PTA / PIA: OS - MAHC - QTR3 - 2025 - OS3106788

Created Date: 11/18/2025 4:04 PM Last Updated: 11/24/2025 4:02 PM

General Information

PTA / PIA Name:	OS - MAHC - QTR3 - 2025 - OS3106788	**PTA / PIA ID:**	3984657
Component Name:	OS - Managed Application Hosting Center	**ATO Boundary Name:**	Managed Application Hosting Center
Overall Status:	Complete	**# of Days - Open:**	63
Submitter:		**Submit Date:**	9/30/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
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)?	No
General 04:	ATO Date or Planned ATO Date.	3/24/2026
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	Alemseged Mera
PTA 01A:	POC Title and Organization	OS
PTA 01B:	POC Email Address	alemseged.mera@hhs.gov
PTA 01C:	POC Phone Number	202-875-4739
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.	None
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Contractor

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 Managed Application Hosting Center (MAHC) was established to maintain a secure data center for hosting multiple HHS applications. MAHC may include any Personally Identifiable Information (PII) that an underlying application creates. HHS applications range in purpose from financial management systems to emergency response systems. Each application/system hosted by MAHC has a Privacy Impact Assessment (PIA). MAHC GSS administrators do not have access to the HHS application backup data stored within the GSS. MAHC personnel only assist with restoring this data to the application servers and database at the request of the application owner. The following applications reside in MAHC GSS and have their own Privacy Threshold Analysis (PTA)/ Privacy Impact Analysis (PIA): Access Management System (AMS); Assistant Secretary for Planning and Evaluation (ASPE); Border Directory; Debt Management and Collection System (DMCS); Integrated Time & Attendance System (ITAS); NDMS (Umbrella for the following 8 applications: TEAMS, CONFERENCE, JPATS, RMS, INCEP, OSEO, HIR, NHIN Gateway. [RMS & TEAMS are the primary apps]); Physical Access Control System (PACS); PSC Revenue, Invoicing and Cost Estimation System (PRICES); Strategic Work Information Folder Transfer (SWIFT); Tandberg Management System (TMS); and WorkSmarter.

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 MAHC collects and stores data for backup purposes only for the applications that it hosts. It does not disseminate information. MAHC may contain any and all data that the hosted applications create. MAHC uses the information only for the purposes of backing up the data. Underlying systems use the data for a broad range of purposes, reflected in those systems' PIAs. Other data stored is related to data log files and management data regarding the performance of that application. All HHS/Office of the Secretary (OS) Staff Divisions (StaffDivs) supported by Program Support Center (PSC) can store data in some of the applications that are hosted in the MAHC. User credentials are maintained for system administrators (OS employees and direct contractors) in MAHC. Log Files and Management Data could contain the following: Server User Access and Authentication Logs, Server Resource Utilization Logs, including Central Processing Unit/Memory/Disk Read and Write Network events, Database user access and authentication logs, Permission Modification logs, and User created/deleted logs. The information is stored for five (5) years.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card HHS Username Password
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.	The MAHC is a General Support System (GSS) that provides the protected environment through which HHS connects to its major applications. MAHC hosts 11 applications, and each application is required to complete a separate PIA. Data processed on the MAHC is considered Sensitive but Unclassified (SBU). Classified information is not permitted on the system. Other data stored is related to data log files and management data regarding the performance of that application. All HHS/OS StaffDivs supported by PSC can store data in some of the applications that are hosted in the MAHC. User credentials are maintained for system administrators (OS employees and direct contractors) in MAHC. Log Files and Management Data could contain the following: Server User Access and Authentication Logs, Server Resource Utilization Logs including Central Processing Unit/Memory/Disk Read and Write Network events, Database user access and authentication logs, Permission and Modification logs, and User created/deleted logs.
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?	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.	Biographical Information User Credentials Contact Information Email Address (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	Login credentials (email address and password) are collected to support and administer Managed Application Hosting Center (MAHC) General Support System (GSS) to access the system, administrators enter login credentials.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	N/A
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	5 USC 301, Departmental regulations
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.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV
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.	N/A
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.	Within HHS

PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	1- The interconnection between ENMS, owned by OS\ITIO, and the MAHC GSS, owned by Sev1Tech, is a two-way path for HHS owned applications to provide data and information to their user community. 2- The interconnection between HHSNet, owned by OS\ITIO, and the MAHC GSS, owned by Sev1Tech, is a two-way path for HHS owned applications to provide data and information to their user community. Those data include: public health care information and data exchange; internal HHS user information and data exchange related to performing assigned duties; and internal HHS user information and data exchange related to HR and back-office functions such as payroll.
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)).	MEMORANDUM OF UNDERSTANDING (MOU) Between Managed Application Hosting Center (MAHC) General Support System (GSS) And HHS ENMS MEMORANDUM OF UNDERSTANDING (MOU) Between Managed Application Hosting Center (MAHC) General Support System (GSS) And HHS OS\ITIO\HHSNet
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.	Both parties shall: • Agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit. Both parties certify that its respective system is designed, managed, and operated in compliance with all relevant federal laws, regulations, and OS policies. • Both parties agree to maintain the higher level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the systems.
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.	Consent for data collection and use depends on the underlying business processes of each application. Consent is not collected for system and data backup purposes in and of itself, but as part of consent for the underlying activities. An option for users to opt-out of having their login credentials stored within the MAHC system is not available because it is fundamental to the function of the system. Potential user cannot 'opt-out' of providing his or her PII .The PII is needed to create a user account in order to access the MAHC system.

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.	MAHC is the general support system and access is provisioned to the users and system administrators through the change request process submitted to add to GSS at the time of on-boarding. Applications supported by MAHC GSS have their own processes in place to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system as defined in their individual privacy impact assessments (PIA).
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.	Although, there is no formal process-in-place, the users are aware of an informal process where they can notify the Sev1Tech Security Lead via email to resolve an individual's concerns about their any misuse of their user names. Since, users typically login with their user name many times a day, any inaccuracies would immediately be detected. Audit logs provide a way to determine if a user name was used by someone other than the user. If so, this would be treated as an security incident and the incident response plan would be activated. Users and system administrators provide notification of PII events at HHS by contacting the Office of Information Technology Infrastructure and Operations (ITIO) Service Desk to report the incident. If the incident is considered a breach, then the Office of the Secretary (OS) Privacy team would be notified and would investigate the nature and impact first. The ITIO Service Desk routes PII incidents to the HHS Computer Security Incident Response Center (CSIRC). The CSIRC notifies the HHS Privacy Incident Response Team (PIRT), Information Privacy and Security Officer (IPSO) for the related system then supports investigation and mitigation of the privacy incident. The PIRT executes investigation, mitigation and any notification related to the privacy incident. If the user credential information is inaccurate such that a name is misspelled or an e-mail is incorrect, then a simple e-mail to the OS Access Authority with the details of the change would be sufficient to correct the problem and amend the record within MAHC.
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.	User names are maintained in one location and all user names (accounts), since a user uses their user name for authentication to the system any integrity, availability, or accuracy would be identified upon the first use and subsequent use of that user name. If the user name was inaccurate in any way the login would fail. There is no reason to check for relevancy as the user would not be able to perform their job duties if the user name was not relevant.
PIA 38:	Identify who will have access to the PII in the system.	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.	Administrators Reasoning: System administrators who are direct contractors have access to PII as they enter the users names and require knowledge of the user name when troubleshooting a users access to the system. Security Administrators are required to review audit logs where user names are present. Contractors Reasoning: Direct contractors perform all duties and responsibilities in the role of System Administrators that include user and password management.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	MAHC GSS administrators do not have access to the HHS application backup data stored within the GSS. MAHC personnel only assist with restoring this data to the application servers and database at the request of the application owner. Prospective users must sign an account request form. The account request form must also be filled indicating the minimal access required to perform one's tasks. Prior to granting access, review and approval is required by the system 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.	MAHC administrators only assist with restoring this data to the application servers and database at the request of the application owner. System Administrators review user accounts at least annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users, including system administrators, are logged and reviewed by the MAHC system IPSO to identify abnormal activities if any.
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 of the system are required to annually sign the HHS Rules of Behavior. Annually they must complete HHS Cybersecurity Awareness Training, and HHS role- based training for Information Security for IT Administrators.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Privilege users access to MAHC GSS will have annual role-based training.
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).	General Records Schedule (GRS) 3.1 Item 020, Item 030, Item 051. General Records Schedule (GRS) 3.2 Item 030, Item 031, Item 040, Item 041. Disposition Authority DAA-GRS-2013-0006-0003. Destroy when business use ceases

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.	User names are stored on devices that reside within Federal Information Security Modernization Act (FISMA) Moderate and High Security boundaries. Administratively these systems are only accessible by HHS cleared contractors that have a need to be on the systems. In order to access these devices technically a user has to be within the network, they are not publicly accessible. The physical devices are in controlled data centers that meet rigorous security controls, to enter the facility security guards, biometric access, security cameras, are in place. The devices reside in cages that can only be accessed by biometric devices and monitored by security cameras. All user names are transmitted using Federal Information Processing Standard (FIPS) 140-2 encryption and stored and maintained on systems that are encrypted using Advanced Encryption Standard (AES) 256-bit encryption.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	11/14/2025
Privacy Analyst Review Comments:	This PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	45

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	11/18/2025
SOP Review Comments:		**# of Days - SOP Review:**	4

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/24/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 11/24/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/24/2025 2:40 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 22	Data Feed Service, pta_pia_OS_Release	9/24/2025	Please also select 'User Credentials'.	
PIA 32B	Data Feed Service, pta_pia_OS_Release	9/24/2025	Please move what is already in this response field to the response for question 32C. For this response, adjust it accordingly so that it covers: For each type selected in PIA 32A: • Name or describe the entities or individuals that have direct access to or receive PII directly from the system; and • Explain why and for what purpose PII is shared with each entity or individual.	
PIA 32C	Data Feed Service, pta_pia_OS_Release	9/24/2025	Please move what is in the response for question 32B to this response field.	