Privacy Impact Assessment (PIA): OS - IAM@HHS - QTR1 - 2024 - OS1918799

Created Date: 6/17/2025 1:10 PM Last Updated: 6/25/2025 7:10 AM

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

1) Answer questions. Select the appropriate answer to each question. Question specific help text may be available via the icon. If your answer dictates an explanation, a required text box will become available for you to add further information.

2) Add Comments. You may add question specific comments or attach supporting evidence for your answers by clicking on the icon next to each question. Once you have saved the comment, the icon will change to the icon to show that a comment has been added.

3) Change the Status. You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.

4) Save/Exit the Questionnaire. You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms
ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	OS - IAM@HHS - QTR1 - 2024 - OS1918799	**PIA ID:**	3346972
Name of Component:	OS - OS - OS - Identity and Access Management System at HHS	**Name of ATO Boundary:**	Identity and Access Management System at HHS
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	470
Submission Status:	Submitted	**Submit Date:**	6/12/2025
Next Assessment Date:	N/A	**Expiration Date:**	6/24/2028
Office:		**OPDIV:**	OS
Security Categorization:		**OpDiv PIA ID:**	OS1918799
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	5/20/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Contractor

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	Internal Flow or Collection
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	This PTA/PIA incorporates the five the Identity and Access Management System at HHS (IAM@HHS) solution consisting of five (5) functional components including: Smart Card Management System (SCMS); Access Management System (AMS); Quantum Secure SAFE; Online Certificate Status Protocol (OCSP); and HHS Directory Services. Collectively, these functional components provide a variety of services to include centralized Personal Identity Verification (PIV) enrollment services, through the SCMS, local card production facility support, card activation, finalization and issuance. The Identity Access Management System at HHS (IAM@HHS) provides logical access to the Department of Health and Human Services (HHS) Enterprise applications through the Access Management System(AMS) and physical access to those HHS facilities that have their Physical Access Control Systems (PACS) integrated with the Quantum/SAFE solution. The HHS Directory Services consists of Enterprise Virtual Directory (EVD), Border Directory (BD) and Active Directory Federation Services (ADFS) which provide additional functional services as part of the

		IAM@HHS solution. Specifically, the EVD provides a single integration point for accessing consolidated and persistent views of HHS identity data. BD serves as a data aggregator for HHS Operating Divisions (OpDivs). This allows each OpDiv to retrieve Global Address List (GAL) information for users from different OpDivs. BD also contains the encryption public key certificate of users through the implementation of AMS-BD integration. The External User Management (XMS) service allows for external users, who hold a PIV or Common Access Card (CAC) badge issued by another federal agency/department, to be granted physical and/or logical access to HHS systems and buildings. The Online Certificate Status Protocol (OCSP) solution is utilized to validate HHS and other Federal agency certificates (e.g., Department of Defense (DoD), General Services Administration (GSA) etc.) used for application and domain authentication across HHS. Changes to the system since the prior PTA/PIA include: NextGenID solution is designed to support expansion of badging services by utilizing commercially available NextGenID PIV enrollment stations to conduct remote PIV enrollment appointments of applicants through a supervised remote identity proofing solution; Smart Card Management System – Access Card Utility (ACU) application update allows remote employees/users to issue themselves a security key token credential (YubiKey) utilized within the internal HHS network; Food and Drug Administration (FDA) eArrive System is an enhancement of FDA's Homeland Security Presidential Directive (HSPD-12) processes through the transition of the existing manual induction process to inducting records via a web service from FDA's Human Resource (HR) system. Integration of the existing FDA eArrive onboarding system with the HHS Smart Card Management System (SCMS) will allow for a streamlined onboarding process. ID.me and Sterling. ID.me is a new virtual connection that will capture an applicant's identity information, Sterling will capture the applicant's fingerprints via Electronic Fingerprint Transmission (EFT), photograph, and document data and transmit it back to the HHS SCMS for processing for Defense Counterintelligence and Security Agency (DCSA) investigation.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	Access Management System (AMS) provides various benefits that enhance the user's experience by reducing the number of usernames and passwords users need to memorize, supporting multiple authentication methods (e.g. password, PIV card, Fast Identity Online (FIDO)), limiting exchange/proliferation of user credentials, and enabling a consistent program-wide authentication service. HHS Directory Services consists of the Enterprise Virtual Directory (EVD), Border Directory (BD) and Active Directory Federation Services (ADFS) which provide additional functional services as part of the IAM@HHS solution. Specifically, the EVD provides a single integration point for accessing consolidated and persistent views of HHS identity data. BD serves as a data aggregator for HHS Operating Divisions (OpDivs). This allows each OpDiv to retrieve Global Address List (GAL) information for users from different OpDivs. BD also contains the encryption public key certificate of users through the implementation of AMS-BD integration. The Online Certificate Status Protocol (OCSP**)** solution is utilized to validate HHS and other Federal agency certificates (e.g. Department of Defense (DoD), General Services Administration (GSA) etc.) used for application and domain authentication across HHS. Physical access is handled by those HHS facilities that have their Physical Access Control Systems (PACS) integrated with the SAFE solution. Finally, Smart Card Management System (SCMS) provides centralized Personal Identity Verification (PIV) enrollment services; local card production facility support and; PIV card activation, finalization, and issuance.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The AMS provides logical access to various enterprise applications in a single sign-on environment, enables federation, and manages permissions for protected resources and applications. It also acts as a centralized authentication source for HHS. To facilitate these accesses, the following information is collected, stored or shared for all users (employees, contractors, affiliates, external federal users): last name and first name shared; AMS username; AMS password; permanent HHSID; permanent email address; permanent other application-specific username (e.g. for mapping from AMS to Learning Management System) ; application roles - shared; user type (contractor, employee, affiliate, or external); Operational Division (OpDiv); OpDiv Affiliation; SCMS Status; AMS Status; certificates; network credentials. HHS Directory Services collects, stores or shares for HHS users (employees, contractors, affiliates): Last name and first name shared; permanent HHSID;

email address; Operational Division (OpDiv); OpDiv Affiliation; SCMS Status.

With OCSP**,** HSPD-12 card certificate information from all users (employees, contractors, affiliates, external federal users) trying to authenticate to HHS networks and systems is collected and shared to determine the validity of a user's digital or identity certificate and to quickly provide revocation information to HHS and non-HHS federal inquiry systems. The following data is collected and shared throughout the Department as well as external federal agencies: information about the digital key, the identity of the subject/ owner (name, email address, DoB, email and certificate), and the digital identity of the entity of the issuer.

SAFE collects and shares identifiable information for federal job applicants (direct contractors as well as federal employees internal and external to the HHS) with the Office of Personnel Management to facilitate investigative background checks. The SAFE application performs the synchronization and near real-time updates of identities from the SCMS, including updates of personal or credential information, handling expired or revoked PIV certificates, and the provisioning of new PIV holders. It also enables security managers to create processes and policies to grant, manage, revoke, and provision physical security identities and access privileges. The following elements are collected, maintained/stored, or shared: building; Signature certificate; certification status; cardholder unique identifier; email; Federal agency smart credential numbers associated with; organization category; name; gender; hair and eye color; height; Staffing Divisions (StaffDivs); phone; PIV Card Validity indicators (for certificates and signatures); Quantum/Secure logs (i.e., creation and modified dates) type of issuance; activation dates; serial numbers; card information (i.e. number, status, type, certificate status, deactivation dates); contract company name; employee number; user credential identifier and PIN.

Finally, SCMS is the “identity store,” a resource that establishes an identity record for everyone. The records maintained are HHS employees’, contractors’, and affiliates’ official identity information, including required biographic and biometric data, sponsorship and employer data, and adjudication results of background investigations. The SCMS collects data elements from the PIV card applicant, including name, date of birth, Social Security Number, organizational and employee affiliations, fingerprints, digital color photographs, work e-mail addresses, and phone numbers, as well additional verification and demographic information (like the results of background investigations).

PTA - 5A:	Are user credentials used to access the system?

PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password CAC Card
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	The AMS provides logical access to various enterprise applications in a single sign-on environment, enables federation, and manages permissions for protected resources and applications. It also acts as a centralized authentication source for HHS. To facilitate these accesses, the following information is collected, stored or shared for all users (employees, contractors, affiliates, external federal users): last name and first name shared; AMS username; AMS password; permanent HHSID; permanent email address; permanent other application-specific username (e.g. for mapping from AMS to Learning Management System) ; application roles - shared; user type (contractor, employee, affiliate, or external); Operational Division (OpDiv); OpDiv Affiliation; SCMS Status; AMS Status; certificates; network credentials. HHS Directory Services synchronizes processes with AMS and the Office of Information Technology Infrastructure and Operations (ITIO) Microsoft Identity Manager and S3processes, and the Enterprise Virtual Directory (EVD) which provides a single integration point for accessing the resulting consolidated and persistent views for employees, contractors, and affiliates for the Department. The following information is collected, stored or shared for HHS users (employees, contractors, affiliates): Last name and first name shared; permanent HHSID; email address; Operational Division (OpDiv); OpDiv Affiliation; SCMS Status. With OCSP**,** HSPD-12 card certificate information from all users (employees, contractors, affiliates, external federal users) trying to authenticate to HHS networks and systems is collected and shared to determine the validity of a user's digital or identity certificate and to quickly provide revocation information to HHS and non-HHS federal inquiry systems. The following data is collected and shared throughout the Department as well as external federal agencies: information about the digital key, the identity of the subject/ owner (name, email address, DoB, email and certificate), and the digital identity of the entity of the issuer. SAFE performs the synchronization and near real-time updates of identities from the SCMS, including updates of personal or credential information, handling expired or revoked PIV certificates, and the provisioning of new PIV holders. SAFE enables security managers to create

		processes and policies to grant, manage, revoke, and provision physical security identities and access privilege. It collects and shares identifiable information for federal job applicants (direct contractors as well as federal employees internal and external to the HHS) with the Office of Personnel Management to facilitate investigative background checks. The information falls into two over-arching categories: (1) documents that establish both identity and employment authorization or (2) documents that establish identity coupled with documents that establish employment authorization. The SAFE application performs the synchronization and near real-time updates of identities from the SCMS, including updates of personal or credential information, handling expired or revoked PIV certificates, and the provisioning of new PIV holders. It also enables security managers to create processes and policies to grant, manage, revoke, and provision physical security identities and access privileges. The following elements are collected, maintained/stored, or shared: building; Signature certificate; certification status; cardholder unique identifier; email; Federal agency smart credential numbers associated with; organization category; name; gender; hair and eye color; height; Staffing Divisions (StaffDivs); phone; PIV Card Validity indicators (for certificates and signatures); Quantum/Secure logs (i.e., creation and modified dates) type of issuance; activation dates; serial numbers; card information (i.e. number, status, type, certificate status, deactivation dates); contract company name; employee number; user credential identifier and PIN.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	Yes

PTA - 9:	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.	https://portal.scms.hhs.gov Accessible for all HHS users, with valid credentials, on HHS network or HHS VPN. This is the main SCMS portal site that has numerous capabilities such as, Sponsor and Adjudicating, but the user's ability to perform different functionality is entirely based upon what role permissions the user has been assigned. https://external.scms.hhs.gov/IdentityGuardSelfService This is a publicly accessible landing page for the IDG self-service portal used for enrolling to get a derived credential for a mobile device. Authorized users will be able to log in and self-issue themselves a credential. This is limited to only the following OpDiv credential holders: Administration for Children and Families (ACF), Agency for Healthcare Research and Quality (AHRQ), Administration for Strategic Preparedness and Response (ASPR), Centers for Medicare & Medicaid Services (CMS), Health Resources and Services Administration (HRSA), National Institutes of Health (NIH), Office of the Secretary (OS), Program Support Center (PSC). https://external.scms.hhs.gov/scheduler This is the root path for the scheduler application. This site does not provide any information, but is used in combination with a URL that is sent to applicants via e-mail to schedule a badging appointment. The URL contains a UUID that expires after 3 days and then is no longer accessible. Only individuals with that URL have access. Scheduler is currently limited to applicants in the following OpDivs: CMS, Centers for Disease Control (CDC), PSC, and ACF. https://ams.hhs.gov/ The department's enterprise Access Management System (AMS), which is FISMA High system and HVA, is used for authentication to access enterprise HHS applications that leverage AMS for Simplified Sign-On (SSO). AMS can be access by all HHS employees, contractors, and organizational affiliates. AMS is publicly accessible through users' web browser (both desktop and mobile web browsers). AMS' authentication methods include: HSPD-12 Access Card/PIV Card/CAC card, Fast Identity Online (FIDO) Credentials, NIH Credentials (via NIH Login), AMS Credentials, PIV-Derived Credentials (mobile only), One-Time Passwords (OTP), and Time-Based One-Time Passwords (TOTP).
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No

PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	Yes
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	The only one of the five IAM@HHS systems accessible on any mobile device is the AMS. Any user having an active AMS account can access the mobile version of AMS using their AMS credentials, Network Credentials (NIH only) FIDO Security Key, and PIV Derived. The purpose of the AMS mobile application is to facilitate to those applications having mobile capability within the AMS. Not all applications are mobile-device enabled and applications requiring Restricted Access, HHS Network cannot be accessed without being on the HHS Network.
PTA - 16:	Does the mobile application/ have a privacy notice?	Yes
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	No
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	No
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Name Email Address Phone numbers Certificates Date of Birth Photographic Identifiers Biometric Identifiers Employment Status User Credentials Other - Free text Field - HHSID, OpDiv/StaffDiv, sponsorship data, gender, eye and hair color, nation/state of birth, facial photographs, biometrics
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	Personal Identity Verification (PIV) enrollment services and applicant information gathering. Allowing logical access to the Department of Health and Human Services (HHS) Enterprise applications through the Access Management System (AMS) and physical access to HHS facilities. HHS uses the PII to authenticate and manage permissions for resources and applications protected by the AMS. The email address is also used for system-generated communications to users for AMS-related functions such as application role assignments and AMS password resets.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The information will not be used for any secondary purposes.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	A general function for using Social Security Numbers (SSNs) to access the systems involves identity verification to secure access control. The process is protected and tested to assure privacy and security. As part of the onboarding of federal employees, contractors, or individuals requiring system access, the agency collects SSNs as part of personal identification.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Privacy Act of 1974 (5 U.S.C. § 552a), Social Security Act Amendments of 1972 (42 U.S.C. § 405(c)(2)(C)), Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Security Modernization Act of 2014 (FISMA), E-Government Act of 2002 (Public Law 107-347)

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301; Information Technology Management Reform Act of 1996 (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104- 347, sec. 203); Paperwork Reduction Act of 1995 (44 U.S.C. ch. 35); Government Paperwork Elimination Act (Pub. L. 105-277, sec. 1701, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Identifying information (name, address, telephone number(s), email address(es), date and place of birth, birthdate, Social Security Number, credential numbers, other identification numbers, etc.), fingerprint and facial biometrics.
PIA - 8B:	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.	Existing SORN: 09-90-0020 Suitability for Employment Records https://www.hhs.gov/foia/privacy/sorns/09900020/index.html , 58 FR 28880 (5/17/93); updated at 59 FR 55845 (11/9/94) and 83 FR 6591 (2/14/18). [Exempt based on (k)(5); see 40 FR 47406 (Final Rule) & 40 FR 41140 (NPRM)]. Yes, an updated SORN is in development.
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Other Government Sources Within the OPDIV Other Federal Entities
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	The system itself is a transactional authenticator, encryptor, and lifecycle manager for information collected on mandatory forms implemented by other agency collection approvals, for instance the Office of Personnel Management, the Office of the Director of National Intelligence, The Department of Homeland Security, and the Department of Treasury, and the Office of Management and Budget.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Personnel data is sent to Defense Counterintelligence and Security Agency (DCSA) for fingerprinting and background checks.

PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	IAM@HHS has ISAs with the following: Health Resources and Services Administration (HRSA) ICS, RAPTS, OIT Workiva WDesk, PRF Acumen Web Portal, Salesforce Provider Relief Funds (PRF), EHBs, NPDB IQRS & NPDB TCK, NHDP Cyfluent EHR, BMISS NextGen Apps, DCPaaS, HEDSAP Applications, and DocuSign. Food and Drug Administration (FDA) CDM Sailpoint IIQ, IBM MaaS360, SGRC (RSA Archer), and eArrive. Administration for Children and Famalies (ACF) AWS GSS, and Amazon Web Services (AWS) General Support System (GSS) Redhat SSO Portal. NIH Login - Federation, CIT IAM GSS, CDM Dashboard, CMS Acumen Web Portals (AWP), ACL CFMS, IHS CDM SailPoint IIQ, CMS SMG DCO Google ChatBot, Assistant Secretary for Financial Resources (ASFR) Grant Solutions, USAS NHI API IAM@ HHS has MOUs with the following: Program Support Center (PSC) Room Reservation System, Locator, MACCS, FOH FedHealth, OneView, Alert HHS, WorkSmarter, and Revenue Invoicing and Cost Estimation Systems (PRICES). Office of the Secretary (OS) EHCM, SGRC, Elastic Cloud Enterprise (ECE), PMS, ISM, ITAS. Office of Financial Systems Policy and Oversight (OFSPO)(CFRS, FBIS, UFMS), HighBond (OHB), ServiceNow. ASFR Grants.gov, and HHSOF ServiceNow. Assistant Secretary for Public Affairs (ASPA) WCMS/WCD Portal, and Strategic Engagement Platform (StEP). Office of the Assistant Secretary for Health (OASH) Commissioned Corps Payroll – Cloud System (CCP-C), Force, Smartsheet Gov, IDP, and TCHC. HCAS PRISM, OCIO OEAD/OAP BIIS-C, OMHA ECAPE, IOS Secretary Policy System (SPS), PACS PSEMS, OIS SGRC (RSA Archer), HHS Office 365 (O365@HHS), DCIO-Ops Microsoft Intune, ORI File Transfer System (ORI-FTS), IOS/ONS Security Manager, Program Information Management System (PIMS), USAS NHI API, HHS IOS HSDW, HHS Connect, HealthData.gov, and HHS Connect EDP, iComplaints (ETK EEO), ONC AWS Security Environment (ASE).
PIA - 11D:	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.	Disclosures are accounted for in accordance with 5 U.S.C. § 552a(c) and OMB Memorandum M-99-05, Attachment B, at 2.(d).
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Users are presented with the pop-up Government Warning banner when they are logging into the AMS at which time they are given an opportunity to opt-out of the collection or use of their data by disagreeing to consent to such activity.

PIA - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained.	In cases involving individuals or small groups of users, notifications of major changes will be delivered via individual e-mails. In cases involving a large amount of users a mass email will be sent via distribution lists informing users of what has occurred, and their options, if there are any resulting procedural or privacy changes. Incidents will also be reported to the HHS Secure One Help Desk and resolved in a timely fashion.
PIA - 15:	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.	Individuals should contact the HHS Computer Security Incident Response Center (CSIRC) or Computer Security Incident Response Team (CSIRT) if they believe their PII has been inappropriately obtained, is incomplete or inaccurate, or is being misused. Individuals are informed of the proper procedures to follow in these circumstances during security and privacy training, which they are required to complete annually.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	Users have the ability to review and update some of their PII on a regular basis, (e.g. name, email) while in AMS. Necessary changes are submitted to the database administrators for update. Additionally, weekly datafeeds from Health and Human Services (HHS) human resource databases update PII in AMS as needed. The AMS undergoes annual system audits during which the system's data integrity, availability, accuracy, and relevancy are examined, and is part of annual audits for other systems such as the Enterprise Human Resource and Payroll (EHRP) for the same purpose.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes

PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Records may be disclosed to student volunteers, employees with appropriate vetting and reason, individuals working under a personal services contract, and other individuals performing functions (including ancillary functions) relating to the purposes of this system of records for HHS. – HHS Badging Office users with approved roles, i.e. Sponsors, Adjudicators, within SCMS Portal are able to access PII in order to perform job duties. Deloitte SCMS helpdesk staff requires access to PII in order to provide user support. Administrators – System Administrators do not have access to PII. Developers – Only Deloitte SCMS Developers/Application Admins with elevated privileges can access PII for overall application upgrades, operations, and maintenance. Contractors – Only Deloitte contractors with elevated privileges can access PII, i.e. Developers/SCMS Helpdesk for the same reason as above.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrative procedures are defined by position risk and sensitivity designations based upon the role in the system is done by a properly vetted individual with account termination after 30 days of no activity. To have a role within the system, annual role-specific training must be taken, and the results available for audit.
PIA - 20:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.	Access to PII is on a need-know basis, and derived by job role and access privileges in both the applications and the application databases.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.	General Cybersecurity Awareness Training and Rules of Behavior in addition to specific roles based training in electronic modules to maintain access to the system components.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Internal system training is available via role-based training presentations posted on the Intranet and on-the-job training. Both review PII concepts and security procedures to ensure personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	Records are retained in accordance with General Records Schedule (GRS) 5.6 Item 010 (DAA-GRS-2017-00060001). Unless retained for specific ongoing security investigations, records of access are maintained for five years for maximum security facilities and then destroyed. Records are maintained for two years for other facilities and then destroyed. All other records relating to individuals are retained and disposed of in accordance with GRS 5.6 Item 181 (DAA-GRS-2017-0006-0001), specifically, upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	The database and individual OPDIV feeder servers are located within secured buildings. Different degrees of security have been implemented at all locations, with some including biometrics and closed circuit TV. Technical controls which minimize the possibility of unauthorized access, use, or dissemination of the data in the system are also in place. These include: user identification, firewalls, VPN, encryption, Intrusion Detection System and Personal Identity Verification (PIV) Cards. Guards, ID Badges and Key cards further ensure PII will be secure.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	6/12/2025
Privacy Analyst Comments:	Vanessa, This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	6/17/2025
		SOP Days Open:	5

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/23/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/23/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	6

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature Page.docx
SAOP Comments:		**SAOP Review Date:**	6/25/2025
		SAOP Days Open:	2

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmos_Release	5/16/2024	Here is a description of the Personal Identity and Authentication description: Name, date of birth, Social Security Number, work e-mail address, phone number, gender,	

			nation and/or state of birth, eye and hair color, height and weight, biometric data (including fingerprints), digital color photograph, ANSI facial image standards, data capture about elements such as glasses, facial obstructions, etc.
PIA - 2	Data Feed Service, piafrmos_Release	5/17/2024	Employees/ HHS Direct Contractors
PIA - 8	Data Feed Service, piafrmos_Release	5/17/2024	09-90-0777 Facility and Resource AC Records GSA/GOVT-7 PIV IDMS
PIA - 9	Data Feed Service, piafrmos_Release	5/17/2024	09-90-0020 Suitability for Employment Records, 58 FR 28880 (5/17/93); updated at 59 FR 55845 (11/9/94) and 83 FR 6591 (2/14/18).
PIA - 10	Data Feed Service, piafrmos_Release	5/17/2024	[Exempt based on (k)(5); see 40 FR 47406 (Final Rule) & 40 FR 41140 (NPRM)]
PIA - 11A	Data Feed Service, piafrmos_Release	5/17/2024	Information in these records may be used by the Office of Personnel Management, Merit Systems Protection Board, U.S. Office of Special Counsel, Equal Employment Opportunity Commission, and the Federal Labor Relations Authority (including the General Counsel of the Authority and the Federal Service Impasses Panel).
PIA - 11C	Data Feed Service, piafrmos_Release	5/17/2024	See attached ISA and MOU List
PIA - 1	Data Feed Service, piafrmos_Release	5/20/2024	I believe based on the comment provided and the other responses in the PTA/PIA, this response should be updated to include the following selections as well: social security number phone numbers date of birth user credentials photographic identifiers biometric identifiers employment status other: HHSID, OpDiv/StaffDiv, sponsorship data
PIA - 4	Data Feed Service, piafrmos_Release	5/20/2024	I would include the following in this response as well (please feel free to adjust the language to fit how you feel it should): Personal Identity Verification (PIV) enrollment services and applicant information gathering. Allowing

			logical access to the Department of Health and Human Services (HHS) Enterprise applications through the Access Management System(AMS) and physical access to HHS facilities.
PIA - 18	Data Feed Service, piafrmos_Release	5/20/2024	This response should detail for each type of individual selected (User, administrator, developers, contractors), the reasons why each selection made in PIA-17 requires access to the PII on the system.
PIA - 19	Data Feed Service, piafrmos_Release	5/20/2024	Please enumerate the procedures listed in the SORN, in the provided response field.
PIA - 23	Data Feed Service, piafrmos_Release	5/20/2024	GRS 18 has been superseded by newer records schedules. I believe, looking at the old schedule, everything that was previously covered under 18 is now under GRS 4.2 and GRS 5.6. Please take a look at the newer schedules and update the response with the appropriate newer GRS. If you are having issues identifying the correct schedule to list, please reach out to records management.
PIA - 11C	Data Feed Service, piafrmos_Release	5/20/2024	For this response we unfortunately need everything listed in the separate document, to be listed in the response box (as best as we can). I have edited it down to the following, please feel free to adjust and add in acronyms that I'm unfamiliar with: IAM@HHS has ISAs with the following: Health Resources and Services Administration (HRSA) ICS, RAPTS, OIT Workiva WDesk, PRF Acumen Web Portal, Salesforce Provider Relief Funds (PRF), EHBs, NPDB IQRS & NPDB TCK, NHDP Cyfluent EHR, BMISS NextGen Apps, DCPaaS, HEDSAP Applications, and DocuSign. Food and Drug Administration (FDA) CDM Sailpoint IIQ, IBM MaaS360, SGRC (RSA Archer), and eArrive. Administration for Children and Famalies (ACF) AWS GSS, and Amazon Web Services (AWS) General Support System (GSS) Redhat SSO Portal. NIH Login - Federation, CIT IAM GSS, CDM Dashboard, CMS Acumen Web Portals (AWP), ACL CFMS, IHS CDM SailPoint IIQ, CMS SMG DCO Google ChatBot, Assistant

			Secretary for Financial Resources (ASFR) Grant Solutions, USAS NHI API IAM@ HHS has MOUs with the following: Program Support Center (PSC) Room Reservation System, Locator, MACCS, FOH FedHealth, OneView, Alert HHS, WorkSmarter, and Revenue Invoicing and Cost Estimation Systems (PRICES). Office of the Secretary (OS) EHCM, SGRC, Elastic Cloud Enterprise (ECE), PMS, ISM, ITAS. Office of Financial Systems Policy and Oversight (OFSPO)(CFRS, FBIS, UFMS), HighBond (OHB), ServiceNow. ASFR Grants.gov, and HHSOF ServiceNow. Assistant Secretary for Public Affairs (ASPA) WCMS/WCD Portal, and Strategic Engagement Platform (StEP). Office of the Assistant Secretary for Health (OASH) Commissioned Corps Payroll – Cloud System (CCP-C), Force, Smartsheet Gov, IDP, and TCHC. HCAS PRISM, OCIO OEAD/OAP BIIS-C, OMHA ECAPE, IOS Secretary Policy System (SPS), PACS PSEMS, OIS SGRC (RSA Archer), HHS Office 365 (O365@HHS), DCIO-Ops Microsoft Intune, ORI File Transfer System (ORI-FTS), IOS/ONS Security Manager, Program Information Management System (PIMS), USAS NHI API, HHS IOS HSDW, HHS Connect, HealthData.gov, and HHS Connect EDP, iComplaints (ETK EEO), ONC AWS Security Environment (ASE).
PIA - 1	Data Feed Service, piafrmos_Release	10/2/2024	Please update the response so that it reads 'sponsorship data' rather than just 'sponsorship'.
PIA - 2	Data Feed Service, piafrmos_Release	10/2/2024	Please confirm in a comment that this response is comprehensive of all categories of individuals. In other questions in the PTA notes that the system collects information from: employees, contractors, affiliates, external federal users.
PIA - 4	Data Feed Service, piafrmos_Release	10/2/2024	Please re-include the information that was un-necessarily deleted from this response. The full response should read: Personal Identity Verification (PIV) enrollment services and applicant information gathering. Allowing logical access to the Department of Health and Human Services (HHS)

			Enterprise applications through the Access Management System (AMS) and physical access to HHS facilities. HHS uses the PII to authenticate and manage permissions for resources and applications protected by the AMS. The email address is also used for system-generated communications to users for AMS-related functions such as application role assignments and AMS password resets.
PIA - 11B	Data Feed Service, piafrmos_Release	10/2/2024	Please provide more specificity, e.g., disclosed to OPM to facilitate background checks. We cannot incorporate information from SORNs by reference because SORNs are not IT-system specific, but you can use language from SORNs to help craft responses.
PIA - 11D	Data Feed Service, piafrmos_Release	10/2/2024	Please review this response with Beth Kramer. This question relates to the agency's ability to provide a record of to whom it has disclosed records and pertinent details. While agencies do not need to account for disclosures made within the agency, the agency must account for all disclosures made outside of the agency, including disclosures pursuant to routine uses and law enforcement agencies (even though the law enforcement agency may be exempt from disclosures to the subject individual). We cannot incorporate information from SORNs by reference because SORNs are not IT-system specific, but you can use language from SORNs to help craft responses.
PIA - 15	Data Feed Service, piafrmos_Release	10/2/2024	They should contact their OpDiv Computer Security Incident Response Team (CSIRT) or CSIRC, not CISOs. Please update the response accordingly.
PIA - 19	Data Feed Service, piafrmos_Release	10/2/2024	This response has not been updated. Please review my previous comment and update the response accordingly.
PIA - 18	Data Feed Service, piafrmos_Release	10/2/2024	This response has not been updated. Please review my previous comment and update the response accordingly.
PIA - 23	Data Feed Service, piafrmos_Release	10/2/2024	This response has not been updated. Please review my previous comment

			and update the response accordingly.
PIA - 1	VILLAFUERTE, NESTOR	6/18/2025	Reviewer notes that PTA-5a & PTA-8 failed to sync.
PIA - 1	BLAND, CRYSTAL	6/23/2025	The Responses to PTA-5A and PTA-8 are: **PTA-5A:** 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. The system providing credentials is: Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is AMS. **PTA-8:** Does the system include a website or online application? • Yes

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	6/25/2025 7:10 AM	**History Log:**	View History Log