

General Information

PTA / PIA Name:	OS - PSC-OV: EMP - QTR1 - 2026 - OS3284580	PTA / PIA ID:	4267613
Component Name:	OS - PSC-OV: Executive Motor Pool	ATO Boundary Name:	Network Infrastructure Edge Services 1.0
Overall Status:	Complete 	# of Days - Open:	40
Submitter:		Submit Date:	3/9/2026
Next Assessment Date:	03/10/2029	Expiration Date:	3/10/2029
Office:		OpDiv:	OS
Security Categorization:	Not Rated		
Make PIA available to Public?:	No	PIA Required:	Yes
General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance	
General 02:	Is this a FISMA-Reportable system?	No	
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes	
General 04:	ATO Date or Planned ATO Date.	12/6/2024	
General 05:	Is the system or electronic information collection, agency or contractor operated?		
History Log:	View History Log		

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Romanus Atanga
PTA 01A:	POC Title and Organization	System Security Privacy Office (SSPO) Program Support Center (PSC), Office of the Director (OD)
PTA 01B:	POC Email Address	romanus.atanga@psc.hhs.gov
PTA 01C:	POC Phone Number	(202) 934-4028
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	There have been no changes since the last PIA.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	This module is used to track requests for rides and driver assignment cases for the HHS Office of the Secretary's (OS) Executive Motor Pool (EMP). It enables case creation for the dispatching of drivers, providing visibility and enabling reporting of service usage. Tracks usage to ensure service is being used in accordance with policies and guidelines. Streamlines billing to customers. Provides scheduling tool for drivers, allowing for insight into their availability. (Future State)

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The PSC (Program Support Center) OneView EMP Module within the PSC Organization collects and maintains the following information: Unique Identifiers (User ID) Personal Information (Name, Email Address, Phone Number) HHS Position Information (Type of Employee/Contractor, Employment Status, Authorized Requestor, Designated Region) EMP Executive Information (Customer Agency, Authorized Requestor) EMP Driver Information (Driver Status, Vehicles (make and model), Vehicle Tag Number, Agency Assignment) Organization Information (Org Path, Alert HHS Org, SCMS Agency Abbreviation, SCMS Sub Agency Abbreviation) Case Information (Case Owner, Pick Up/Drop Off Location Address) Trip Detail Information (Passengers, Assigned Driver, Passenger Notes) Trip Outcome Information (Pick Up Time , Drop Off Time, No Show, Wait Time for Customer, Not on Time Explanation, Stop During Ride, Return to HHH Garage w/no Passengers) Location Information (Building Name, Type, Addresses) All data in OneView is only deleted as required when functionality is deprecated or when data is specifically requested to be removed by the Product Owner. OneView offers the ability to track change history on fields and these changes are stored and visible within OneView for a period of 18 months. PSC (Program Support Center) has purchased field encryption which gives PSC (Program Support Center access to the changes for an extended amount of time up to 10 years if necessary, but only 24 months through the standard user interface.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	The system providing credentials is - Access management system (AMS)

PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	The PSC OneView EMP Module collects and maintains the following information: Unique Identifiers (User ID) Personal Information (Name, Email Address, Phone Number) HHS Position Information (Type of Employee/Contractor, Employment Status, Authorized Requestor, Designated Region) EMP Executive Information (Customer Agency, Authorized Requestor) EMP Driver Information (Driver Status, Vehicles (make and model), Vehicle Tag Number, Agency Assignment) Organization Information (Org Path, Alert HHS Org, SCMS Agency Abbreviation, SCMS Sub Agency Abbreviation) Case Information (Case Owner, Pick Up/Drop Off Location Address) Trip Detail Information (Passengers, Assigned Driver, Passenger Notes) Trip Outcome Information (Pick Up Time , Drop Off Time, No Show, Wait Time for Customer, Not on Time Explanation, Stop During Ride, Return to HHH Garage w/no Passengers) Location Information (Building Name, Type, Addresses) The types of information collected to Book & Track Rides/Driver Assignments, Track & Resolve Customer Service Requests, Track & Resolve Open Tasks, Store Location Information for Trip Bookings, & Maintain Individual Contact Information.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Vehicle Identifiers (e.g., VIN, license plate number) Biographical Information Name Employment Status/History Contact Information Email Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Unique Identifiers (User ID) Personal Information (Name, Email Address, Phone Number) HHS Position Information (Type of Employee/Contractor, Employment Status, Authorized Requestor, Designated Region) EMP Executive Information (Customer Agency, Authorized Requestor) EMP Driver Information (Driver Status, Vehicles (make and model), Vehicle Tag Number, Agency Assignment) Organization Information (Org Path, Alert HHS Org, SCMS Agency Abbreviation, SCMS Sub Agency Abbreviation) Case Information (Case Owner, Pick Up/Drop Off Location Address) Trip Detail Information (Passengers, Assigned Driver, Passenger Notes) Trip Outcome Information (Pick Up Time , Drop Off Time, No Show, Wait Time for Customer, Not on Time Explanation, Stop During Ride, Return to HHH Garage w/no Passengers) Location Information (Building Name, Type, Addresses)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	User Personally Identifiable Information (PII) within the OneView Executive motor Pool (EMP) Module is used by the system to identify individuals & geographical Pick Up/Drop Off Locations.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	N/A - There is no secondary use for PII.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system, including activities such as the collection of PII necessary for operating it, are authorized by 5 U.S.C. 301, which authorizes the Secretary to create regulations necessary for meeting the missions of his or her agency. Further, 42 U.S.C § 3502 creates the Office of the Assistant Secretary for Administration (ASA) at HHS, and among the duties delegated to the ASA are oversight of these services, which are necessary to maintaining the infrastructure of the agency.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Records can be searched using names/last names
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-0777 Facility and Resource Access Control Records SORN history: 75 FR 47812 (8/9/10), *83 FR 6591 (2/14/18) 09-90-0020 Suitability for Employment Records SORN history: 58 FR 28880 (5/17/93); updated 59 FR 55845 (11/9/94), *83 FR 6591 (2/14/18) [Exempt based on (k)(5); see 40 FR 47406 & 40 FR 41140] 09-90-1901 HHS Correspondence, Comment, Customer Service, and Contact List Records, 86 FR 12699 (3/4/21).
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Other HHS OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	Not Applicable - The system does collect PII from authorized users during their onboarding process. However, the Office of Management and Budget (OMB) approval number is not applicable.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS

PIA 32B:

For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.

This information is shared/disclosed in other areas within HHS because Projects and Applications are associated/have direct relationships with Contracts and Contacts and is required in order to be managed within the system. All data/information is encrypted per FIPS-140-2 in transit and in rest. Certain data is shared across all modules, such as Account and Contacts. While some modules do have a need to create Contact records for Case Management, the data collected on their Contacts is restricted to the same as Contacts transmitted to OneView via SCMS (Smart Card Management System). Contact data from SCMS (Smart Card Management System) is limited to the following fields:

Company Name
Email
Region
SCMS Agency Abbreviation
SCMS Sub-Agency Abbreviation
Status
Org Path
Alert HHS Organization
HHS ID (restricted to only System Administrators)

Some modules may request to track situational data such as being an authorized EMP requestor, and these fields are restricted to only the users of the Modules who need those data points. Account Data is manually created for the purposes of associating Contacts with an Account, as this is required by Salesforce. Contacts are also associated to Agency or Sub-Agency. Most other users associate to the Program Support Center Account. No Award information will be stored or accessible in OneView as OneView isn't the system of record for the Contract data

PIA 32C:

List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

Memorandum of Understanding (MOU) Between (PSC) Alert HHS Emergency Notification System And Program Support Center (PSC) OneView Application

MOU Between PSC OV and PSC Work Smarter

MOU between PSC OV and Identity Access Management system (IAM@HHS) AKA Smart Card Management System (SCMS)

PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	Both parties (aka systems: OneView & SCMS (Smart Card Management System) collaborate transparently to ensure the joint security of the connected systems and the data they store, process, and transmit. Both parties (aka systems: OneView & SCMS (Smart Card Management System) have shared responsibilities, some of which are inherited from the Salesforce Federal Risk and Authorization Management Program (FedRAMP) platform, that its' respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and OS policies. Both parties collaborate to maintain the higher level of security (Federal Information Processing Standards (FIPS-199) FedRAMP Moderate) that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the systems as noted in the System Security Plan as well as the Incident Response Plan.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	Individuals are aware of what PII is collected because they either supply it themselves directly or because the use of the information is implicit in the employer/employee relationship. Individuals use this system to track status of employment and/or to receive notifications of work place activities. The uses of their PII are therefore consistent with their expectations and preferences. Individuals can opt-out of providing the information for collection by choosing different employment options.
PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	No major changes to the system that would affect the rights and interests of the data subjects are anticipated. However, if this should change, changes could be communicated by updating the system of records notice (SORN), by phone, e-mail, through newsletters, through supervisors, and/or on the system Intranet itself. Individuals must supply this information if they wish to obtain the status of their HHS account progress (or for some modules, if they wish to receive information on related benefits).
PIA 36:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.	Employees are always able to correct inaccurate information by contacting the business process owner (or the Computer Security Incident Response Team (CSIRC) for more serious misuses). If the issue is not able to be resolved using the previously mentioned method, then that person can speak with their agency's Applicant Rights Representative, and they will be able to provide further guidance.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	When individuals contact users of the system, they are requested to verify some of their information. Some examples include mandatory annual recertification; request for a badge (periodic expiration); the start of a background investigation. Relevant PII data generated within the system is voluntarily provided by the prospective applicant. PII data received into the module from interconnected systems is secured, masked, and access controlled by permissions and user roles. The interface control between systems ensure integrity, relevancy, and accuracy of the data is maintain and updated in accordance with the availability/frequency specified in their design.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	- Users: Users can only input/edit specific PII data for records but not all. PII is stored only in the database and is masked in the UI (User Interface). Users in this role cannot access certain records that they do not own which are associated with accounts that they do own but require access to PII information to fulfill their employment duties that range from a number of different roles such as project managers, hiring managers, product owners, etc. - Administrators: Administrators can view all and edit user personal information and all records so that they can also build on the platform as they are needed in order to manage and accommodate any new system requests/requirements. - Developers: Developers are users who have similar privilege as that of Administrators and are needed to edit & writing custom code within the system to accommodate for custom/nonstandard salesforce functionality. - Contractors: There are two types of Contractor roles that have access to PII. One which is an internal role used to fulfill their employment duties that range from a number of different roles such as project managers, hiring managers, product owners, etc. The second which is an external role identified as a Contractor applicant that is pending approval and can only access their own PII during that time. Contractors with Level 6 Public Trust and HHS Personal Identity Verification (PIV) Cards may serve as system administrators. System administrators have access to all data including PII in the system to provide system support and over all process improvement. Access to PII available based on rights assigned by the Administrators. Users, Developers, or Contractors that are system administrators will have access to see and troubleshoot issues for managers.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Default Least Privilege dictates overarching system access; and in addition, system users undergo suitability screening to ensure they are qualified and meet the required authorization tier for the access that their role requires. Prerequisites for further access is done upon pre-hire and an evaluation in job responsibilities or promotion. Access to PII is tied to an employee's role and is granted based on their position designation, but no more.
PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	Only authorized system administrators/contractors with the appropriate level of clearance have access to PII within the System (EMP Module). Access to PII is tied to an employee's role and is granted based on their position designation, but no more.

PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	All employees and HHS Direct Contractor must undertake HHS cybersecurity awareness, role based, and privacy trainings
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Role-based training is provided to perform the job and in some roles certification is a requirement of access per NIST 800-53. Developers and system administrators do receive specialized training. This training involves learning advanced configuration settings within the modules and may include vendor provided computer based training, HHS training on adhering to privacy regulations, participating in audits and reviews. The general privacy training for users of the system is handled by the HHS Learning Management System (LMS).
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Retention and destruction practices are consistent with the National Archives and Records Administration (NARA) General Records Schedules (GRS) 20, item 2a4, GRS 3, Item 3, Section a.1.b, "Routine Procurement Files," GRS 11, Item 4, "Credentials Files," and GRS 18, Item 22, Section a.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	PII information is secured for the EMP module which inherits its administrative, technical and physical controls from OneView. For example, administrative controls such as administrative process and procedure to obtain PIV Card, access to internal documentations, require for group and role membership; technical controls such as use of external system, information search and retrieval, data mining; physical controls such as two forms of identification, physical access log, lockable casing. Specific application of Administrative, Technical, and Physical controls are listed and detailed within the control catalogue of the HHS OCIO Sponsored FEDRAMP ATO package and maintained at the FISMA Moderate level. Module users are granted specific roles and privileges with specific access rights for their roles within the individual modules.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	Privacy Analyst Review Date:	3/10/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	# of Days - PA Review:	1

SOP Review			
SOP Review Decision:	Approved	SOP Review Date:	3/10/2026
SOP Review Comments:		# of Days - SOP Review:	0

Agency Privacy Analyst Review			
Agency Privacy Analyst Review Decision:	Approved	Agency Privacy Analyst Review Date:	3/11/2026
Agency Privacy Analyst Review Comments:		# of Days - APA Review:	1
Reviewer: Godisgreat Peters 3/11/2026 This PIA is ready for SAOP review and approval. 3/2/2026 Please see comment and update accordingly. PIA-22: Please select or include the following "Phone Number Business/personal), and organization/agency. Also is vehicle (i.e., make and model) and driver (i.e. driver license) information collected? If so please include in your response. Reviewer: Christopher Akhibi 2/19/2026 Please see comments and update accordingly: PTA 5: Please, use 'with' instead of w/no and spell out of "LOE" PIA 39: Please, spell out "PIV"			

SAOP Review					
SAOP Review Decision:		Approved	SAOP Review Date:		3/11/2026
SAOP Review Comments:			# of Days - SAOP Review:		0
SAOP Signature					
Date	User	Type	Name	Original Value	New Value
3/11/2026 11:08 AM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA 22A	Data Feed Service, pta_pia_OS_Release	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	
PIA 22A	Data Feed Service, pta_pia_OS_Release	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	
PIA 22A	AKHIBI, CHRISTOPHER	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	
PIA 22A	AKHIBI, CHRISTOPHER	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	
PIA 22A	PETERS, GODISGREAT	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	
PIA 22A	BLAND, CRYSTAL	3/9/2026	Business phone number is selected. Agency is included in EMP Executive Information. Vehicle information included (make, model, and tag) Driver license number is not collected	