PTA / PIA: OS - PMS - QTR4 - 2025 - OS3239096

Created Date: 1/9/2026 4:02 PM Last Updated: 1/23/2026 4:04 PM

General Information

PTA / PIA Name:	OS - PMS - QTR4 - 2025 - OS3239096	**PTA / PIA ID:**	4182056
Component Name:	OS - OS - Payment Management System	**ATO Boundary Name:**	Payment Management System
Overall Status:	Complete	**# of Days - Open:**	25
Submitter:		**Submit Date:**	12/29/2025
Next Assessment Date:	01/22/2029	**Expiration Date:**	1/22/2029
Office:		**OpDiv:**	OS
Security Categorization:	High		
Make PIA available to Public?:	No	**PIA Required:**	Yes
General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance	
General 02:	Is this a FISMA-Reportable system?	Yes	
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes	
General 04:	ATO Date or Planned ATO Date.	5/10/2024	
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency	
History Log:	**View History Log**		

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Ralph Johnson
PTA 01A:	POC Title and Organization	ISSO HHS
PTA 01B:	POC Email Address	ralph.johnson@hhs.gov
PTA 01C:	POC Phone Number	(301) 945-5551
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Defend The Spend (DTS) integration XMS/ID/me authentication

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 PMS is a web based system that electronically transmits Federal grant funds to grantees via the Federal Reserve Bank (FRB). The PMS accountants transmit grantee payment requests via authorized FRB virtual private network (VPN)and Automated Clearing House (ACH) payments. Access maintained by the FRB. PMS provides real time accounting information to grantees and Federal agencies. We transmit to Treasury same day wires and international payments. The agreement with Treasury is the Delegated Disbursement Authority.

PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The PMS maintains automated interfaces with grant awarding agencies. The information the agency collects, maintains, or disseminates is an HHS standard financial record, which is exchanged to identify new grants and modification to existing grants. The PMS provides output to agencies with regard to disbursement data, synchronization data, standard form (SF) SF-224 data (statements of transactions) (Financial Management Service (FMS) 224) reporting by agencies for which The Treasury Dept. disburses), and daily payment information to agencies that request it. The information contains personally identifiable information (PII) in the form of Social Security Number (SSN), bank and routing data, Internal Revenue Service (IRS) data (Employer Identification Number), Personal Names, mailing address, taxpayer ID, Personal Phone Numbers, and Personal Email Addresses. Grantee information is collected via a Standard Form (SF) 1199A, Direct Deposit form, that is either mailed, faxed or emailed from the grant recipient to a Federal staff member that enters the information into the PMS. The PMS maintains PMS user information for access purposes. This information includes; user names, passwords and email addresses. PMS employees total encryption; data at rest, in transit and live. Account Credentials are stored on the Access Management System (AMS) and the PMS application. PMS uses two factor authentication. We transmit to Treasury same day wires and international payments. The agreement with Treasury is the Delegated Disbursement Authority. All HHS financial systems are required to be reviewed by and have access to, by the HHS Office of the Inspector General (OIG) Information Shared(a): We provide Grantee Banking information, Eg. Bank Routing number and Account number so that the Dept of Treasury or The Federal Reserve Bank can issue funds to the requesting Grant Recipient bank account. Information Shared(b): To maintain the accounting transactions for accuracy and reconciliation, PMS sends Accounting data only to the Accounting System of records with in the Department of HHS The agreements between the PMS and internal and external Federal Agencies are Inter Agency Agreement's (IAA's) maintained at the Payment Management Service Office. We do not issue MOU's or ISA. PMS enforces password credentials to be changed every 60 days – as long as the account is active. If not changed and/or the account is not accessed in 90 days, the account is disabled. Credentials and PII are stored permanently - data is not purged nor archived.
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.	XMS/ID.me 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.	Info is collected for authentication into the PMS system. Email and PIV/CAC info is collected depending on auth method.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://pms.psc.gov/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The PMS is a web based system that electronically transmits Federal grant funds to grantees via the Federal Reserve Bank (FRB). The PMS accountants transmit grantee payment requests via authorized FRB virtual private network (VPN)and Automated Clearing House (ACH) payments. Access is maintained by the FRB. The system grants access to PMS agency users, e.g., PMS accountants, and the system is accessed via log in page using ID.me, AMS, or PIV.
PTA 10:	Does the website have a posted privacy notice?	No
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Web bug/beacons- Does Not Collect PII Session Cookies- Does Not Collect PII Persistent Cookies- Does Not Collect PII
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Taxpayer ID Number (TIN) Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business)
PIA 23:	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 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	For the Payment Management System (PMS), PII is considered Banking Information. The primary use of the banking information is disbursement of grant funding to authorized grantees, cash flow, and reporting. Banking Information is also used to report disbursement data back to the financial system of record. (This is accounting information only) (US Federal Government Authorized Accounting Systems, i.e. United Financial Management System (UFMS)) for reconciliation purposes.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	PII may be used if required by reporting requirements, to audit the grant funding process, or for the Operating Division (OpDiv) to review its activity and evaluate issues related to efficiency, budgeting, and operations. Data is never released without program authorization.
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.	PMS operates for the purpose of providing a central system capable of paying most Federal assistance grants, block grants, and contracts. HHS is required to record these transactions and include the Taxpayer Identifier Number (TIN) associated with each payee. In a very limited number of instances PMS uses the SSN as the TIN when a grantee does not have a separate Employer Identification Number (EIN), as allowed under tax laws. PMS is a subledger to the financial system as such our primary attribute for PII is the TIN as a disbursing agent.

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.	In a very limited number of instances PMS uses the Social Security Number (SSN) as the TIN when a grantee does not have a separate EIN, as allowed under tax laws, Executive Order (EO) 9397, Numbering System for Federal Accounts Relating to Individual Persons, November 22, 1943, which states in part that any Federal department, establishment, or agency may, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to Title 26, section 402.502 of the 1940 Supplement to the Code of Federal Regulations and pursuant to paragraph 2 of this order.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The implementation of this system, is authorized by 5 U.S.C. 301 and section 205(c) of the Federal Property and Administrative Services Act of 1949, as amended by 40 U.S.C. 486(c), as delegated by the Secretary. Budget and Accounting Act of 1950 (Pub. L. 81-784); Debt Collection Act of 1982 (Pub. L. 97- 365); Debt Collection Improvement Act of 1996 (Pub. L. 104-134, sec. 31001. More precise HHS acquisition rules are issued in the Code of Federal Regulations (CFR) at 48 CFR Chapter 3. Office of Management and Budget (OMB) Circular No. A-102 addressing the administration of grants to state and local governments and federallyrecognized Indian tribal governments; OBM Circular No. A-110 addressing the administration of grants to institutions of higher education, hospitals, and other non-profit organizations; OMB Circular No. A-123 addressing internal controls; and, The Treasury Financial Manual (TFM) Volume I, Part 5, Chapter 1000 specifying responsibilities and liabilities of agencies with delegated disbursing authority.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	Social Security Number, Name, Email Address, Phone Number, Mailing Address, Taxpayer ID
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-0024, Fin. Txns.of HHS Acctg & Fin. Offices, General Services Administration(GSA)/GOVT 9, System for Award Management

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Other Federal Entities Non-Government Sources Private Sector
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.	The Payment Management System is not a direct public facing system and does not collect PII information from the general public. The information used is in established agreements between the Granting Agencies and their Grantee population.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	Defend The Spend DTS - for payment approvals Other Fed Agencies (see PIA 32C for complete list) - to support payment management services

PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	HHS NextGen XMS HRSA Electronic Handbooks (EHBs) Integrated Financial and Acquisition Management System (iFAMS) Financial Management Modernization Initiative (FMMI) NIH Electronic Research Administration (eRA) Fiscal Service Oracle e-Business Suite (OeBS) Treasury TWAI NIH Hosting (Application) NIH Hosting (SharePoint) GrantSolutions AMS NIH Business System (NBS) DOL ETA
PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	MOUs/ISAs are drafted, signed by all parties, and submitted into HHS Archer to track active interconnections. These documents are reviewed annually, based on specified timeline, or if changes are made to the system/POCs.
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.	Notification and consent is obtained by the completion of the Grant Application (they have opted-in to the collection, hence no need to provide an opt-out), which explicitly states the nature of the use of the PII. The Grant Application includes the electronic process whereby PII data is shared with awarding institutions, the Federal Reserve and other involved banking institutions.
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.	Users supply information voluntarily for the purposes of conducting business or otherwise receiving payments from HHS. Consent for this collection is implicit in the process. In the event any changes were made to the system that affected individuals rights or interests, these individuals could be contacted using the PII they have provided. Conversely, a user that wished to learn more about the use of their PII may consult the PMS website, which directs users to the HHS Cybersecurity Team and/or the HHS Office of the Privacy Coordinator.

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.	Grantee may contact their Certifier or HHS directly by email or phone. The user achieves access to the PMS utilizing a web portal that is the PMS home page (https://pms.psc.gov/). At the bottom of the PMS home page, the user can click Privacy Policy, which takes them to the HHS.gov Privacy Policy Notice page (http://www.hhs.gov/Privacy.html) where there is a Notice and link in the first section of the page to go to the HHS.gov health Information Privacy page (http://www.hhs.gov/ocr/privacy/index.html). On the left pane of this page there is a link for How To File A Complaint (http://www.hhs.gov/ocr/privacy/hipaa/complaints /index.html)
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.	Payments are made to grantees on an ongoing basis. The grantees have access to their accounts and can submit changes and requests for payment. As this is the best source of obtaining this information we leave that review to the grantee as updates follow a standard practice. System Security controls are reviewed annually or when changes to the system occur. Several audits occur annually to ensure security requirements are met.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users only have access to their specific accounts. System admins/staff troubleshoot user issues, facilitate the resetting of passwords, etc. Contractors (tier 3 support) troubleshoot user issues that cannot be resolved by admin/staff.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Based on the sensitivity of the PII in PMS, security measures are employed in granting access to the system. Users are granted access to screens containing PII only if they have 1) need to use that information as part of their official duties, and; 2) have received a security level VI clearance or higher. This applies to contractors as well and is enforced by HHS security and privacy protection policies. PMS personnel must hold appropriate clearances that provide for *operations and maintenance (O&M) for the system. Grantees are provided access to their own information and do no have the ability to access other grantee information. PMS employees segregated access and least privileges for Granting Agency users, Grantees, PMS accountants (Federal staff) and PMS application developers (direct contractors) as well as PMS Help Desk personnel whom perform password resets and provide general PMS instructions to the Grantees. *Operations and Maintenance (O&M) - When a mature system like the PMS is in a steady state of operation and is continuing to perform, a contract is issued to maintain the system, we call this an O&M contract. A replacement system would not be an O&M contract for example. Operations would mean daily or monthly security patching requires testing before implementation into the production environment. Maintenance means the day to day activities that a financial system requires to function for example, databases need to be maintained daily to avoid corruption by adjusting table space. The O&M contractors mentioned are Direct Contractors.
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.	There are very limited number of instances where an SSN is entered in the system as the TIN. However, all DPM system users have access to all PII. For system developers, only those individuals who need access to databases to test the performance of the system have access to any database contents, but again, they have access to all PII. PMS access has segregated access and least privileges for Granting Agency users, Grantees, PMS accountants (Federal staff) and PMS application developers (direct contractors) non-direct contractors (PMS Help Desk) are used for Password resets and general PMS information.
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.	All users receive Department-level Privacy Awareness Training and Information System Security training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	High level users of the PMS complete privacy and security training specific to the National Institutes of Health.

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).	The records stored in the Payment Management System (PMS) are considered temporary and should be managed in accordance with the following records disposition schedules: 1.General Records Schedule (GRS) 1.1: Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. Item 010. Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. 2. GRS 3.1: General Technology Management Records. Item 010, Information technology development project records. Temporary. Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. 3. GRS 3.1: General Technology Management Records. Item 011, System development records. Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.
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.	All PMS data, PMS databases and the PMS application are fully encrypted, i.e.., data at rest, data in transit and live PMS application access. All data collected to support the processes of the PMS is stored in tables. The information is secured through multiple levels of security and access controls have been established to authenticate the user and to determine if the user has the authorization to perform actions requested. The access controls are supplemented with a secure network at both National Institutes of Health (NIH) and PMS. Administrative Controls: Certification & Accreditation (C&A), Approved System Security Plan(SSP), Contingency Plan, Backups, Off-site Storage, User Manuals, Contractor Agreements, Least Privilege, PII Policy Technical Controls: Authentication, Firewall, Virtual Private Network, Intrusion Detection, Process for monitoring and responding to security incidents, Encryption, Common Access Cards (CAC), public key infrastructure (PKI) Physical Controls: Guards, ID Badges, Closed Circuit Television(CCTV), Keycards, Kastle Keys, Coded keys that provides elevator floor access, Biometrics

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	1/8/2026
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	10

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	1/9/2026
SOP Review Comments:		**# of Days - SOP Review:**	1

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	1/15/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 1/15/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	1/23/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
1/23/2026 12:40 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
PIA 38	Data Feed Service, pta_pia_OS_Release	12/29/2025	Users only have access to see their own PII (email, phone, etc.) Admins are PMS staff Only approved Database contractors have access to PII	