Fleet Management System

Privacy Impact Assessment

November 20, 2018

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer

GSA IT

1800 F Street, NW

Washington, DC 20405

Table of contents

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 the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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 for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline 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?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

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

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

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

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about Fleet Management System, Travel and Transportation Logistics (TTL) may, in the course of CARS/MARS application and GSAFleet2Go mobile app, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] 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, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of 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 that are codified in the Privacy Act of 1974.[2]

System, Application or Project

Fleet Management System

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. FMS 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).

System, application or project includes

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).

Overview

The Fleet Management System identifies individuals by name in conjunction with other data elements such as gender, race (for Police report), birth date, age, geographic indicator, personal e-mail address, home address, home phone number, health records, Driver's License Number, personal credit card information, and similar personal 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 attached form) is securely transferred to the Enterprise Content Management System (ECMS) server. The FMS user receives the PDF documents or image format and uploaded via online program using an online screen and transfers the documents to ECMS server by calling a web service program. All files are encrypted during transmission to the ECMS server. The document is stored securely in ECMS. The FMS online screen also allows the user to retrieve the documents through the web service program to review or replace the documents already uploaded into ECMS server.

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 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) and the accident photos. 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 Why is GSA collecting the information?

Fleet Management System need to process the accident information from the affected parties in the case of accidents/incidents where non-government 3rd parties are involved. It's mandatory for GSA Fleet to send the billing information to FMESB for collecting the amount from federal agencies and third party customers.

1.2 What legal authority and/or agreements allow GSA to collect the information?

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. FMS was originally developed in 1985/1986 to automate the management of the GSA Fleet leased vehicle inventory. The platform has been through several significant updates since then.

FPMR Subpart 101-39.4 - "Accidents and Claims" requires federal agencies operating a GSA-leased vehicle to notify GSA Fleet of an accident and to provide all related documentation.

1.3 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 being collected?

CARS does not allow the stored forms or images to be accessed via a personal identifier; therefore, no SORN is required. The records are only accessed by a system-generated Control Number or a piece of information associated with the vehicle (e.g., license plate or VIN). PII is not used to access any records in CARS. CARS does not allow retrieval of 3rd Party Claim information using the CARS Third Party Multi-Inquiry Function. The information can be retrieved either through a Vehicle Tag # or Claim number.

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 transferred immediately and directly to the ECMS server. All files are encrypted during transmission to the ECMS server. Except non-government 3rd party data to recover the expenses for involving in the accident/incident, all other data is not stored in CARS. Once transferred to the ECMS server, the information is only accessible by authorized CARS users and, as stated above, not accessed via a personal identifier.

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.

1.4. Has any 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 PRA does not apply to the information collected.

1.5. 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 may be retained beyond 3 years if required for business reasons. 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

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

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.

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 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 secured with monthly scan of the server and any findings are fixed within the required timeframe.*

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing 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.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

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.

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 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 secured with monthly scan of the server and any findings are fixed within the required timeframe.*

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII 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 Whose information is included in the system, application or project?

PII information is collected for both the driver of the 3rd party vehicle and the owner (if different from the driver).

3.2 What PII will the system, application or project include?

The following PII information is transmitted for both the driver of the 3rd party vehicle and the owner (if different from the driver):

-- 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

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

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.

3.4 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 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 following PII information is transmitted for both the driver of the 3rd party vehicle and the owner (if different from the driver):

-- 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 Drivers 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 ¾ - Front [optional]*
3. *VIN Plate on Window or Door [optional]*
4. *Driver's Side ¾ - Rear [optional]*
5. *Rear License Plate [optional]*
6. *Passenger's Side ¾ - Rear [optional]*
7. *Passenger's Side ¾ - 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 ¾ - Front [optional]*
3. *VIN Plate on Window or Door [optional]*

4. *Driver's Side ¾ - Rear [optional]*
5. *Rear License Plate [optional]*
6. *Passenger's Side ¾ - Rear [optional]*
7. *Passenger's Side ¾ - 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 users of 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 accident, 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 chose to not allow this functionality and simply manually enter their location information.*
2. *Camera: As part of data collection of accident, users can use the camera to capture accident scenes and upload it to backend system. Users need to manually allow the app to access the camera functionality. If they permit then the users can capture images of 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 are 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 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 accident, users can use the gallery to upload accident scenes images already captured by the user and then upload it to 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 are 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 encrypted using FMS encryption keys. The encryption keys are securely stored as per the security specification for FMS.*
4. *Push Notification: As part of the alerting the users for vehicle recall and preventive maintenance, push notifications are send 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.*

3.5 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.

3.6 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 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.

3.7 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 non-government 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 sensitivePII 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.*

3.8 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.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

None

SECTION 4.0 LIMITS ON USES AND SHARING OF 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.

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. 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 private key updated every 90 days 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 individuals.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and 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 private key updated every 90 days when transmitted to FMESB, which then decrypts the data on their end.

4.5 Are there any privacy risks for this system, application or project that relate to use limitation? If so, how will GSA mitigate these risks?

None.

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 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. Providing this information is verified by the police with the originals and 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.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

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. Providing this information is verified by the police with the originals and sent to AMC by the customer. 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.

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 is identified and allowed to access the application. FMS Regional Managers request the user access through an online FMS screen. The FMS central office personnel decides verifies and decides 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 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*

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 for the information system(s) or application?

Yes. Issuing final ATO is in progress and extension granted until March 31, 2019.

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

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 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.

6.4 Are there mechanisms in place to identify 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.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

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 decides verifies and decides 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 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 secured with monthly scan of the server and any findings are fixed within the required timeframe.*

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 are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

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?

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.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

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 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 secured with monthly scan of the server and any findings are fixed within the required timeframe.*

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.

GSA mandates all employees to complete annual Security and Privacy Awareness Training, training on how to Share Data Securely in a Collaborative Environment and other trainings as appropriate.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

Yes. The mandated training helps understand the significance of risks involved in safeguarding the data collected from the individuals.

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, application or project ensure that the information is used in accordance with the stated practices in this PIA?

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

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

None.

---

[1] OMB Memorandum *Preparing for and Responding to a 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."

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