Privacy Impact Assessment (PIA): OS - ARPIS - QTR1 - 2025 - OS2372882

Created Date: 5/21/2025 1:03 PM Last Updated: 6/9/2025 1:23 PM

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 - ARPIS - QTR1 - 2025 - OS2372882	**PIA ID:**	3204034
Name of Component:	OS - Archibus	**Name of ATO Boundary:**	Network Infrastructure Edge Services 1.0
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	101
Submission Status:	Submitted	**Submit Date:**	6/2/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	OS
Security Categorization:	Low	**OpDiv PIA ID:**	OS2372882
Legacy PIA ID:		**Make PIA available to Public?:**	No

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
2:	Is this a FISMA-Reportable system?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	11/28/2025
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.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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.	The Automated Real Property Inventory System (ARIS) is primarily used for real property inventory data tracking and for rent chargeback in HHS/PSC-managed properties. It is also used for mandatory annual inventory reporting to the Federal Real Property Council, in compliance with Executive Order 13327.
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.	Computer Aided drawings , real estate property data, rent attribution data, backend-username/roles are all stored within the system. The property and space data is stored until we dispose of the property or space. The user account is stored until the person leaves.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS Email Address

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.	Computer Aided Drawings (CAD) information contained within Archibus is used to manage Human Service/ Program Support Center (HHS/PSC)-managed properties. These drawings include the floor plans, space types, and room number). Real estate property data is stored within the system to track rent attribution data and rent attribution data is used send email reminder to points of contact. Backend usernames/roles are stored within the system as users and assigned roles within the system. There are three types of users: Administrator (reserved for technical support personnel only), power users (for those who perform advance analysis of real estate data), and standard users (who view, input, or download stand reports).
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
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.	The Automated Real Property Inventory System (ARIS) is primarily used for real property inventory data tracking and for rent chargeback in HHS/PSC-managed properties. It is also used for mandatory annual inventory reporting to the Federal Real Property Council, in compliance with Executive Order 13327. To be answered. Users access the website once authenticated into the HHS network via https://archibus.hhs.gov Users accessing the site are from HHS to include OpDivs. Users that have access to the system are in space mgmt, real property, strategy cmpt aided drafting techs and users that have been designated from each division that report such info.
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 - 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?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
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.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
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?	
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?	
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.	Name Email Address User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	51 - 200
PIA - 4:	For what primary purpose is the PII used?	User credentials, name and email address are used to identify the individual accessing Archibus.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	There are no secondary uses for PII.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy [OMB M-01-05]
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.	Username, email address and name can be used to retrieve records within the system.
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.	09-90-0777 Facility and Resource Access Control Records
PIA - 9:	Identify the sources of PII in the system.	Government Sources Within the OPDIV Other HHS OPDIV
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.	Archibus does not collect information for members of the public. The system is internal to the agency and used by agency personnel.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
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)).	
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.	
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.	Users requiring access to the system must provide their name and HHS email address.
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 can opt-out of providing their information by not providing their information which will result in them being denied access to the system.
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.	Program Support Center (PSC) will notify users via email using their HHS email address.
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.	An email would be sent to the user stating the what, if any, incident has occured and the steps that will be used to mitigate the issue.
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.	Bi-annual checks of user credentials will be conducted in March and October to ensure records for users and administrators with access to the system are still current.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators 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.	Administrators/Contractors who manage user accounts. Some power users can monitor user/system activity with Computer Aided Drawings (CAD).
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	User requests for the system are submitted via email to the System Owner for approval. Once approved the account is created within the system and assigned their determined role.
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.	Role-based accounts have predefined permissions for power users, administrators.
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.	cybersecurity awareness, cybersecurity essentials, IT administrator training
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	No additional training is required.
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).	General Records Schedule (GRS) 5.4. Item 010, Disposition Authority: DAA-GRS-2016-0011-0001. Destroy when 3 years old or 3 years after superseded, as appropriate, but longer retention is authorized if required for business use. However, Federal Real Property Data and rent attribution records are maintained indefinitely.
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.	All PII is secured through administrative, technical, and physical controls, with user credentials, names, and HHS email addresses stored within a Cloud-based Managed Application Hosting Center (C-MAHC). These systems are accessible only to HHS-cleared contractors with a need to access them. Devices are within FISMA Moderate and High Security boundaries, and access requires being on the network. The physical devices are housed in controlled data centers with strict security measures, including biometric access and monitoring. User names are encrypted using FIPS 140-2 and stored on systems encrypted with AES 256-bit encryption.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	6/2/2025
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:**	6/4/2025
		SOP Days Open:	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/5/2025 All comments have been addressed. 5/22/2025 Please see comment and update accordingly. PIA-24: Didn't provide the technical and physical controls. I recommend revising response to read "All PII is secured through administrative, technical, and physical controls, with user credentials, names, and HHS email addresses stored within a Cloud-based Managed Application Hosting Center (C-MAHC). These systems are accessible only to HHS-cleared contractors with a need to access them. Devices are within FISMA Moderate and High Security boundaries, and access requires being on the network. The physical devices are housed in controlled data centers with strict security measures, including biometric access and monitoring. User names are encrypted using FIPS 140-2 and stored on systems encrypted with AES 256-bit encryption."	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	6/9/2025
		SAOP Days Open:	4

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	5/5/2025	Please include a comment to address this question from the general information section, or update the response in the general information section if possible: 4: ATO Date or Planned ATO Date.	
PIA - 4	Data Feed Service, piafrmos_Release	5/5/2025	Please remove the carriage returns and add commas to this response so that it reads more clearly: User credentials, Name, and Email Address are used to identify the individual accessing Archibus.	
PIA - 12	Data Feed Service, piafrmos_Release	5/5/2025	This response should only be “mandatory” if an individual’s refusal to provide at least some of the PII maintained in the system may lead to a civil or criminal penalty. I believe this response should be updated: “voluntary” should be selected in situations regardless of the repercussions that may result from an individual’s refusal to provide the requested PII.	
PIA - 12A	Data Feed Service, piafrmos_Release	5/5/2025	If the response to PIA-12 is updated to 'voluntary', then please clear/delete this response from the response field.	
PIA - 13	Data Feed Service, piafrmos_Release	5/5/2025	I would consider adding a sentence along the lines of: 'Users can opt-out of providing their information by not being able to/not being granted access to the system.' If you find that this fits how the	

			system and access would function.
PIA - 14	Data Feed Service, piafrmos_Release	5/5/2025	Please define the acronym 'PSC' on first use within this response.
PIA - 24	Data Feed Service, piafrmos_Release	5/5/2025	Please define the acronym 'C-MAHC' on first use within this response.
PIA - 23	Data Feed Service, piafrmos_Release	5/5/2025	Please cite specific records retention schedules. Please list any of NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) that apply to the information maintained in the system; and/or State if NARA is determining the appropriate RCS Job Number or GRS for some or all of the information maintained in the system and that the PII should be maintained until a determination is provided. If you need assistance in determining this please reach out to: Karen Ballesteros and HHSRecordsManagement@hhs.gov An example of this would be the following response: "General Records Schedule (GRS) 3.2. Item 010, Disposition Authority: DAA-GRS-2013-0006-0001. Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system."
PIA - 1	VILLAFUERTE, NESTOR	5/22/2025	Please include name and e-mail in your response in PTA-5 and PTA-6 in the next iteration of the PTA.
PIA - 24	VILLAFUERTE, NESTOR	5/22/2025	Please provide specific details on how PII is secured through the three categories. ie. Administrative - Policies and procedures in place Technical - Firewall, encryption, MFA, etc. Physical - Security guard, biometrics, etc.
PIA - 1	BLAND, CRYSTAL	5/22/2025	In addition to the previous comment also add "user credentials" to PTA-5 and PTA-6 on the next iteration of

			the PTA.
PIA - 24	BLAND, CRYSTAL	5/22/2025	Revise Response to read "All PII is secured through administrative, technical, and physical controls, with user credentials, names, and HHS email addresses stored within a Cloud-based Managed Application Hosting Center (C-MAHC). These systems are accessible only to HHS-cleared contractors with a need to access them. Devices are within FISMA Moderate and High Security boundaries, and access requires being on the network. The physical devices are housed in controlled data centers with strict security measures, including biometric access and monitoring. User names are encrypted using FIPS 140-2 and stored on systems encrypted with AES 256-bit encryption."

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:	6/9/2025 1:23 PM	**History Log:**	**View History Log**