Privacy Impact Assessment (PIA): OS - PSC-WS: ARS - QTR1 - 2025 - OS2339871

Created Date: 4/4/2025 5:03 PM Last Updated: 4/15/2025 8:57 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 - PSC-WS: ARS - QTR1 - 2025 - OS2339871	**PIA ID:**	2968848
Name of Component:	OS - OS - OS - PSC-WS: Acquisition Reporting System	**Name of ATO Boundary:**	PSC WorkSmarter
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	63
Submission Status:	Submitted	**Submit Date:**	4/1/2025
Next Assessment Date:	N/A	**Expiration Date:**	4/14/2028
Office:		**OPDIV:**	OS
Security Categorization:		**OpDiv PIA ID:**	OS2339871
Legacy PIA ID:	983656	**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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	10/11/2024
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.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	No changes have occurred to the ARS system since the last Privacy Impact Assessment (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.	Acquisitions Reporting System (ARS) is a centralized reporting system for the Department of Health and Human Services (HHS) acquisition offices acquiring support from the Program Support Center (PSC). Information is pulled from Purchase Request Information System (PRISM) by way of a database link. ARS which is a child application of the PSC WorkSmarter platform provides reporting that is not available via PRISM such as active/expired contracting listing, unused requisition lines, and pending awards. ARS also generates/calculates acquisition fees sent to PSC Revenue, Invoicing, and Cost Estimation System (PRICES) via a flat file (a text file containing invoice information that can be read and parsed by a receiving program), provides technical staff the ability to generate ad hoc reports, provides a mechanism for acquisition-centric workload tracking (pre-award), and hosts the ticketing system for help desk support staff.
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 information contained in ARS (as a result of either reporting or as a result of help desk ticket information) include the following data: user names, vendor and contracting officer names (and professional contact information), vendor mailing addresses, phone numbers, vendor financial account information, legal documents (e.g. copy of a contract document), web Uniform Resource Locator (URL), email addresses, and vendor tax ID numbers (TIN). The system does not store username/password combinations (those are handled at the platform level), but it does provide a mapping between the usernames used in ARS and PRISM. Data collected is saved permanently.
PTA - 5A:	Are user credentials used to access the system?	No
PTA - 5B:	Please identify the type of user credentials used to access the system.	

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.	ARS is a centralized reporting system for HHS acquisition offices acquiring support from the PSC. Information is pulled from PRISM by way of a database link. Reports can be run on demand by the user or scheduled to be sent via email. Reports are cached by ARS and purged during regular system maintenance. Since PSC is a Fee For Service, additional reports are run to generate a flat file to another PSC system called PRICES so the system can collect our acquisition fees for processing the contract on behalf of the HHS Customer. The data in this flat file includes contract number, contract amount, accounting information, HHS Customer Contact Information, and the fee amount. In addition to reporting capabilities, the ARS acts as a Help Desk ticketing system for tier 1 and 2 support of PRISM . Tier 1 includes support such as password resets and help with system navigation; while Tier 2 includes support such as walking a user through the creation of a solicitation or to process an assignment of claims. The types of information that is stored in ARS for help desk support is the user's contact information (name, email address, phone number), a description of the problem, associated screenshots (if applicable), and any issue/resolution steps needed to resolve the ticket. Information contained in ARS (as a result of either reporting or as a result of help desk ticket information) include the following data: user names, vendor and contracting officer names (and professional contact information), vendor mailing addresses, phone numbers, vendor financial account information, legal documents (e.g. copy of a contract document), web URLs, email addresses, and vendor tax ID numbers (TIN).
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?	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.	ARS is a child application of the PSC WorkSmarter platform, which provides a website for users to access the applications on the platform. All access to the ARS application of WorkSmarter website is limited to those pre-identified users, who must log in with their federal Personal Identity Verification (PIV) card. PSC WorkSmarter application users access the system via https://worksmarter.appiancloud.com. PSC WorkSmarter user security groups are designed in a way that only provides access to certain modules/information on need to know basis. User roles are also adjusted to give each user specific privileges to access certain areas of the platform. All PSC WorkSmarter user accounts, including ARS application users, are set up and authorized by system administrators before users can log into the Website. HHS Federal employees and direct contractors have access to the website. All users are required to complete a background investigation and receive a valid HHS PIV card before gaining access to the system. Users can access the website by logging into Access Management System (AMS). System administrators with a public trust and valid PIV have access to the website to provide system support and over all process improvement.
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?	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.	Social Security Number Name Email Address Phone numbers Certificates Taxpayer ID Financial Account Info Legal Documents
PIA - 2:	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 - 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?	Acquisitions Reporting System (ARS) contains information necessary to support a procurement relationship between the Department of Health and Human Services (HHS) and the vendor community. There are limited instances where an individual's information is in identifiable form. In addition to names of contractors who serve as HHS buyers, ARS may also contain Personal Identifiable Information (PII) for service fellows and sole proprietorships that provide vendor services as individuals. Contract Officer Representative (COR) information (name and email address) is used by the Contract Closeout Initiation (CCI) system, which is a robotic processing automation tool that will automatically send notifications to COR in order to close out awards. These notifications will also include the vendor's name, Point of Contact (POC) email, and Taxpayer Identification (ID) numbers, as needed.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	ARS does not use any PII data to identify and process and perform testing, training or research.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	The system stores Vendors' TAX identification Numbers (TINs), which may occasionally include Social Security Numbers (SSNs) in the case where a vendor is a sole proprietorship. The TIN is used to uniquely identify the vendor for federal award actions, enabling efficient retrieval of additional information about that vendor. This is essential for identification and reporting purposes within the system, ensuring accurate and compliant data management.
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	There is no specific legal authority for use of the SSN, but the system stores vendors' TINs, which may sometimes include SSNs if the vendor is a sole proprietorship. The system retrieves the vendor's information from the System for Award Management (SAM). Tax laws permit sole proprietors to use their SSN as their TIN if they do not have a separate Employer Identification Number (EIN). The TIN serves to uniquely identify the vendor for federal award actions, facilitating the efficient retrieval of additional vendor information. It is crucial for identification and reporting within ARS, ensuring accurate and compliant data management.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	42 US Code, The Public Health and Welfare. This is the Title of the US Code that implements HHS and provides it with the legal authority to operate.
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.	ARS uses the user's WorkSmarter and Purchase Request Information System (PRISM) usernames in order to retrieve records associated with that user. For example, help desk tickets that the user has created, or awards that the user has created in PRISM.
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.	GSA/GOVT-9
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Phone Email
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 does collect PII from authorized users in order to allow them to perform tasks. However, the Office of Management and Budget (OMB) approval number is not applicable.
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)).	N/A
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.	
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.	End users of ARS are informed at the time of training and at each refresher training for upgrades/updates to the system. While submission of PII is required, vendors submit this information as part of doing business with the government in order to be paid for services to HHS. Vendors have the choice to not do business with HHS. There is no option to opt-out of the collection of this data as it's a requirement to do business or be employed by the federal government.
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.	No consent is obtained as it is implicitly granted in order to do business or be employed by the federal government.
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.	PSC Platform Operations and maintenance (O&M) team addresses all concerns regarding individuals' PII information. Individuals who are concerned about their PII being inappropriately obtained, used, or disclosed, or that the PII is inaccurate can contact the helpdesk by calling 301-492-4555 or emailing PSCWorkSmarter@psc.hhs.gov. PSC Platform O&M team then investigates and escalate the issue to HHS Office of Information Security if required.

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.	Data received from HHS Consolidated Acquisitions Solution (HCAS) is reviewed at least annually by the source data systems. COR data in HCAS is updated and verified by individual contracting officers on an ongoing basis. Vendor data is verified only when an issue arises with vendor payments. Vendor data is updated by the vendor in General Services Administration (GSA) system SAM which gets interfaced to (Unified Financial Management System) UFMS then to HCAS and reported by ARS.
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.	System administrators and developers have access to all data including PII in the system to provide system support and over all process improvement. However, they do not use PII on a regular basis to perform daily operational and maintenance activities. System Administrators have access to name and email address to be able to reset passwords upon request as well as managing user accounts. Developers have access to names and email addresses for purposes of developing new child applications, fixing issues, or enhancements (e.g. a form may need to display the user's name logged onto the system or send an email notification). HHS/OpDiv Direct and Third-Party Contractors with LEVEL 6/T 4 Public Trust and valid HHS Personal Identity Verification cards may serve as administrators or developers.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	In order to have access to ARS, each person must have passed background investigation and received level 6 public trust and HHS PIV Cards. In addition, these individuals must submit request to access the information and Federal manager at PSC makes a final determination whether to grant this request or not

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.	Only authorized system administrators/contractors with level 6 clearance have access to PII within the PSC WorkSmarter application and at the server level or have the ability to configure and make any changes within the application. The system has been designed to allow only the least system privileges necessary to perform specific system functions. Access authorizations and enforcements are managed through the Active Directory in computer management>system tools>local users and groups. HHS restrictions, Rules of Behavior, Role Based Access Controls for users are also in place with monitoring/logging and review processes to determine need to use, least privilege access for PII. The only users with access to ARS all have access to the same PII data elements by design. There is no desire nor need to limit visibility to specific data based on role.
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.	HHS cybersecurity awareness training, role based PII data handling training is provided to all personnel using PSC WorkSmarter.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	PSC WorkSmarter administrators receive Role Based training for privacy awareness. All system users must complete Annual HHS Cybersecurity Awareness Training; the Rules of Behavior for Use of HHS Information Resources and signe the accompanying acknowledgement. Monthly town-hall style training sessions as well as one-off training to cover system features are provided to end users of the system.
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).	The data will be maintained per General Records Schedule (GRS) 3.2. Item 010, Systems and data security record, 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/ Information Technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system.

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.	ARS is a child application of the PSC WorkSmarter platform, which provides a website for users to access the applications on the platform. All access to the WorkSmarter is limited to those pre-identified users, who must log in with their federal PIV card. Role Based Access Controls are used to secure and protect PII data within the PSC WorkSmarter system. Only authorized system administrators and developers with LEVEL 6/T4 Public Trust can access PII, make any changes, or update certain configuration properties for the PSC-WS application. No other PSC-WS user has this ability. All system changes made through the Administration Console by authorized users are logged to an audit log which captures the user name of the administrator user name who made the change along with the previous and new values of the change property. Only administrators have access to the HHS/OCIO Managed Application Hosting Center Cloud (C-MAHC) servers by way of HHS network access via a firewall opening, and since the data is stored in a Federal Risk and Authorized Management Program (FedRAMP) approved environment the Cloud Service Provider will ensure physical controls are in place.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/4/2025
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:**	4/4/2025
		SOP Days Open:	3

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	4/14/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 4/14/2025 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	10

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer_Signature_Crystal_Bland.docx
SAOP Comments:		**SAOP Review Date:**	4/15/2025
		SAOP Days Open:	1

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	3/7/2025	Some TINs could be SSN.	
PIA - 8B	Data Feed Service, piafrmos_Release	4/1/2025	ARS is not a system of record. The system is not the main database where official information about individuals or processes is stored within the organization. The system retrieves the vendor's information from the System for Award Management (SAM), and when the vendor is a sole proprietorship and use SSN as the TIN, ARS cannot determine whether an SSN has been used when retrieving this information.	
PIA - 1	BLAND, CRYSTAL	4/14/2025	On the next iteration of the PTA: Per PTA-9, PTA-5a should be marked "Yes, but user credentials are maintained in another system AMS."	

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:	4/15/2025 8:57 AM	**History Log:**	View History Log