General Information

PTA / PIA Name:	OS - PSC-OV:Gateway - QTR1 - 2026 - OS3284576	**PTA / PIA ID:**	4306468
Component Name:	OS - PSC-OV: Gateway	**ATO Boundary Name:**	Network Infrastructure Edge Services 1.0
Overall Status:	Complete	**# of Days - Open:**	35
Submitter:		**Submit Date:**	2/24/2026
Next Assessment Date:	03/05/2029	**Expiration Date:**	3/5/2029
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 and Privacy officer (SSPO)
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 major changes since the last PIA. Additional data is being collected: Additional Unique Identifiers: New Hire ID, Social Security Number, Alien Registration Number, Passport Number, Visa Number) Employment Information (Supervisor Name, Pay Plan, Series, Grade, Division, Country of Issuance, Effective Date of Appointment, Customer Name, Agency Address, Agency City, Agency State, Agency Post code, Payroll Office Contact, Payroll Office Phone Number, e-Verify Case Number, Supervisor Email, Duty Location City, Duty Location State, Duty Location Code) Additional applicant information: Date of Birth, Place of Birth City, Place of Birth State, Country of Citizenship)
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.	Gateway is a transparent and efficient workplace readiness module that allows applicants and users to track the progress of the intake, suitability, and badging process. Gateway depends upon an integration with Smart Card Management System (SCMS) for the latest Contact data with related email address, HHS ID and onboarding status. The initial application creation and forms submission and review process begin in Gateway, but once submitted to SCMS, via e828 (an SCMS application), other milestones and activities are managed in e828 and transmitted back to Gateway for tracking. Gateway was built initially to onboard new Contractor applicants, and now supports new and existing Contractor applicants and Inter Operations Division (Op/Div). transfers. Employee onboarding is not yet supported in Gateway. The OneView Gateway solution is intended to provide a simplified user experience that supports tracking of overall onboarding status and subtasks for both Applicants and their respective Managers. - Phase 1: Pre-Screening: The Gateway module is currently only able to accept contractor applicants. Hiring managers will initiate a new Gateway Application from the Gateway Applicants tab of the Gateway module in OneView. The Hiring Manager will then populate the required fields for Agency Information, Applicant Information, and Security Information sections. The Hiring Manager will be unable to save the new application if any of the required fields are not populated. Upon successful creation of the application record, an application number is assigned to the contractor, a callout to the e828 system initiates the process in the source system, and the Applicant is sent an email notifying them to log-in and submit their information. The Gateway Applicant receives a Welcome Email with instructions for accessing and logging into the Gateway Community. Once the Applicant has successfully logged into the Gateway Community they will be able complete the required pre-screening steps and track the

		progress of their application. The Applicant is required to verify their General Information Form for accuracy and make updates accordingly. Changes to the fields on the General Information Form will be reflected on the Applicants Contact and Application records once submitted. The Applicant is then required to upload copies of their Resume and their signed OF-306 Form. Applicants should also upload a signed ROB (Rules of Behavior) form. Government Sponsors are able to indicate if the applicant requires elevated access or basic access so that the ROB form can include the appropriate pages. The Rules of Behavior Gateway Step is updated so that the form action/components are the same as that of the OF-306 form values. Update Nintex Docgen Template has been updated to generate a short form if Applicant access is Basic / long form if applicant access is elevated. Once all forms are submitted, the upload function will no longer work for Applicants. Applicants are required to review and certify required U.S. Department of Health and Human Services (HHS) Privacy Act Statement, Non-Disclosure Agreement (NDA), Security Awareness Training, and Rules of Behavior Forms. After submitting the pre-screening forms, the Hiring Manager is notified that the forms have been submitted and ready for review. - Phase 2: Security Evaluation: The Applicant is able to log in to the Salesforce portal where they can view and track their onboarding status through each of the onboarding phases and steps therein. Integration with SCMS allows for system-based triggers to push live status updates to the OneView Gateway. - Phase 3: Pre-Entrance Forms: These steps are specific to Federal Employee Applicants; Contractor Applicants will skip directly to 'Schedule Appointment for Personal Identity Verification (PIV) Card Pick Up'. - Phase 4: Workplace Readiness: In this phase, the employee attends New Employee Orientation (NEO), receives their PIV card, completes workplace readiness activities, receives assets, and completes additional training.
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 OneView Gateway Module within the PSC Organization (Org) collects and maintains the following information: Unique Identifiers (User ID, New Hire ID, Social Security Number, Alien Registration Number, Passport Number, Visa Number) Application Information (Application ID, Agency, Sub-Agency, Division, Region, Government Sponsor Name, Government Sponsor Email, Project Officer Name, Project Officer Email) Employment Information (Supervisor Name, Pay Plan, Series, Grade, Division, Country of Issuance,

Effective Date of Appointment, Customer Name, Agency Address, Agency City, Agency State, Agency Post code, Payroll Office Contact, Payroll Office Phone Number, e-Verify Case Number, Supervisor Email, Duty Location City, Duty Location State, Duty Location Code)

Applicant Information (Applicant, Applicant Type, Applicant Position, Applicant First Name, Applicant Middle Name, Applicant Last Name, Applicant Suffix, Applicant Preferred Name, Applicant Email, Applicant Phone, Applicant Extension, Service Type, Request Type, position automated designated tool (PDAT) Form Completed Status, HHS ID, Applicant ID, External Application ID, Current Zip Code for Badge Location, Personal Card Issuer Facility (PCIF), Date of Birth, Place of Birth City, Place of Birth State, Country of Citizenship)

Contract Information (Company Name, Company Street, Company City, Company Country, Company Phone, Company Street 2, Company Zip Code, Company State, Contract Number, Contract Start Date, Contract End Date, Badge Expiration Date, Agency's Obligating Document #)

Security Processing Information (Federal Emergency Responder, Require Unified Financial Management System (UFMS) Access, Required IT Admin, HHS Simple Mail Transfer Protocol (SMTP) Email Address, User Principal Name (UPN) Email Address, Security Processing Notes)

Status Information (Current Phase, Current Onboarding Step, External System Status, Application Status, Gateway Display Status, Gateway Display Status Last Updated, Rejected Reason, Created By Contact, Last Modified Contact/ Date/Time, Application Owner)

Gateway Step Information (Gateway Step Name, Parent Step, Supervisor Onboarding Step, Gateway Display Status, Phase, Step Description, Service Type, Step Hover Text, Step Order, Form Type, Active Status, Form Action, Display As, Form Component, Mark Step Completed Status, Form Component, Mark Step Completed Status, Do Not Send Form Status, Create History Record for Step Status)

Gateway related Reports & Dashboards

Customer Information (Customer Name, Account Record Type, Parent Account, Customer Owner, Agency, Billing Address, Shipping Address, Phone, Phone Extension, Website, Gateway Customer Type, Gateway Abbreviation, SCMS Agency ID, Requesting Organization, Description)

Contact Information (Name, Contact Owner, Title, Contact Record Type, Customer Name, Type, Status, Suffix, Agency, Service Area, Mailing Address, Email, Business Email, Region, Phone, Mobile, OneView Portal User, Description, HHS ID, Organizational Path, AlertHHS Organization, SCMS Agency Abbreviation, SCMS SubAgency Abbreviation)

Related Files (Legal Documentation)

Related Project Overview Information (Owner Name, Project Status, Project Number, Project Phase, Project Name, Level, Description, Assistant Secretary for Administration (ASA) Reportable Project Status, Parent Project, Schedule Automated Status Report, Project/Program Manager, Portfolio, Service Area Point of Contact (POC), Service Area, Strategic Improvement, Cost Center)

Related Project Health Information (% Complete, Overall Project Health Icon, % Schedule Complete, Overall Project Health, Automate Overall Project Health Status)

Related Project Dates Information (Planned Start Date, Planned End Date, Actual Start Date, Actual End Date)

Related Project Quantitative Detail Information (Total Planned Cost, Planned Labor Cost, Planned Travel Cost, Planned Software Cost, Planned Hardware Cost, Planned Agreements, Planned Fees, Total Actual Cost, Actual Labor Cost, Actual Travel Cost, Actual Software Cost, Actual Hardware Cost, Actual Agreements, Actual Fees)

Related Project Scorecard Files

Related Weekly Status Updates (Weekly Status Update Name, Text Preview, Project)

Related Task Information (Project Task Name, Major Task Status, Description, Status, Related Project, Start/End Date, Assigned to Contact, Related Milestone)

Related Project Milestone Information (Milestone Name, Status, Description, Start/End Date, Related Project)

Related Project Risk/Issue (Risk/Issue Name, Status, Mitigation Strategy, Date Logged, Resolution Date)

Related Case Information (Case Owner, Case Number, Initial Response Date/Time, Priority, Support Ticket Type, Status, Primary Module Impacted, Contact Name, Web Email, Phone, Case Origin, Subject, Description, Portfolio, Service Area, Type of Service Request, Other Type, Type of Change, Other Type of Change, Existing Uniform Resource Locator (URL), New URL, 508 Compliant Status, Case Origin)

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 following types of information are collected to track a Contact's Application Status, Submit new Applications, & Maintain Individual Contact Information: Unique Identifiers (User ID, New Hire ID, Social Security Number, Alien Registration Number, Passport Number, Visa Number) Application Information (Application ID, Agency, Sub-Agency, Division, Region, Government Sponsor Name, Government Sponsor Email, Project Officer Name, Project Officer Email) Employment Information (Supervisor Name, Pay Plan, Series, Grade, Division, Country of Issuance, Effective Date of Appointment, Customer Name, Agency Address, Agency City, Agency State, Agency Post code, Payroll Office Contact, Payroll Office Phone Number, e-Verify Case Number, Supervisor Email, Duty Location City, Duty Location State, Duty Location Code) Applicant Information (Applicant, Applicant Type, Applicant Position, Applicant First Name, Applicant Middle Name, Applicant Last Name, Applicant Suffix, Applicant Preferred Name, Applicant Email, Applicant Phone, Applicant Extension, Service Type, Request Type, position automated designated tool (PDAT) Form Completed Status, HHS ID, Applicant ID, External Application ID, Current Zip Code for Badge Location, Personal Card Issuer Facility (PCIF), Date of Birth, Place of Birth City, Place of Birth State, Country of Citizenship) Contract Information (Company Name, Company Street, Company City, Company Country, Company Phone, Company Street 2, Company Zip Code, Company State, Contract Number, Contract Start Date, Contract End Date, Badge Expiration Date, Agency's Obligating Document #) Security Processing Information (Federal Emergency Responder, Require Unified Financial Management System (UFMS) Access, Required IT

Admin, HHS Simple Mail Transfer Protocol (SMTP) Email Address, User Principal Name (UPN) Email Address, Security Processing Notes)

Status Information (Current Phase, Current Onboarding Step, External System Status, Application Status, Gateway Display Status, Gateway Display Status Last Updated, Rejected Reason, Created By Contact, Last Modified Contact/ Date/Time, Application Owner)

Gateway Step Information (Gateway Step Name, Parent Step, Supervisor Onboarding Step, Gateway Display Status, Phase, Step Description, Service Type, Step Hover Text, Step Order, Form Type, Active Status, Form Action, Display As, Form Component, Mark Step Completed Status, Form Component, Mark Step Completed Status, Do Not Send Form Status, Create History Record for Step Status)

Gateway related Reports & Dashboards

Customer Information (Customer Name, Account Record Type, Parent Account, Customer Owner, Agency, Billing Address, Shipping Address, Phone, Phone Extension, Website, Gateway Customer Type, Gateway Abbreviation, SCMS Agency ID, Requesting Organization, Description)

Contact Information (Name, Contact Owner, Title, Contact Record Type, Customer Name, Type, Status, Suffix, Agency, Service Area, Mailing Address, Email, Business Email, Region, Phone, Mobile, OneView Portal User, Description, HHS ID, Organizational Path, AlertHHS Organization, SCMS Agency Abbreviation, SCMS SubAgency Abbreviation)

Related Files (Legal Documentation)

Related Project Overview Information (Owner Name, Project Status, Project Number, Project Phase, Project Name, Level, Description, Assistant Secretary for Administration (ASA) Reportable Project Status, Parent Project, Schedule Automated Status Report, Project/Program Manager, Portfolio, Service Area Point of Contact (POC), Service Area, Strategic Improvement, Cost Center)

Related Project Health Information (% Complete, Overall Project Health Icon, % Schedule Complete, Overall Project Health, Automate Overall Project Health Status)

Related Project Dates Information (Planned Start Date, Planned End Date, Actual Start Date, Actual End Date)

Related Project Quantitative Detail Information (Total Planned Cost, Planned Labor Cost, Planned Travel Cost, Planned Software Cost, Planned Hardware Cost, Planned Agreements, Planned

		Fees, Total Actual Cost, Actual Labor Cost, Actual Travel Cost, Actual Software Cost, Actual Hardware Cost, Actual Agreements, Actual Fees) Related Project Scorecard Files Related Weekly Status Updates (Weekly Status Update Name, Text Preview, Project) Related Task Information (Project Task Name, Major Task Status, Description, Status, Related Project, Start/End Date, Assigned to Contact, Related Milestone) Related Project Milestone Information (Milestone Name, Status, Description, Start/End Date, Related Project) Related Project Risk/Issue (Risk/Issue Name, Status, Mitigation Strategy, Date Logged, Resolution Date) Related Case Information (Case Owner, Case Number, Initial Response Date/Time, Priority, Support Ticket Type, Status, Primary Module Impacted, Contact Name, Web Email, Phone, Case Origin, Subject, Description, Portfolio, Service Area, Type of Service Request, Other Type, Type of Change, Other Type of Change, Existing Uniform Resource Locator (URL), New URL, 508 Compliant Status, Case Origin)
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://pscpm.my.site.com/gateway/s/login/ (for applicants applying for their badge) https://pscpm.lightning.force.com/lightning/page/home
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No

PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	Gateway is a transparent and efficient workplace readiness module that allows applicants and users to track the progress of the intake, suitability, and badging process The Salesforce Government Cloud is a dedicated portion of Salesforce’s Platform as a Service (PaaS) and Software as a Service (SaaS) multi-tenant public cloud infrastructure, specifically isolated for use by U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded research and development centers (FFRDCs). All personnel have their status categorized with a sensitivity level in accordance with control PS-2 Personnel Categorization. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. All internal users access the system using pscpm.my.salesforce.com and Single Sign-On via AMS. External users consist of Experience Cloud users leveraging a type of micro-site for a specific use case. These users include PSC employees and contractors.
PTA 10:	Does the website have a posted privacy notice?	No
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	No
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	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 Social Security Number Employee ID Number Biographical Information Name Date of Birth Legal Documents Contact Information Email Address (Personal) 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, New Hire ID, Social Security Number, Alien Registration Number, Passport Number, Visa Number) Application Information (Application ID, Agency, Sub-Agency, Division, Region, Government Sponsor Name, Government Sponsor Email, Project Officer Name, Project Officer Email) Employment Information (Supervisor Name, Pay Plan, Series, Grade, Division, Country of Issuance, Effective Date of Appointment, Customer Name, Agency Address, Agency City, Agency State, Agency Post code, Payroll Office Contact, Payroll Office Phone Number, e-Verify Case Number, Supervisor Email, Duty Location City, Duty Location State, Duty Location Code) Applicant Information (Applicant, Applicant Type, Applicant Position, Applicant First Name, Applicant Middle Name, Applicant Last Name, Applicant Suffix, Applicant Preferred Name, Applicant Email, Applicant Phone, Applicant Extension, Service Type, Request Type, position automated designated tool (PDAT) Form Completed Status, HHS ID, Applicant ID, External Application ID, Current Zip Code for Badge Location, Personal Card Issuer Facility (PCIF), Date of Birth, Place of Birth City, Place of Birth State, Country of Citizenship) Contract Information (Company Name, Company Street, Company City, Company Country, Company Phone, Company Street 2, Company Zip Code, Company State, Contract Number, Contract Start Date, Contract End Date, Badge Expiration Date, Agency's Obligating Document #) Security Processing Information (Federal Emergency Responder, Require Unified Financial Management System (UFMS) Access, Required IT Admin, HHS Simple Mail Transfer Protocol (SMTP) Email Address, User Principal Name (UPN) Email Address, Security Processing Notes) Status Information (Current Phase, Current Onboarding Step, External System Status, Application Status, Gateway Display Status, Gateway Display Status Last Updated, Rejected Reason, Created By Contact, Last Modified Contact/ Date/Time, Application Owner) Gateway Step Information (Gateway Step Name, Parent Step, Supervisor Onboarding Step, Gateway Display Status, Phase, Step Description, Service Type, Step Hover Text, Step Order, Form Type, Active Status, Form Action, Display As, Form Component, Mark Step Completed Status, Form Component, Mark Step Completed Status, Do Not Send Form Status, Create History Record for Step Status) Gateway related Reports & Dashboards Customer Information (Customer Name, Account

Record Type, Parent Account, Customer Owner, Agency, Billing Address, Shipping Address, Phone, Phone Extension, Website, Gateway Customer Type, Gateway Abbreviation, SCMS Agency ID, Requesting Organization, Description)

Contact Information (Name, Contact Owner, Title, Contact Record Type, Customer Name, Type, Status, Suffix, Agency, Service Area, Mailing Address, Email, Business Email, Region, Phone, Mobile, OneView Portal User, Description, HHS ID, Organizational Path, AlertHHS Organization, SCMS Agency Abbreviation, SCMS SubAgency Abbreviation)

Related Files (Legal Documentation)

Related Project Overview Information (Owner Name, Project Status, Project Number, Project Phase, Project Name, Level, Description, Assistant Secretary for Administration (ASA) Reportable Project Status, Parent Project, Schedule Automated Status Report, Project/Program Manager, Portfolio, Service Area Point of Contact (POC), Service Area, Strategic Improvement, Cost Center)

Related Project Health Information (% Complete, Overall Project Health Icon, % Schedule Complete, Overall Project Health, Automate Overall Project Health Status)

Related Project Dates Information (Planned Start Date, Planned End Date, Actual Start Date, Actual End Date)

Related Project Quantitative Detail Information (Total Planned Cost, Planned Labor Cost, Planned Travel Cost, Planned Software Cost, Planned Hardware Cost, Planned Agreements, Planned Fees, Total Actual Cost, Actual Labor Cost, Actual Travel Cost, Actual Software Cost, Actual Hardware Cost, Actual Agreements, Actual Fees)

Related Project Scorecard Files

Related Weekly Status Updates (Weekly Status Update Name, Text Preview, Project)

Related Task Information (Project Task Name, Major Task Status, Description, Status, Related Project, Start/End Date, Assigned to Contact, Related Milestone)

Related Project Milestone Information (Milestone Name, Status, Description, Start/End Date, Related Project)

Related Project Risk/Issue (Risk/Issue Name, Status, Mitigation Strategy, Date Logged, Resolution Date)

Related Case Information (Case Owner, Case Number, Initial Response Date/Time, Priority,

		Support Ticket Type, Status, Primary Module Impacted, Contact Name, Web Email, Phone, Case Origin, Subject, Description, Portfolio, Service Area, Type of Service Request, Other Type, Type of Change, Other Type of Change, Existing Uniform Resource Locator (URL), New URL, 508 Compliant Status, Case Origin)
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?	Personally Identifiable Information (PII) is utilized by a module built within OneView called 'Gateway.' Gateway is a transparent and efficient tool used to track the progress of the intake, suitability, and badging process for workplace readiness. Gateway depends upon an integration with SCMS (Smart Card Management System) for the latest Contact data with a related address, HHS ID, and onboarding status. Gateway was initially built to onboard new Contractor applicants, and now supports new and existing Contractor applicants and Inter Op/DIV transfers. The OneView Gateway solution is intended to provide a simplified user experience that supports tracking of overall onboarding status and subtasks for both Applicants and their respective Managers. The initial application creation and forms submission and review process begin in Gateway, but once submitted to SCMS (Smart Card Management System), other milestones and activities are managed and transmitted back to Gateway for tracking. Upon creation of a new Gateway Application, the hiring manager will populate the required fields for Agency Information, Applicant Information, & Security Information sections. An application number is then assigned to the contractor/applicant and the system initiates a process that sends log-in information to the user used to complete the required pre-screening steps and track the progress of their application. The applicant is then required to upload copies of their Resume, their signed OF-306 Form, and their signed Rules of Behavior Form. After submitting all prescreening forms, the hiring manager is notified that the forms have been submitted and ready for review. User Personally Identifiable Information (PII) within the OneView Gateway Application is used by the system to identify individuals, create an identity known as HHS ID (Health and Human Services Identity), and perform badging and investigation services. Once a Gateway Application is created, an HHS ID is created and becomes the sole identifier for a person of record.
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 of PII.

PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	The Social Security Number (SSN) is needed to identify records unique to the individual. Although disclosure of the SSN is not mandatory, failure to disclose the SSN may prevent or delay the processing of the background investigation. The authority for soliciting and verifying the SSN is Executive Order 9397, as amended by EO 13478.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	The authority to collect SSN is implied in the statutes and E.O.s governing background investigations (see, e.g., E.O. 10450 at Sec. 9, requiring an index and adequate identifying information). E.O. 9397, as amended by E.O. 13478, allows SSN to be used as the enumerator when an enumerator is required or permitted by a program-specific law
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.	Case Numbers or HHS e-mails.
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] 09-90-0001 Telephone Directory/Locator System SORN history: 47 FR 45514 (10/13/82); updated 59 FR 55845 (11/9/94), *83 FR 6591 (2/14/18)
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.	N/A- 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) 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 for Gateway Onboarding Applications. Most other users associate to the Program Support Center Account. Active Contract data will be visible in OneView for Gateway and only includes Contract Number, Vendor, Vendor Contact information, Contract Start Date and Contract End Date. 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 OneView 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 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 (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.	Before a contractor/federal employee is approved, the applicant submits PII through federal government systems such as e-Qip. Once submitted, the applicant's PII is then recorded by the individual's government sponsor and ultimately stored in OneView. The applicant is then granted access to "Gateway" where they are able to enter any additional information, confirm the information stored is correct, and monitor their application's progress to approval/denial. When the user submits additional information and confirms the PII currently stored, the user will be presented with a pop-up window that asks the user to confirm/or not confirm their submission. 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. Users 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 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. HHS restrictions, Rules of Behavior, Role Based Access Controls for Privileged users are in place with monitoring/logging and review processes to determine need to use, least privilege access for PII.

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.	The technical access is by default FIPS 140-2 compliant. Ensuring that data in transit and data at rest is encrypted. Only authorized system administrators/contractors with level 6 clearance have the ability to configure and make any changes within the application. The system has been designed to allow only the least system privileges necessary to perform specific system functions. HHS restrictions, Rules of Behavior, Role Based Access Controls for users are also in place with monitoring/logging and review processes to determine need to use, least privilege access for PII. Gateway 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. Only authorized system administrators/contractors with level 6 clearance have access to PII within the System (Gateway 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.	Each employee 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 Gateway module which inherits its administrative, technical and physical controls from OneView. OneView system has been designed to allow only the least system privileges necessary to perform specific system functions. Role Based Access Controls are used to secure and protect PII data within the system. Only authorized system administrators and developers with LEVEL 6/T4 Public Trust can access PII, make any changes, or update certain configuration properties for the PSC OneView application. No other user has this ability. All users are granted specific roles and privileges with specific access rights for their roles within the individual modules with a need to know basis Since the data is stored in a FedRAMP approved environment the Cloud Service Provider ensures physical controls are in place. all Administrative, Technical, and Physical controls are listed and detailed within the control catalogue of the HHS Office of the Chief Information Officer (OCIO) Sponsored FedRAMP Authorization to Operate (ATO) package and maintained at the Federal Information Security Modernization Act (FISMA) Moderate level.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	2/26/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	2

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	2/26/2026
SOP Review Comments:	Hello, Please review my comments and make the appropriate changes within your responses. Thank you, Muriel.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	3/2/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 3/2/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	4

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	3/6/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	4

SAOP Signature

Date	User	Type	Name	Original Value	New Value
3/6/2026 1:35 PM	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
PTA 04	Data Feed Service, pta_pia_OS_Release	2/17/2026	Please define the acronym Op/DIV, NDA, and PIV on first use.	
PTA 05	Data Feed Service, pta_pia_OS_Release	2/17/2026	Please define the acronym Org, UFMS, SMTP, UPN, ASA, URL, and POC on first use.	
PIA 22	Data Feed Service, pta_pia_OS_Release	2/17/2026	Please select Other for any other PII elements not included in the list. Ensure that your response to the question is consistent with your responses to PTA 05, PTA 05A, PTA 05B, PTA 05C, and PTA 06.	
PTA 04	Data Feed Service, pta_pia_OS_Release	2/24/2026	Defined Op/DIV, NDA, and PIV .	
PTA 05	Data Feed Service, pta_pia_OS_Release	2/24/2026	Defined Org, UFMS, SMTP, UPN, ASA, URL, and POC .	
PIA 22A	Data Feed Service, pta_pia_OS_Release	2/24/2026	Included all PII not listed in PIA 22	
PIA 22	Data Feed Service, pta_pia_OS_Release	2/24/2026	Selected "Other" and included all PII in PIA 22 A to align with responses to PTA 05, PTA 05A, PTA 05B, PTA 05C, and PTA 06.	