Privacy Impact Assessment (PIA): OS - OUW - QTR1 - 2025 - OS2504917

Created Date: 4/18/2025 5:04 PM Last Updated: 5/7/2025 10:25 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 - OUW - QTR1 - 2025 - OS2504917	**PIA ID:**	3041432
Name of Component:	OS - OASH Unified Web	**Name of ATO Boundary:**	OASH Unified Web
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	41
Submission Status:	Submitted	**Submit Date:**	4/25/2025
Next Assessment Date:	N/A	**Expiration Date:**	5/6/2028
Office:		**OPDIV:**	OS
Security Categorization:	Moderate	**OpDiv PIA ID:**	OS2504917
Legacy PIA ID:		**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?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	9/13/2027
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 Office of the Assistant Secretary for Health (OASH) Unified Web (OUW) cloud environment is an HHS FISMA-Reportable Major Application that is publicly accessible. OUW has an OASH Landing page and with current and future links to the thirty (30+) OASH websites. The OASH websites will be migrated in phases within the OUW boundary as Minor Applications. The OUW boundary consist of a backend Unified Web Drupal Web Content Management System (CMS) infrastructure environment that is hosted in the HHS Cloud-based Managed Application Hosting Center (C-MAHC) GSS. The HHS C-MAHC is hosted in the Amazon Web Services (AWS) US East/West FedRAMP Moderate IaaS (FedRAMP Package ID: AGENCYAMAZONEW) cloud environment.

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.	For the OUW Major Application: Non-privacy Information about OASH, Careers, and Grants & Agreements. The information is stored as long as it is current. For example, as Career information changes the information would be updated. System infrastructure and web application logs are retained for a minimum of 365 days or as required for any investigation or other operational requirement that may occur. For the ODPHP Web Site Minor Application: Organization name, location, website, and submitter's contact information (e.g., name, email, phone number). ODPHP will hold PII data in Salesforce for 5 years, reviewing the data as needed. If the contract with Salesforce is terminated, all PII will be deleted from the Salesforce application. System infrastructure and web application logs are retained for a minimum of 365 days or as required for any investigation or other operational requirement that may occur. For the OWH Web Site Minor Application: Email addresses; System infrastructure and web application logs are retained for a minimum of 365 days or as required for any investigation or other operational requirement that may occur. For the ORI Web Site Minor Application: • Information about Office of Research Integrity (ORI)'s organization, purpose, history, missions, policies and regulations, and contact information. PII in this information contains leadership's names and titles. (Permanent) • Integrity oversight materials – guidance on handling research misconducts, and downloadable forensic tool, (Permanent) • Education on research integrity materials – resources on all research integrity and research misconduct topics. These educational contents are provided as web pages, videos, interactive videos, PDFs, zip packages, or external links. PII in this information contains some authors' names. (Permanent) • Assurance program – policies and procedures for institutions. PII in this information contains ORI Assurance Specialist's contact information. (Permanent) • Case Summaries – posting of cases in which administrative actions were currently imposed to respondents due to findings of research misconduct. PII in this information contains respondents' names. (Remove as it reached end date of administrative actions) • ORI Update – updates on ORI website or any ORI related announcements (10 years)

PTA - 5A:	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. The system providing credentials is
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.	For the OUW Major Application: Non-privacy Information about OASH, Careers, and Grants & Agreements. No information is collected on individuals. For the ODPHP Web Site Minor Application: Organization name, location, website, and submitter's contact information (e.g., name, email, phone number) is collected in order to notify the organization whether its application was approved and, if approved, to enter into a Letter of Understanding with the organization, send it a digital NYSS Champion badge, (and include its email address in a mailing list to receive, e.g., notifications about new resources) For the OWH Website Minor Application: Access to GovDelivery (for customers and internal support personnel) is through the administration console. Email address information and access date/time are collected, for reasons of documenting system access and date/time for that access. Sending of bulletins is also logged for the purposes of being able to audit activities in the system at a later date. For the ORI Web Site Minor Application: The website does not collect any information to share with another system. The information is public accessible for monitoring institutional compliance per regulation as stated in PHS Policies on Research Misconduct 42 C.F.R. Part 93 and 42 C.F.R. Part 50, Subpart A.
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)?	Yes

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.	For the OUW Major Application: To provide information on the following: Information about OASH, Careers, and Grants & Agreements. Public users have access to the system because will be publicly accessible. For the ODPHP Web Site Minor Application: Data received in the sports@hhs.gov email mailbox gets embedded in the health.gov Drupal site as a web form that will post back to the Salesforce server. The public does not actually view or interact with the Salesforce TPWA. Data received on health.gov will post back to the salesforce server. For the OWH Web Site Minor Application: The OWH public websites is managed using Drupal. All health content and resources are maintained, updated, and archived in accordance with OWH's annual editorial calendar. The health content maintained throughout the OWH websites is expert reviewed and cleared through the HHS Assistant Secretary for Public Affairs (ASPA) before being posted on the public sites. All other content pertains to OWH initiatives and health observances and is reviewed by OWH senior leadership before being promoted to production. For the ORI Web Site Minor Application: The purpose of the website is to provide the public information about ORI, its missions, policies and regulations, programs, and resources for the constituents. The URL for the website is https://ori.hhs.gov
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?	Yes
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?	Yes
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 Phone numbers Mailing Address Other - Free text Field - IP Address
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Members of the public
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?	For the Office of Disease Prevention and Health Promotion (ODPHP) Web Sites Minor Application hosted within the OASH Unified Web (OUW) Major Application System the Primary Purpose for the PII used: Registration for online events, registration for National Youth Sports Strategy Sponsors and Champions. ODPHP Web sites include resources such as public blogs and allow individuals to volunteer to make informational posts. Contributors must first apply and are granted access if they are able to supply a valid e-mail account. They may then choose to make postings, which will include their names and organizations along with the information or ideas posted. Emails are used for informational purposes only to contact interested recipients with blog and website updates. Individuals are not required to sign up for email updates. For the Office of Women's Health (OUW) Web Sites Minor Application hosted within the OASH Unified Web (OUW) Major Application System the Primary Purpose for the PII used: The application uses multifactor authentication to verify only privileged user identity. This includes the user's email address, password, and an approved Internet Protocol (IP) address.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	They are no secondary uses for which the PII will be used (e.g. testing, training or research) for the ODPHP Web sites and OWH Minor Applications hosted within the OASH Unified Web (OUW) Major Application System.
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.	For the ODPHP Web Site has been migrated within the OUW cloud major application and the legal authority is: It was established by the National Consumer Health Information and Health Promotion Act of 1976 (Section 1706 of the Public Health Service (PHS) Act as amended) and continued under the "Omnibus Health Act of 1988," was mandated a number of responsibilities, including participation in policy development; oversight and coordination of HHS activities in disease prevention and health promotion; identification of unmet needs related to health information and disease prevention and development of resources to meet such needs; and dissemination of health information. For the OWH website has been migrated within the OUW cloud major application and the legal authority is: 5 USC 301, Departmental Regulation
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.	The ODPHP and OWH websites are not covered by a separate PIA. With the migration into the OASH Unified Web (OUW) Cloud environment, the PIA for these sites is a part of the OUW PIA. The ODPHP Web Site Minor Application uses the following PII data elements are used to retrieve records: Name, Organization name, email. The OWH Web Site Minor Application uses the following PII data elements are used to retrieve records: Email addresses and user credentials User credential (HHS.gov email) account information from the privileged accounts C-MAHC AWS IAM granted access to the OUW Drupal Content Management System (CMS) is used for Signal SignOn (SSO) and retrieval by the HHS Access Management System (AMS) to provide the phishing-resistant Multifactor Authentication (MFA) for privileged users to access the OUW backend Drupal Content Management System (CMS).
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.	The ODPHP Web Site Minor Application SORN is: Persnl. Rcrds. in Operating Offices 09-90-0018 The OWH Web Site Minor Application SORN is: N/A
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online
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 ODPHP Web Site Minor Application: The Office of Management and Budget (OMB) Information collection approval may not be required because only contact information is requested to enable the system to provide a login to the subscriber to HealthyPeople or for the content syndication component of HealthFinder. Applicant information is properly discarded after it is reviewed. We are working with the Paperwork Reduction Act Officer to confirm if an OMB Information collection approval number and expiration date is needed. The OWH Web Site Minor Application: N/A- This is not applicable because Office on Women's Health (OWH) is not using any information collection instruments, such as surveys or questionnaires, that would require Office of Management and Budget (OMB) approval.

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.	
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.	The ODPHP Web Site Minor Application: Individuals are aware of what PII is being collected because, in all instances where PII is collected, the data subjects submit their PII themselves and is not Individuals are aware of what PII is being collected because, in all instances where PII is collected, the data subjects submit their PII themselves and is not shared or used for any purpose other than the purpose for which the information is submitted. Individuals who submit PII, submit their PII with the intent of having it be used in this way. In the course of using the system, individuals are supplied with privacy, security, and Freedom of Information Act (FOIA) disclaimers. Users can opt out of submitting their information by not signing up for login access. The access is not required to access any publicly facing portion of the site and is only necessary to submit stories to be displayed on the site. Stories submitted consist of: Data related to ODPHP HealthyPeople (HP) work and comments on quality of the data collected. Relevant materials that demonstrate the HP program's activities. Relevant image files - Stock photos are used on the live website. The user is allowed to submit pictures and other information for review. Once the story is submitted, it goes to the ODPHP vendor staff person who edits and rewrites large portions of the story and turns it into a publicly available story from the field The OWH Web Site Minor Application: The online form tells users that they are submitting their email address to receive more information about a specific health topic from Office on Women's Health. The user has the option to call OWH as well if they prefer not to provide their PII.

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.	The ODPHP Web Site Minor Application: The data subjects submit their PII themselves and it is not shared or used for any purpose other than the purpose for which the information is submitted. No major changes to the system that would affect the way in which the information is used are anticipated. Individuals provide their contact information because they wish to use the system to learn and share information. That is the only reason for which the information is collected. If a major change were to happen to the way that user's personal information is used, then those users would be notified ahead of time through email to confirm their willingness to display their information The OWH Web Site Minor Application: If a major change were to occur, the Office on Women's Health would notify users via their e-mail and obtain their consent before using their email addresses in some other way.
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.	The ODPHP Web Site Minor Application: If users believe their information has been misused in any way, contact information for the system owner is provided. Additionally, the FOIA Appeals Process point of contact's information is provided in the footer of every Web site. The OWH Web Site Minor Application: All messages to individuals include several ways for people to get in touch with the OWH. People may email or call OUW's help desk (toll-free number) for OWH Website question, or unsubscribe. The unsubscribe function is automated, through OWH's email address and help desk are monitored by full-time, dedicated staff.
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.	The ODPHP Web Site Minor Application: Information is submitted by the data subjects themselves, and is therefore, assumed to be accurate. Any suggestion made by a member of the public that information was inaccurate would be investigated and altered appropriately. The OWH Web Site Minor Application: Web Content Management System (application): The application inherits HHS rules for password complexity, longevity, and login attempts, thus ensuring credential integrity. All accounts are granted and removed under the sole authority of the system owner, ensuring that all active accounts are both accurate and relevant.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors Third-Party Contractor (Contractors other than HHS 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.	The ODPHP Web Site Minor Application: The ODPHP website system is Government Owned/Contractor operated. The web content is managed by a web application administrator/developer contractors and access to relevant PII is necessary to assist ODPHP with the management of information for the ODPHP website. The OWH Web Site Minor Application: The OWH website system is Government Owned/Contractor operated. To create, review, and distribute OWH news announcements and manage website content. The web content is managed by a web application administrator/developer contractors and access to relevant PII is necessary to assist OWH with the management of information for the OWH website.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The ODPHP Web Site Minor Application: ODPHP Staff work closely with contract staff on each area to determine appropriate access. Public comments and blog posts are reviewed and moderated by agency staff prior to publication. Administrators review submissions regularly and approve new entries for public display on the website as appropriate. The OWH Web Site Minor Application: Access to The Office on Women's Health (OWH) account is limited to federal employees who are responsible for the creation, review and distribution of OWH news announcements, and for the management of website content.
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.	The ODPHP Web Site Minor Application: Only website administrators have access to PII such as email contact information to follow up with individuals related to the content or posting of their blog posts. Specific admin roles are setup in Drupal to ensure that only the appropriate administrators have access to information. For example: the administrator role for stories from the field stories only has access to Stories from the Field related user submissions. The OWH Web Site Minor Application: Web Content Management System (application): The application supports multiple user role and granular permissions, based on role. The system owner controls how and to whom roles are assigned. Thus, people who only need to edit and create content cannot make other changes within the application; nor can they view information about other users. Only the application owner and system administrator can access all of the data in the application.

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.	The OUW Major Application complies with the security training requirements set by the HHS Office of Information Security. All System users maintaining the OUW System and Minor Application websites (ODPHP, OWH) are required to take annual on-line training for Privacy Awareness, general Information Systems Security Awareness.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	In addition, the HHS Learning Management System (LMS) provides the following Role Based Information Training for OUW users with privileged access to HHS IT systems: Introductory Role-Based Training for IT Administrators Part 1; Rules of Behavior for Privileged Users - Part 2. Privileged Users are also required to sign a Rules of Behavior (PRoB) form.
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 ODPHP Web Site Minor Application: 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. The OWH Web Site Minor Application: User Credentials retention schedule: 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 - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	The OUW servers (which includes the ODPHP and OWH websites) hosted in the HHS C-MAHC AWS US East/West location employs multiple levels of perimeter protection to prevent unauthorized access and information disclosure. All PII collected resides on servers in a secured facility. The system undergoes an annual Certification and Accreditation review, as well as Security Testing & Evaluation of all sites and servers every 3 years. All remote server access is restricted to an "as needed" basis and is password protected. Access to the building that houses the HHS C-MAHC environment in the AWS US East/West Data Center is restricted to authorized employees, and access to the Data Center itself is restricted further. Only government credentialed personnel with specific access to the Data Center may enter the facility, all access is logged and monitored. Access to the OUW servers that store PII are restricted to HHS authorized Virtual Private Network (VPN) users, who have been granted access to the OUW cloud environment. All OWH servers and Web sites are monitored for unauthorized access attempts, there are procedures in place to address any such findings. Additionally, only OUW administrators are allowed to connect and interact with the servers. Administrator accounts are strictly monitored and reside on an Active Directory controller specific to the OUW cloud environment. All personnel who have access are required to pass HHS privacy training. Administrative controls: Site administrators receive regular training in security rules and procedures for protecting PII. This training must be completed on an annual basis. Technical controls: Usernames and passwords utilizes hashing for encryption. User accounts are automatically locked after 60 days of inactivity. User accounts are logged off of the site after 15 minutes of inactivity. Physical controls: Our hosting solution provides physical security including video surveillance, biometric security, and round-the-clock onsite guards.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/30/2025
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:**	5/5/2025
		SOP Days Open:	10

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/6/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 5/6/2025 All comment seems to have been addressed. This PIA is ready for SAOP review and approval. 4/25/2025 Please see comment and update accordingly: Q3: what is the ATO Date? On the next iteration of the PTA update the following: PTA-5: please remove the bullet points for 508 compliance. Include Mailing address and IP address in your response. PTA-6: Spell out NYSS. PIA-1: Please remove User Credentials per PTA-5A User Credentials are not maintained in this system. • Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is: C-MAHC AWS IAM for OUW privileged accessing OUW front-end servers/service accounts with authentication using User Name and password. AMS for OUW privileged users accessing the OUW backend Drupal Web Content Management System (CMS). Public users do not require credentials to access the publicly available site PIA-8A: Are these websites covered by a separate PIA? How are user credential use for retrieval when this system doesn't store or maintain user credentials. PIA-18: Please provide the reason why these roles have access to PII in the system • Users • Administrators • Developers • Contractors	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	5/7/2025
		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	VILLAFUERTE, NESTOR	4/23/2025	Q3 states that the system does not have an ATO; the ATO date stated has passed. On the next iteration of the PTA, please remove the bullet points on PTA-5 for 508 compliance. Please define NYSS in PTA-6. PIA-1: IP Addresses were not mentioned in the PTA.	
PIA - 1	BLAND, CRYSTAL	4/25/2025	In the next iteration of the PTA update the following: PTA-5: include Mailing address and IP address in your response.	
PIA - 1	BLAND, CRYSTAL	4/25/2025	PIA-1: Please remove User Credentials per PTA-5A User Credentials are not maintained in this system. • Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is: C-MAHC AWS IAM for OUW privileged accessing OUW front-end servers/service accounts with authentication using User Name and password. AMS for OUW privileged users accessing the OUW backend Drupal Web Content Management	

			System (CMS). Public users do not require credentials to access the publicly available site
PIA - 8A	BLAND, CRYSTAL	4/25/2025	Are these websites covered by a separate PIA? How are user credential use for retrieval when this system doesn't store or maintain user credentials.
PIA - 18	BLAND, CRYSTAL	4/25/2025	Please provide the reason why these roles have access to PII in the system • Users • Administrators • Developers • Contractors

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:	5/7/2025 10:25 AM	**History Log:**	**View History Log**