## Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

## Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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, 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.[2]

[1]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."

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

## General Information

PIA Identifier: 405
System Name: GSAFleet.gov
CPO Approval Date: 5/17/2023
PIA Expiration Date: 5/16/2024

## Information System Security Manager (ISSM) Approval

Joseph Hoyt

## System Owner/Program Manager Approval

Mohamed Chaouchi

## Chief Privacy Officer (CPO) Approval

Richard Speidel

## PIA Overview

**A:** System, Application, or Project Name:
GSAFleet.gov

**B:** System, application, or project includes information about:

GSAFleet.gov supports the $1.5+ billion-per-year vehicle purchasing program for the entire federal government. It also supports the $2+ billion-per-year Fleet vehicle leasing program that covers full vehicle life-cycle management for GSA's leased vehicle inventory. GSAFleet.gov includes the following components/subsystems below:

- Catalog
- Store
- Vehicle Management Services
- Maintenance and Repair
- Vehicle Marketplace
- Business Management

The system is used by the GSA Fleet organization, Customer Agencies, Fleet-related vendors and the general public. Additionally PII may be collected as part of Fleet's Accident Management and Vehicle Sales processes.

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

- Approximate GSA Fleet Management users: 550
- Approximate GSA non Fleet Management users: 100
- Approximate non GSA users: 35,600 comprising of
    - 35,000 Customers
    - 600 Vendors
    - 3,500 registered users on the two public facing sites operating under a single authorized account

Third-party accident records: Approximately 50,000
Sales records: Approximately 200,000

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

The following PII information is collected when a user registers for GSAFleet.gov:

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

- Social Security Numbers

Additionally, PII may be collected as part of Fleet's Accident Management and Vehicle Sales processes. The Accident Management component of GSAFleet.gov may collect PII when 3rd parties are involved in an accident or incident.

The following PII information (data elements for accident investigation and recovery) for non government entities 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
- PII for police reports
- Third party insurance
- Vehicle Information
- Personal credit card information or as required in the SF91 form - https://www.gsa.gov/forms-library/motor-vehicle-accident-report.

The Vehicle Marketplace component of GSAFleet.gov collects PII as part of the vehicle sales process. Data elements collected during the sales process include Name, Organization, Address of the successful bidder as well as the amount paid, and social security numbers. GSAFleet.gov collects, transmits, and stores social security numbers. GSAFleet.gov collects, transmits, and stores social security numbers for purposes of users to purchase vehicles via GSAFleet.gov. Social security numbers are transmitted to Experian to determine a user's credit worthiness to purchase a vehicle.

## Overview:

Advanced Fleet Platform (AFP) modernization effort encompasses the transition of legacy Fleet business operations that includes:

● Instituting a product mindset focused on the business services and user experience to make sure they are well understood, and to adapt to their changing needs
● Updating business processes and organizational infrastructure
● Migrating from legacy Unisys mainframe-based and Microsoft Windows Server-based systems to an up-to-date cloud-based application.

The modernization of this system will be incremental with the first minimum viable product (MVP) scheduled for release in February, 2021. This MVP release will be followed by incremental release of functionalities until all existing capabilities are migrated from legacy Fleet applications.

AFP includes the following components also known as Fleet products:

● Catalog
● Store
● Vehicle Management Services
● Maintenance and Repair
● Vehicle Marketplace
● Business Management

Below is a description of each component:

Catalog – The Catalog marries customer needs, industry standards, government policies, and vendor availability to make offerings and services available for agency acquisition.

Store – The Store is a simple and personalized shopping experience for researching and acquiring GSA Fleet offerings. Store provides tools to analyze current fleets, provide best value recommendations for right-sizing and right-sourcing, and help customers to be great stewards of taxpayer dollars.

Vehicle Management Services (VMS) – VMS provides customers with safe, reliable vehicles and tools to meet their mission. VMS is the face of GSA Fleet for customers.

Maintenance and Repair – The Maintenance and Repair product maintains the safety and reliability of vehicles in order to keep them on the road utilizing technical and industry expertise to make decisions based on best value.

Vehicle Marketplace – GSA Fleet Vehicle Marketplace is a one-stop-shop for vehicle buying needs. This is used to remarket government vehicles for the greatest return on investment to the taxpayer.

Business Management – Business Management maximizes the value of taxpayer dollars while ensuring sustainable financial operations of the organization. Business Management helps capture and characterize the financial impact of business activities, in order to inform future decisions.

The system is used by GSA Fleet Managers, Fleet Service Representatives, Drivers, Vendors, Sales Contracting Officers, Contract Specialist, and General Public.

### 1.0 Purpose of Collection

**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?
No

**1.2a:** If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
**1.2: System of Records Notice(s) (Legacy Text):** What System of Records Notice(s) apply/applies to the information?
GSA reviewed its Privacy Act systems to ensure that they are relevant, necessary, accurate, up-to-date, covered by the appropriate legal or regulatory authority, and in response to OMB M–07–16. This notice is a compilation of updated Privacy Act system of record notices. https://www.federalregister.gov/documents/2008/04/25/E8-8925/privacy-act-of-1974-notice-of-updated-systems-of-records

https://www.federalregister.gov/documents/2008/04/25/E8-8925/privacy-act-of-1974-notice-of-updated-systems-of-records

**1.2b:** Explain why a SORN is not required.

**1.3:** Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

**1.3: Information Collection Request:** Provide the relevant names, OMB control numbers, and expiration dates.

**1.4:** What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
System records are retained and disposed of according to GSA records maintenance and disposition schedules.

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-grs2016-0011_sf115.pdf

### 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? Yes

**2.1 Explain:** If not, please explain.

### 3.0 Data Minimization
**3.1:** Why is the collection and use of the PII necessary to the project or system?
Accidents: GSAFleet.gov collects PII that is required for police reports, third-party insurance, and to recover the expenses for an accident/incident in which a 3rd party is at fault.

Sales: GSAFleet.gov collects PII that is required for the sale/transfer of government property, as well as to collect the proceeds of the sale.

**3.2:** Will the system, application, or project create or aggregate new data about the individual?

Yes

**3.2 Explained:** 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 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 by the authorized users and stored in the database for retrieval and sending the data to OCFO Pegasys System.

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

In accordance with the Federal Information Security Management Act of 2002 (FISMA), every GSA system must receive a signed Authority to Operate (ATO) from a designated GSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program.

Additionally, GSAFleet.gov defines roles and responsibilities associated with each permission given to the users. Based on that, access is only granted to required users with a need-to-know. Annual Privacy Training provides guidelines for the use of sensitive information. The transactions reports are produced and are available for management review. The roles/permission of a user are reviewed annually and certified by their managers. However, managers may downgrade or remove a user's roles/permissions at any time.

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

GSA Employees

**3.4 Explain:** Please elaborate as needed.

GSAFleet.gov is not designed to monitor the public. However, GSA employees or contractors with the ability to log into system transactions are logged via the audit logs.

**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, and may contain:

- 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 Accident Management Center's (AMC) inbox. Documents faxed from the police station are converted to digital format and emailed to the AMC account.

The AMC uploads the Police Report and SF91 associated with the specific incident/accident record, however, the system does not store these documents or associated data locally. The system does not store the Police Report in the database. The Police Report is collected in PDF or image format and stored in EDMS. All files are encrypted during transmission to the EDMS server.

During the vehicle sales process, Experian produces a credit report. Social security numbers are transmitted to Experian to determine a user's credit worthiness to purchase a vehicle.

**3.6** Will the data included in any report(s) be de-identified?
No

**3.6 Explain:** If so, what process(es) will be used to aggregate or de-identify the data?

**3.6 Why Not:** Why will the data not be de-identified?
None

**4.0 Limits on Using and Sharing 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?
Yes

**4.2:** Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
Private-Sector Organizations

**4.2How:** If so, how will GSA share the information?
When GSA seeks to recover expenses for an accident/incident in which a nongovernment 3rd party is at fault, a file of requisite 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

**4.3Other Source:** What is the other source(s)?

**4.4:** Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
Yes

**4.4WhoHow:** If so, who and how?
Accidents: The PII data is collected in PDF or image format and stored in the EDMS server using web service call. All PII files are sent securely to EDMS and stored in the EDM Server encrypted. Once transferred to the EDMS server, the information is only accessible by authorized users.

In the case of accidents/incidents where non-government 3rd parties are involved, PII information is captured 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 nongovernment 3rd party is at fault, a file of requisite 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.

**4.4Formal Agreement:** Is a formal agreement(s) in place?
Yes

**4.4NoAgreement:** Why is there not a formal agreement in place?

### 5.0 Data Quality and Integrity

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

Accident: It is the responsibility of 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 the customer.

Sales: It is the responsibility of the winning bidder or Auction House who provides this information. The system users with appropriate permission can update the information through an online screen in the application to fix any erroneous data reported.

### 6.0 Security

**6.1a:** Who or what will have access to the data in the system, application, or project?

Accidents: GSAFleet.gov is designed to operate based on user profile and permissions. Only users with a need-to-know to perform duties are provided access to PII. User access must be reviewed and certified at least annually.

Social security numbers are transmitted to Experian to determine a user's credit worthiness to purchase a vehicle.

**6.1b:** What is the authorization process to gain access?

**Privacy Risk**: GSAFleet.gov users are authorized by Managers with necessary permissions to receive data, files and uploaded to the server. User's permissions are reviewed and certified annually. However, if the GSAFleet.gov database is compromised, then there is potential risk to individuals whose information is stored within the system.

**Mitigation**: User's roles and permissions are reviewed and certified annually. GSAFleet.gov are secured with monthly scans of the server and any findings are fixed within the required timeframe.

**6.2:** Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

**6.2a:** Enter the actual or expected ATO date from the associated authorization package.
2/1/2022

**6.3:** How will the system or application be secured from a physical, technical, and managerial perspective?
A security controls assessment of GSAFleet.gov has been conducted at the Federal Information Processing Standards (FIPS) 199 Moderate Impact level in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 2, "Guide for Applying the Risk Management Framework to Federal Information Systems", and General Services Administration (GSA) IT Security Procedural Guide CIO-IT Security-06-30, "Managing Enterprise Risk". The system has been assessed by Valiant using the assessment methods and procedures required by the system's assessment process as described in CIO-IT Security-06-30 to determine the level of risk associated with operating the system and the effectiveness of the system's security controls in satisfying the security requirements of the system.

User account requests must be approved by their designated manager. Managers are responsible for applying the correct roles and permissions to their users. All user roles and permissions must be reviewed and certified annually. User access requires multi-factor authentication through OKTA or SSO. The system maintains logs for each and every transaction coming into the system and updates are tracked based on the user profile. All GSAFleet.gov data is encrypted in transit. The only exception is HTTP requests from the internet, which are immediately redirected to HTTPS. All data stored at rest is also encrypted. GSAFleet.gov encrypts its EC2 instances and EBS stores to protect the confidentiality and integrity of their information at rest. GSAFleet.gov also sets up, configures, and manages its systems within the AWS-provided VPC to partition it away from other domains/environments to ensure proper segregation.

To ingest PII data from the Legacy system:
***1) Legacy file for the dataset containing original (not encrypted) PII and other fields will be transferred via SFTP to the encrypted S3 bucket in Fleet VPC***
***2) The file will be subsequently ingested by Streamsets pipeline from S3, which will encrypt PII fields and store dataset in the AFP (MySQL) Database in the respective environment (Dev, Test, Stage, Prod). The target database tables will contain encrypted PII fields and other fields from the dataset as not encrypted.***
***3) If AFP Web application needs to display the PII data to the authorized users, it will perform decryption of respective database fields before display.***
***4) If AFP Web application needs to update or add PII data, on request of authorized user, it will perform encryption of PII fields before storing data to AFP Database***

**6.4:** Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

**6.4What:** What are they?
As per the GSAFleet.gov System Security Plan (SSP), GSAFleet.gov has procedures in place for identifying and handling security incidents and privacy breaches. For example, GSAFleet.gov transmits security events to GSA's enterprise-wide Security Information and Event Management (SIEM) monitoring tool. GSAFleet.gov application personnel

monitor use of the system. 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.

**7.0 Individual Participation**

**7.1:** What opportunities do individuals have to consent or decline to provide information?

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), police report, or for 3rd party insurance claims or vehicle sales.

**7.1Opt**: Can they opt-in or opt-out?

Yes

**7.1Explain**: If there are no opportunities to consent, decline, opt in, or opt out, please explain.

**7.2:** What are the procedures that 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 or vehicle sales. A GSAFleet.gov user with appropriate permission may provide access to the information. 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. Individuals are provided

information about their credit worthiness determination and can request a copy of their credit report from Experian.

**7.3:** Can individuals amend information about themselves?
Yes

**7.3How**: How do individuals amend information about themselves?
GSAFleet.gov users have the ability to amend PII by submitting an email request or by phone call. Users are provided step-by-step instructions via GSA Fleet Technical Support team at fleet.helpdesk@gsa.gov or 866-472-6711 from 8:00 a.m. - 7:00 p.m. ET, Monday–Friday.

### 8.0 Awareness and Training

**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.

### 9.0 Accountability and Auditing

**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.

GSAFleet.gov is designed to operate based on user profile and permissions. Access and permissions are based on a need-to-know to perform job duties.  User access and related permissions are reviewed and certified annually