(s) can be produced on individuals?**

Standard procedure is for a Police Report and Standard Form 91 (SF91 - Motor Vehicle Accident Report) to be submitted for all accidents/incidents, whether there is a nongovernment 3rd party involved or not. The SF91 is completed by the government driver. The Police report contains information about **both parties** involved, to include:

- Driver's First Name, Middle Initial, Last Name
- State of License / License ID Number
- Home Address (Street Number, City, State, Zip)
- Home Phone Number
- Date of Birth / Sex / Name on vehicle registration
- Vehicle Tag Number / Year / Make / Model
- Circumstances / Summary of the Accident

The Police Report and SF91 are sent electronically (i.e., as attachments) to the AMC's e-mailbox. Documents faxed from the police station are converted to digital format and emailed to this email account.

The AMC uploads the Police Report and SF91 associated with the specific incident/accident record in CARS, however, CARS does not store these documents or associated data locally. **CARS do not capture/store/maintain sensitive PII directly in the database.** The PII data is collected in PDF or image format and uploaded via a J-upload facility that is accessed **through** the CARS application, but the data is transferred immediately and directly to the ECMS. Any/All PII data are not stored in or retrieved

from the CARS database. All files are encrypted during transmission to the ECMS server. The CARS program calls the ECMS web services program and sends the file to ECMS server for storage and retrieval.

**3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?**

None

**SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION**

*GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.*

**4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?**

Yes – the information is limited to only the information that is needed to carry out the purpose of the collection

**4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?**

The PII data is collected in PDF or image format and uploaded via an online program in CARS application, but transferred immediately and directly to the ECMS server using web service call. All PII files are sent securely to ECMS and stored in ECMS server encrypted. Once transferred to the ECMS server, the information is only accessible by authorized CARS users.

In the case of accidents/incidents where non-government 3rd parties are involved, PII information is captured directly in CARS for both the driver of the 3rd party vehicle and the owner (if different from the driver).

When GSA seeks to recover expenses for an accident/incident in which a non-government 3rd party is at fault a file of requisite CARS data is transmitted to OCFO (after data is transmitted to OCFO it generally is not sent anywhere else; only in case of fraud or courts it is sent over to GSA IG for investigative purposes). The PII information is transmitted for both the driver of the 3rd party vehicle and the owner

(if different from the driver). The data is AES-256 encrypted with a private key updated annually when transmitted to FMESB, which then decrypts the data on their end.

**4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?**

Directly from the Driver(s) or any other witnesses.

**4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?**

The PII data is collected in PDF or image format and uploaded via an online program in CARS application, but transferred immediately and directly to the ECMS server using web service call. All PII files are sent securely to ECMS and stored in ECMS server encrypted. Once transferred to the ECMS server, the information is only accessible by authorized CARS users.

In the case of accidents/incidents where non-government 3rd parties are involved, PII information is captured directly in CARS for both the driver of the 3rd party vehicle and the owner (if different from the driver).

When GSA seeks to recover expenses for an accident/incident in which a non-government 3rd party is at fault a file of requisite CARS data is transmitted to OCFO. The PII information is transmitted for both the driver of the 3rd party vehicle and the owner (if different from the driver). The data is AES-256 encrypted with a private key updated annually when transmitted to FMESB, which then decrypts the data on their end.

**SECTION 5.0 DATA QUALITY AND INTEGRITY**

*GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.*

**5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?**

It is the individual who provides this information, whether for purposes of the Motor Vehicle Accident Report (SF91), the police report, or for 3rd party insurance claims. Provided this information is verified by the police with the source (an individual) and it is then sent to AMC by the customer. The CARS users with appropriate permission can

update the information through an online screen in the CARS application to fix any erroneous data reported.

## **SECTION 6.0 SECURITY**

*GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

### **6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?**

FMS and CARS application is designed to operate based on user profile and permissions. Only authorized GSA Fleet AMC / MCC technicians are identified and allowed to access the application. FMS Regional Managers request the user access through an online FMS screen. The FMS central office personnel verify and decide whether to grant the permission required and authorize the use of the system.

**Privacy Risk:** FMS CARS users are authorized by FMS Managers with necessary permissions to receive data, files and upload the same into ECMS server and certified annually, there is no risk associated with the function. However, if the ECMS system or FMS database is compromised, then there is potential risk to individuals whose information is stored within the system.

**Mitigation:** Login ID (LID) certification is done annually after careful review of each and every LID and their associated permission. ECMS server and FMS database is 19 secured with monthly scan of the server and any findings are fixed within the required timeframe.

### **6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?**

Yes. The current ATO is scheduled to expire December 31, 2020.

### **6.3 How will the system or application be secured from a physical, technical, and managerial perspective?**

Physical access to the facility is monitored by 24-hour guard protection, a badge control system and an interior and exterior video surveillance capability consisting of 59 cameras and motion detection sensors. The Site Security Office staff responds to physical security incidents. Physical access is limited to only authorized Unisys personnel and protected by

card key access. From a practical standpoint the risk of a bad-actor to enter the computer room and plug into a switch is remote.

The Site Security Office monitors physical intrusion alarms and surveillance equipment; specifically, a door alarm system is installed that is triggered on unauthorized attempts and CCTV monitoring is deployed.

Login ID (LID) certification is done annually after careful review of each and every LID and their associated permission. ECMS server and FMS database is secured with a monthly scan of the server and any findings are fixed within the required timeframe.

Only authorized GSA Fleet employees have access to the system. The system maintains logs for each and every transaction coming into the system and updates are tracked based on the user profile.

All media are kept in badge-access controlled areas. Tapes are encrypted using AES 256 and are kept in physical hardware cabinets. Once data is backed up onto tapes, the tapes are ejected from the tape library (aka 'silo') and placed in special tubs and taken to Iron Mountain facilities by the Iron Mountain vendor.

#### **6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?**

As per the FMS System Security Plan (SSP), FMS has procedures in place for identifying and handling security incidents and privacy breaches. For example, FMS transmits security events to GSA's enterprise-wide Security Information and Event Management (SIEM) monitoring tool. FMS application personnel monitor use of the system and the status of the mobile app. They are responsible for reporting any potential incidents directly to the Information Systems Security Officer. This Officer coordinates the escalation, reporting and response procedures on behalf of GSA.

### **SECTION 7.0 INDIVIDUAL PARTICIPATION**

*GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.*

**7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.**

The GSA Privacy Office develops privacy policies and manages the GSA privacy program. The GSA IT Security Policy and GSA requirements for PIAs, SORNs, Privacy Act Statements, Annual Reviews of system notices ensure that GSA identifies the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection; limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice for which the individual has provided consent. If consent is not provided by the individual then the collection of information will not take place.

It is the individual who provides this information, whether for purposes of the Motor Vehicle Accident Report (SF91), the police report, or for 3rd party insurance claims. The CARS users with appropriate permission may provide access to the information through an online screen in the CARS application.

## **7.2 What procedures allow individuals to access their information?**

Individuals have the ability to access their PII maintained in the GSA system(s) of records. GSA publishes CFR Part 105-64 GSA Privacy Act Rules, which governs how individuals may request access to records maintained in a Privacy Act system of records. GSA also provides access procedures in the system of records notices and adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act Requests.

It is the individual who provides this information, whether for purposes of the Motor Vehicle Accident Report (SF91), the police report, or for 3rd party insurance claims. The CARS users with appropriate permission may provide access to the information through an online screen in the CARS application. The police report filled out by the individuals involved in the accident/incident is verified by the law enforcement personnel before exchanging with the drivers. No other cross verification is done for non-government 3rd party information collected where 3rd party is responsible for the accident.

## **7.3 Can individuals amend information about themselves? If so, how?**

Yes, the police report filled out by the individuals involved in the accident/incident is verified by the law enforcement personnel before exchanging with the drivers. No other cross verification is done for non-government 3rd party information collected where 3rd party is responsible for the accident.

The GSA Privacy Office develops privacy policies and manages the GSA privacy program. GSA provides a process for individuals to have inaccurate PII maintained by

the organization corrected or amended, as appropriate; and, establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners, and where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. More information about PII redress can be found in CFR Part 105-64 GSA Privacy Act Rules.

## **SECTION 8.0 AWARENESS AND TRAINING**

*GSA trains its personnel to handle and protect PII properly.*

### **8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.**

The GSA Privacy Office develops privacy policies and manages the GSA privacy program. GSA has developed, implemented, and regularly updates, develops, implements, and updates IT Security Awareness and Privacy Training 201, a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities. All GSA account holders electronically sign the GSA Rules of Behavior before taking privacy training exit exams. GSA privacy training includes targeted role-based privacy training for personnel having responsibility for PII and ensures that personnel certify acceptance of responsibilities for privacy requirements.

GSA mandates all employees to complete annual Security and Privacy Awareness Training. It provides training on how to Share Data Securely in a Collaborative Environment.

## **SECTION 9.0 ACCOUNTABILITY AND AUDITING**

*GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.*

### **9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?**

The GSA Privacy Office develops, disseminates, and updates quarterly FISMA reports and works with other program offices to respond to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to



senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

FMS and CARS application is designed to operate based on user profile and permissions. Only authorized GSA Fleet AMC / MCC technicians are identified and allowed to access the application. FMS Regional Managers request the user access through an online FMS screen. The FMS central office personnel verify and decide whether to grant the permission required and authorize the use of the system.

---

<sup>[1]</sup>OMB Memorandum [\*Preparing for and Responding to the Breach of Personally Identifiable Information\*](#) (OMB M-17-12) defines PII as: “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” The memorandum notes that “because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.”

<sup>[2]</sup> Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

<b>Acronym</b>	<b>Description</b>
AIE	Agency Incurred Expenses
AIM	Acquisition Management Program
AMC	Accident Management Center
ARM	Automated Remarketing Module
ATO	Authorization to Operate
CAM	Customer Acquisition Module
CARS	Comprehensive Accident Reporting System
CCTV	Closed-circuit television
DRM	Dispatch Reservation Module
ECMS	Enterprise Content Management System
FAS	Federal Acquisition Service
FedFMS	Federal Fleet Management System
FISMA	Federal Information Security Management Act
FIPPs	Fair Information Practice Principles
FMESB	Financial Management Enterprise Service Bus
FMR	Federal Management Regulation
FMS	Fleet Management System
FMVRS	Federal Motor Vehicle Registration System
FPMR	Federal Property Management Regulation
GEAR	Government Effectiveness Advanced Research
GSA	General Services Administration
HTTPS	Hypertext Transfer Protocol Secure
ICR	Information Collection Request
LID	Login ID

MARS	Mechanical Accountability Reporting System
MCC	Maintenance Control Center
NARA	National Archives and Records Administration
OCFO	Office of Chief Financial Officer
OMB	Office of Management and Budget
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act
SIEM	Security Information and Event Management
SORN	System of Records Notice
SSP	System Security Plan
STR	Short Term Rental
TLS	Transport Layer Security
TTL	Travel and Transportation Logistics
VFE	Vehicle Fleet Exchange
VIN	Vehicle Identification Number