PTA / PIA: OS - HHSCGPT - QTR3 - 2025 - OS3059692

Created Date: 8/29/2025 11:30 AM Last Updated: 8/29/2025 1:02 PM

General Information

PTA / PIA Name:	OS - HHSCGPT - QTR3 - 2025 - OS3059692	**PTA / PIA ID:**	3728217
Component Name:	OS - HHS ChatGPT	**ATO Boundary Name:**	HHS ChatGPT
Overall Status:	Complete ✓	**# of Days - Open:**	2
Submitter:		**Submit Date:**	8/28/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OpDiv:**	OS
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Initiation
General 02:	Is this a FISMA-Reportable system?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	8/29/2025
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	Chelsea Ward
PTA 01A:	POC Title and Organization	ISSO
PTA 01B:	POC Email Address	chelsea.ward@hhs.gov
PTA 01C:	POC Phone Number	2028689773
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	Chat Generative Pre-Trained Transformer (ChatGPT), developed by OpenAI, is a state-of-the-art language model designed to assist with a variety of tasks through natural language understanding and generation. Its primary purpose is to facilitate human-computer interaction by providing coherent and contextually relevant responses to text-based queries. ChatGPT is a tool that can help improve employee productivity. The model can summarize text, simplify complex information, generate creative responses, answer questions and provide explanations as examples of functions. ChatGPT will be available for use across all HHS Operating Divisions. Although ChatGPT is not designed to collect personally identifiable information (PII), users must adhere to HHS privacy guidelines and rules of behavior. These guidelines prohibit select inputs, including PII, Protected Health Information (PHI), financial or procurement-sensitive information, classified and controlled unclassified information (CUI), internal deliberative or pre-decisional content, sensitive operational or technical information, and nonpublic workforce information. The Privacy Impact Assessment (PIA) will be updated if HHS privacy guidelines change and introduce new privacy risks.
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.	ChatGPT doesn't actively seek or extract Personal Identifiable Information (PII). No PII beyond User Credentials (Username & Password) are collected. The ChatGPT application will not have the ability to share information externally. The credentials are only stored for the length of time that the access is required. User prompt/question inputs and prompt/question outputs - If a person includes personal data details within the query such as name, address, or phone number in the message, that information will become part of the conversation history, but it's not used to identify the individual. Data is stored for 30 days and data is encrypted at rest and in transit internally. ChatGPT will not share information externally but will train the model on personal inputs for optimization.”
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 system collects user credentials from federal employees and contractors to support authentication, compliance, and access control. ChatGPT will not share information externally but will train the model on personal inputs for optimization.
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://chatgpt.com/
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 purpose is to provide natural language processing and AI-based text generation to assist users with drafting content, researching, summarizing, learning, and analyzing. The site is a public facing website. HHS users will need to login using their HHS email address and then will be logged in through Single Sign-On (SSO).
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by 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.	Other technology - Does Not Collect PII
PTA 12B:	What other technology is used?	None
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?	Yes
PTA 14A:	Is the mobile application HHS developed and managed or a third-party application?	Third-party
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.	The purpose of the mobile app is similar to the website - to provide natural language processing and AI-based text generation to assist users with drafting content, researching, summarizing, learning, and analyzing. The mobile app is accessible by the public, but HHS user credentials will be required to login. Once made available to HHS users, the mobile applications will be downloadable through the Company Portal mobile app on GFE devices.
PTA 16:	Does the mobile application have a privacy notice?	Yes
PTA 17:	Does the mobile application contain links to non-federal government websites external to HHS?	Yes
PTA 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	No
PTA 18:	Does the mobile application use measurement and customization technology?	Yes

PTA 18A:	Describe the type(s) of measurement and customization technologies or techniques in use in the mobile application and what information is collected.	Analytics (cookies/SDKs) to measure usage.
PTA 19:	Does the mobile application have any information directed at children under the age of thirteen?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	Yes
PTA 21A:	What are the AI tools and how are they used?	AI-based text generation to assist users with drafting content, researching, summarizing, learning, and analyzing. The site is a public facing website. HHS users will need to login using their HHS email address and then will be logged in through Single Sign-On (SSO). Analytics (cookies/SDKs) is used to measure usage.

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
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.	50,000 – 99,999
PIA 25:	For what primary purpose is the PII used?	The PII is used to create user accounts and to control system access. The system collects basic contact and employment information about federal employees and contractors to support authentication, compliance, and access control. AI known use cases include: Drafting; Editing; Summarization; Brainstorming; Meeting Prep; Explaining Concepts; Comparative Analysis; Policy & Compliance Guidance; Data Exploration; Interactive Learning; Quiz & Exam Prep; Simulation; Speech/Presentation Writing; Translation; Content Creation; Code Assistance; Documentation; Automation Guidance; Storytelling; Idea Generation; Visualization Support; Scheduling Help; Wellness & Self-Reflection. ChatGPT will not share information externally but will train the model on personal inputs for optimization. Although ChatGPT is not designed to collect PII, users on the privacy guidelines and the rule of behavior set future AI use cases that introduce new privacy risks.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None
PIA 28:	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 29:	Are records in the system retrieved by one or more PII data elements?	No
PIA 30:	Identify the sources of PII in the system.	Government Sources 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.	The collection of information from employees does not require Paperwork Reduction Act clearance.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	For user credentials for employees and contractors: Users may not opt-out of the collection or use of the PII as it is a condition of employment or contract agreement and used for account creation and to control system access.
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 provide consent as a condition of employment or other agreement to access the system. If relevant changes were to occur, they could be communicated using the account.
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any Office of the Chief Information Officer (OCIO) Office of Operations (OPS) system, may contact the OCIO-OPS Service Desk to create an incident ticket to investigate and mitigate the issue.
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.	Accuracy is ensured by individual review at the time of account creation. Users may correct or update their information to ensure that their PII is relevant and necessary to be granted access to the system. This is done via a current employee form in the Service Now Catalog
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 will have limited access to PII in the system for day-to-day communications & work functions. Administrators will have access to PII in the system to operate and maintain system. As well as, to provision, de-provision and maintain accounts within Azure Cloud Services (ACS). Contractors will have access to PII in the system as all Contractors are Direct Contractors as they are the primary personnel that serve as administrators of ACS. As ACS administrators they will be using the collected PII to create, manage and remove the accounts.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Only Administrators may access/alter PII. At the time of initial employment, new staff, (including direct contractors) that will be designated HHS Generative Pre-trained Transformer (HHSGPT) administrators are required to have a Tier 5 investigation or better on file. Once their Tier 5 has been adjudicated the new HHSGPT administrator is required to complete the following: Read and sign the HHS Rules of Behavior for users. Read and sign the HHS Rules of Behavior for elevated users. Complete information security awareness training for IT Administrators. (Pass accompanied quiz with an 80% or better. Administrators that fail to the meet 80% requirement will be required to retake training and retake the quiz. HHSGPT administrators must annually re-certify the training.) Submit and be approved for an elevated account. Submit for and receive an Alternate-Personal Identity Card (ALT)- Personal Identity Verification (PIV).
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.	Least privilege concepts are applied to the environment to help ensure that administrators only have the minimum required access needed to properly perform their job functions. Administrators have the least privileged account necessary to process data while limiting them in performing other unnecessary tasks such as installing software or modifying system configurations. These concepts follow the tenets outlined by applicable system security plan(s).

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 employees and contractors must have or completed the following before initial access is granted to HHSGPT: Have an adjudicated clearance on file. Read and sign the HHS OCIO Rules of Behavior Complete the HHS IT security brief or their agency's/OPDIV's equivalent. All users will have 1 of 3 roles assigned within HHSGPT; User, Manager, and Administrator. Base on the role assigned, the user must complete certain types of training on an annual basis to maintain network access. For Users: HHS security training for users. HHS privacy awareness training. For Managers: HHS security training for users HHS security training for managers HHS Privacy Awareness training For Administrators: HHS Security Training for users HHS security for administrators
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	N/A
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).	ChatGPT currently only maintains the minimum necessary PII to allow system access. OCIO Ops uses the following records schedule: General Records Schedule (GRS) 3.2: Information Systems Security Records. 030, System access records. General Records Schedule (GRS) 3.1: General Technology Management Records. 010, Information technology development project records. General Records Schedule (GRS) 3.1: General Technology Management Records. 011, System development records. GRS3.1 10 & 11 records are maintained in SGRC Archer (Security Governance, Risk and Compliance), 5 years after the system is decommissioned.

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.	Administrative: Access to PII is permitted only through authorization by the OCIO Ops Information Privacy & System Security Officers (IPSO), after all required forms are signed, confidentiality training performed and request for ALT-PIV has been processed. Technical: Elevated access in HHSGPT is managed through Microsoft Active Directory utilizing the "least privilege" concept. All employees and contractors must have valid ALT-PIV credentials with specific access assigned. Physical: All PII is securely stored within the Enterprise Network Management System (ENMS) data centers. The ENMS data center facilities maintain physical access controls at all entry/exit points equipped with a card scanner/personalized pin code). In the event the individual is not a current authorized user, a security guard may grant access to the facility where there is a holding room for proper identification and authorization.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	8/28/2025
Privacy Analyst Review Comments:	This PTA/PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	8/28/2025
SOP Review Comments:		**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	8/29/2025
Agency Privacy Analyst Review Comments:		**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	8/29/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
8/29/2025 11:43 AM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				