

General Information

PTA / PIA Name:	OS - HCAS - C - QTR1 - 2026 - OS3350600	PTA / PIA ID:	4375226
Component Name:	OS - HHS Consolidated Acquisition System - Cloud	ATO Boundary Name:	HHS Consolidated Acquisition System - Cloud
Overall Status:	Complete 	# of Days - Open:	44
Submitter:		Submit Date:	3/31/2026
Next Assessment Date:	04/09/2029	Expiration Date:	4/9/2029
Office:		OpDiv:	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	No	PIA Required:	Yes
General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.		Initiation
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)?		No
General 04:	ATO Date or Planned ATO Date.		4/20/2026
General 05:	Is the system or electronic information collection, agency or contractor operated?		Contractor
History Log:	View History Log		

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Mohammad Rahim
PTA 01A:	POC Title and Organization	Information System Security Officer (ISSO) U.S. Department of Health and Human Services (HHS) Office of the Secretary (OS) Office of the Chief Information Officer (OCIO)
PTA 01B:	POC Email Address	Mohammad.Rahim@hhs.gov
PTA 01C:	POC Phone Number	(202) 836-2674

PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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.

The HHS Consolidated Acquisition System - Cloud (HCAS - C) is a Department of Health and Human Services (HHS) integrated department-wide acquisition solution based on Procurement Information System for Management (PRISM). It is a Unison Software as a Service (SaaS) commercial off-the-shelf (COTS) product and is integrated with the Unified Financial Management System (UFMS) system across the HHS Operating Divisions. HCAS - C provides HHS Divisions with the tools needed to effectively support the acquisition management lifecycle, from initial planning and requisitioning, through award and closeout. HCAS - C streamlines the procurement process, performs routing, provides audit trails, financial tracking, and enhanced analytics reporting capabilities. It also includes contract management capabilities supporting award types prescribed by the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), and tracks and reports on HCAS - C procurement activity throughout the fiscal year. HCAS - C reports contract actions via the General Services Administration (GSA) Federal Procurement Data System - Next Generation (FPDS-NG).

The interface between HCAS - C and UFMS is bi-directional. HCAS - C receives generated requisitions (e.g., non-sensitive personally identifiable information [PII] award data) from UFMS to be validated and assigned to an award, to generate an obligation. HCAS - C transmits the obligation information (e.g., non-sensitive PII award data) back to UFMS for receipt and invoice processing. The web services interface transmits the acquisition transactions between the iProcurement module of UFMS and HCAS - C. It involves the movement of approved requisition transactions to HCAS - C and approved obligation transactions from HCAS - C to UFMS. Additionally, HCAS - C receives vendor data directly from the GSA System for Award Management (SAM), an official website of the U.S. Government commonly known as SAM.gov. The vendor data received from SAM includes first name, last name, vendor name, business email, mailing address, phone number, vendor point of contact (POC) email, representations and certifications, exclusion status, Taxpayer Identification Number (TIN), Employer Identification Number (EIN), and Unique Entity Identifier (UEI). This information is utilized for vendor validation and acquisition processing, and required for HCAS - C to award the requisition and create the obligation.

The legacy HCAS is migrating from the on-premises hosting environment at the National Institutes of Health Center for Information Technology (NIH-CIT) to the Unison Contracting SaaS (UCS) Federal Risk and Authorization Management Program (FedRAMP) environment, becoming HCAS - C. The host will change to Unison Software, Inc. (Unison).

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.	HCAS - C collects and maintains acquisition, vendor, and user information. Acquisition information consists of all data required for HCAS - C users to generate documents throughout the acquisition process. Document examples include Requisitions, Solicitations, Advanced Procurement Plans, and various award types. Acquisition information is input into the system utilizing two (2) methods: manual entry and system generation. Vendor information is collected from SAM, and consists of first name, last name, vendor name, business email, mailing address, phone number, vendor POC email, representations and certifications, exclusion status, TIN, EIN, and UEI. This information is retrieved via an application programming interface (API) between HCAS - C and SAM. HCAS - C does not typically receive or store full TINs, social security numbers (SSNs), or sensitive financial data. This information is managed by the financial systems. HCAS - C user information consists of user identification (ID), name, phone number, email, and HHS Personal Identity Verification (PIV) ID. All user information is input into HCAS - C by a system administrator. The HHS PIV ID is an agency issued employee identifier and is used for accessing multiple agency applications. The user ID is system specific and solely used within HCAS - C. All of the information outlined above once added, remains in the system indefinitely via the HCAS – C database managed by the direct contractor, Unison.
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.	Access to HCAS - C is controlled by the Identity and Access Management System at HHS (IAM@HHS), 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.	HCAS - C regularly utilizes the information specified in question PTA-5 in support of the day-to-day acquisition workflow, via the creation and processing of various procurement documents. All types of information collected and maintained by HCAS - C is utilized as part of this process. Examples of the types of information found within these procurement documents include vendor information that is received from SAM, such as first name, last name, vendor name, business email, mailing address, phone number, vendor POC email, representations and certifications, exclusion status, TIN, EIN, and UEI. User information is only utilized to authenticate users to the application, and for their profile setup and assignment of security permissions.

PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	Yes
PTA 21A:	What are the AI tools and how are they used?	HCAS - C utilizes the following artificial intelligence (AI) tools: PRISM Ally AI - An integrated AI assistant within the PRISM acquisition system that provides contextual guidance, drafting support, and policy interpretation to users. It operates within the system security boundary and assists users without altering data or approvals; and PRISM AI Clause Guidance - Is an integrated AI capability that assists contracting personnel in identifying and applying appropriate procurement clauses. It provides recommendations based on acquisition context, but contracting officers retain responsibility for final selection and compliance with FAR, HHS Acquisition Regulation (HHSAR), and agency policy. The AI tools are not trained using the PII collected in the system. The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks.

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 Taxpayer ID Number (TIN) Biographical Information Name Contact Information Email Address (Business) Mailing 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.	User ID, EIN, PIV ID
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?	The primary purpose of the personally identifiable information (PII) utilized within HHS Consolidated Acquisition System - Cloud (HCAS - C) is to authenticate users to the application, and profile permissions assignment. Users include federal division users and direct contractors (Unison). Users are authenticated to the system via the HHS Access Management System (AMS). An HCAS - C user identification (ID), HHS Personal Identity Verification (PIV) card (network user ID), name, and email are utilized to authenticate users and allow them to log into HCAS - C. The HCAS - C user ID correlates to the user's profile and their assigned role and permissions. The system does not disclose the use of PII, it is only utilized to authenticate users and assign them permissions. Users cannot access another user's PII.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	N/A
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.	Vendor records within HCAS - C encompass the Taxpayer Identification Number (TIN)/Employer Identification Number (EIN) which is pulled directly from the System for Award Management (SAM) to ensure that vendors are properly registered and authorized to receive government contract awards. For sole proprietors or other small business owners, the TIN/EIN may in fact be their personal Social Security number (SSN). The TINs/EINs collected are only for businesses. This is transmitted as part of the payload that is sent to the Unified Financial Management System (UFMS) during award processing (i.e., Indefinite Delivery/Indefinite Quantity [IDIQ], Blanket Purchase Agreement [BPA] Call, purchase order [PO], etc.).

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 collection of PII necessary for operating HCAS - C is permitted under the following legal authorities: Executive Order (E.O.) 13478: Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers, which states that it is the policy of the United States that Federal agencies should conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use; Title 31 United States Code (U.S.C.) 3512: Executive agency accounting and other financial management reports and plans, which describes government responsibilities to ensure effective control over, and accountability for, assets for which the agency is responsible; and Title 44 U.S.C. 3101: Records management by agency heads; general duties, which describes government responsibilities to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency, and designed to furnish the information necessary to protect the legal and financial rights of the government and of persons directly affected by the agency's activities.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Information use and disclosure specific to HCAS - C is permitted under the following legal authorities: Title 5 U.S.C. 301: Departmental regulations, which authorizes the Secretary of HHS to prescribe regulations for the government of his or her department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property; and Title 42 U.S.C. 3502: Assistant Secretary for Administration; appointment and duties, established the Assistant Secretary for Administration (ASA) at HHS who performs duties as prescribed by the Secretary, including oversight of the services necessary for maintaining the infrastructure of the agency.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Government Sources Other Federal Entities
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.	An Office of Management and Budget (OMB) information collection approval number is not required because HCAS - C does not collect information from the public.

PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
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.	The PII utilized within HCAS - C is not collected directly from individuals; therefore, no prior notice is given and consent cannot be obtained. The information is collected from SAM; individuals receive notification and provide consent during the SAM account creation process. HCAS - C user information consisting of non-sensitive PII elements (i.e., name, phone number, and email) is collected during the account creation process. This information is required for HCAS - C account creation. Individuals are aware of what PII is collected, and their information is supplied voluntarily. The use of PII is therefore consistent with their expectations.
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.	The PII utilized within HCAS - C is not collected directly from individuals; therefore, no notice is given and consent cannot be obtained when major changes occur to the system. The information is collected from SAM; individuals would be notified by the General Services Administration (GSA) of any major changes occurring within the system that may affect their PII. HCAS - C user information consisting of non-sensitive PII elements (i.e., name, phone number, and email) is collected during the account creation process. Any changes to a user's HCAS - C account must be requested by the user and approved by the designated Federal User Provisioning Official.
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.	The PII utilized within HCAS - C is not collected directly from individuals; therefore, no process exists to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, disclosed, or the PII is inaccurate. The information is collected from SAM; any concerns regarding an individual's PII would be addressed by GSA. HCAS - C user information consisting of non-sensitive PII elements (i.e., name, phone number, and email) is collected during the account creation process. Any concerns regarding a user's HCAS - C account are triaged by the HCAS - C Help Desk and any required changes are approved by the designated Federal User Provisioning Official.

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.	The PII utilized within HCAS - C is not collected directly from individuals; therefore, no process is in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of PII. The information is collected from SAM; periodic reviews of an individual's PII would be managed by GSA. HCAS - C user information consisting of non-sensitive PII elements (i.e., name, phone number, and email) is collected during the account creation process. At a minimum, HCAS - C user accounts are reviewed on a biannual basis to ensure the integrity, availability, accuracy and relevancy of the information.
PIA 38:	Identify who will have access to the PII in the system.	Users 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.	HHS Division Users - Federal staff require access to PII for the purpose of completing a variety of procurement tasks (i.e., award creation and award modification). HCAS - C Direct Contractor (Unison) - The direct contractor (Unison) as the system developer and maintainer, requires access to PII for the purpose of assisting federal staff with their day-to-day procurement operations.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII within HCAS - C is limited to authorized personnel only. Role-based restrictions permit access to information that is required for individuals to perform their job functions. The direct contractor (Unison) and federal staff assigned to the System Administrators security group can access each user's HCAS - C user ID. All contractors designated as system administrators are required to have this role to assist in maintaining the system and completing other duties as necessary. Prior to being granted access to the System Administrators security group, new system administrators must be approved by the System Owner and Business Owner.
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.	Access to PII is within HCAS - C is provided on a need-to-know basis and limited to authorized personnel only. Based on user group assignments, federal staff are granted read, write, and execute privileges to specific assigned data elements; the system limits access to PII based on their assigned role and responsibility. Multifactor authentication (MFA) and encryption provide additional technical controls. HCAS - C account access is monitored and logged.

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.	To ensure awareness of their responsibilities for protecting the information being collected and maintained, all system users (system owners, managers, operators, contractors and/or program managers) are required to complete the HHS Cybersecurity Awareness Training, and role-based training if applicable, prior to obtaining access to HCAS - C and annually thereafter. This training informs users of their security roles and responsibilities when utilizing the system. All mandatory security and privacy awareness training is managed and tracked at the HHS Division level.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to general security and privacy awareness training, system users (system owners, managers, operators, contractors and/or program managers) are required to read and acknowledge the HHS Rules of Behavior (RoB) for General Users prior to accessing HCAS - C and annually thereafter. Records management training and role-based training for system administrators are also required annually, in addition to refresher security and privacy awareness training courses. All relevant training is stored in the HHS Learning Management System (LMS) and the Cyber Security Learning Management System (CLMS). Training is managed and tracked at the HHS Division level.
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).	SAM is the data source for vendor PII. Therefore, the responsibility for PII retention and destruction would fall beneath the purview of GSA, who is responsible for SAM. HCAS - C user accounts are deactivated after sixty (60) days of inactivity. If the individual returns to use the application, it requires a new account request to be processed for reactivation. Accounts records are maintained indefinitely for historical auditing capabilities, and stored in compliance with the following National Archives and Records Administration (NARA) Records Schedule: Routine Administrative Records. Routine program records supporting leadership and/or general administration of all programs. Disposition Instruction: Temporary. Cutoff at the end of the calendar year. Destroy no sooner than 3 years after cutoff but longer retention is authorized. Disposition Authority: DAA-0440-2015-0002-0002
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.	Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, PII in HCAS - C is secured utilizing the following administrative, technical, and physical controls: Administrative Controls: Only authorized personnel have access to PII within HCAS - C; system administrators monitor user activity. Administrative controls provide privileged access to the System Administration security group, which allows them access to the HCAS - C user ID. New system administrators must be approved by the System Owner and Business Owner. Additional administrative controls include general security

and privacy awareness training, supplementary training as required, service-level agreements (SLAs), contractor agreements, and system documentation. Additional administrative safeguards are documented in the System Security and Privacy Plan (SSP). Administrative countermeasures utilized to protect and control access to PII are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and enforced utilizing the policies and procedures provided by HHS.

Technical Controls: HCAS - C implements PIV cards, virtual private network (VPN), and MFA to control access. The system is configured utilizing the concept of least privilege, enabling individuals to access elements of PII as necessary to accomplish assigned tasks in accordance with organizational mission and business functions. Additional technical controls include firewalls, Federal Information Processing Standards (FIPS) 140-2 for data protection (i.e., data at rest, data in use, and data in transit) regular offsite backups of data, and via audit records, logging changes made to system components. Further technical safeguards are documented in the SSP. Technical countermeasures utilized to protect and control access to PII are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and enforced utilizing the policies and procedures provided by HHS.

Physical Controls: HCAS - C is a commercial off-the-shelf (COTS) application, utilizing the Software as a Service (SaaS) cloud-based model. The system is located within the Federal Risk and Authorization Management Program (FedRAMP)-authorized cloud environment, Unison Contracting SaaS (UCS). The physical and environmental protection provided by UCS includes security guards at the data center where the system resides, twenty-four (24) hour video surveillance, personnel badges, restricted access to facilities, restricted access to documentation, emergency power equipment, heating, ventilation, and air conditioning (HVAC) systems, and fire suppression equipment. Additional physical safeguards are documented in the SSP. Physical security countermeasures utilized to protect and control access to PII and protect facilities from intrusion and environmental hazards are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and enforced utilizing the policies and procedures provided by HHS.

OpDiv Privacy Analyst Review			
Privacy Analyst Review Decision:	Approved	Privacy Analyst Review Date:	4/1/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	# of Days - PA Review:	1

SOP Review			
SOP Review Decision:	Approved	SOP Review Date:	4/1/2026
SOP Review Comments:		# of Days - SOP Review:	0

Agency Privacy Analyst Review			
Agency Privacy Analyst Review Decision:	Approved	Agency Privacy Analyst Review Date:	4/9/2026
Agency Privacy Analyst Review Comments:	Reviewer: Christopher Akhibi 4/9/2026 All comments addressed, this PIA is ready for SAOP review and approval. 3/30/2026 Please see comment and update accordingly. PTA 4: Please, spell out PII, first time use of the acronyms in the below sentence. The interface between HCAS - C and UFMS is bi-directional. HCAS - C receives generated requisitions (e.g., non-sensitive PII award data).... PTA 21A: Please, rephrase this statement: The AI tools are cannot trained using the PII collected in the system to "The AI tools are not trained using the PII collected in the system."	# of Days - APA Review:	8

SAOP Review					
SAOP Review Decision:		Approved		SAOP Review Date:	4/10/2026
SAOP Review Comments:				# of Days - SAOP Review:	1
SAOP Signature					
Date	User	Type	Name	Original Value	New Value
4/10/2026 1:53 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	3/11/2026	Additionally, HCAS - C receives vendor data (supplier, user, and ship-to office locations) directly from the GSA System for Award Management (SAM), an official website of the U.S. Please consider clarifying what vendor data is.	
PTA 06	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please consider clarifying as these two sentences seem to contradict each other. (PTA 04, 2nd Paragraph) The interface between HCAS - C and UFMS is bi-directional. HCAS - C receives generated requisitions from UFMS to be validated and assigned to an award, to generate an obligation. HCAS - C does not share collected information with any other system.	
PIA 27	Data Feed Service, pta_pia_OS_Release	3/11/2026	TIN/EIN please remember to spell out all first use acronyms. How are you confirming if a TIN/EIN is an SSN or not? Please provide a legal justification for the collection of SSN if can be used in lieu of a TIN/EIN. Once confirmed that SSNs are collected PIA 22 and PIA27A should be updated.	
PIA 22	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please also select: 'name' and 'other'. In the 'other' free text field please include the following: User ID, EIN, PIV ID	
PIA 25	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please define the following acronyms on first use within the response: HCAS - C	

AMS
PIV

PIA 27	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please define the following acronyms on first use within the response: SAM IDIQ
PIA 35	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please define the following acronyms on first use within the response: GSA
PIA 45	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please define the following acronyms on first use within the response: COTS SaaS UCS
PIA 27A	Data Feed Service, pta_pia_OS_Release	3/11/2026	For reference, the response from the non-cloud version if SSN is potentially collected. This information is provided pursuant to E.O 13478 which, states that a federal department may, whenever the head thereof finds it advisable to establish a new system or permanent account numbers pertaining to individual persons, utilize the social security account numbers. 31 U.S.C. 3512 Describes government responsibilities to ensure effective control over, and accountability for, assets for which the agency is responsible. 44 U.S.C. 3101 Describes government responsibilities to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.
PTA 21A	Data Feed Service, pta_pia_OS_Release	3/11/2026	Please include in this response: The following statement "The Privacy Impact Assessment (PIA) will be updated to reflect any future AI use cases that introduce new privacy risks."

And please detail if the AI tool be trained using the PII collected in the system.

PTA 04	Data Feed Service, pta_pia_OS_Release	3/11/2026	Add a parenthesis for differentiating the type of information that is shared bi-directional. E.G. (Non-PII award data)
PTA 04	AKHIBI, CHRISTOPHER	3/30/2026	Please, spell out PII, first time use of the acronyms in the below sentence. The interface between HCAS - C and UFMS is bi-directional. HCAS - C receives generated requisitions (e.g., non-sensitive PII award data)....
PTA 21A	AKHIBI, CHRISTOPHER	3/30/2026	Please, rephrase this statement: The AI tools are cannot trained using the PII collected in the system. to: The AI tools are not trained using the PII collected in the system.