Privacy Impact Assessment (PIA): CDC - SEAD3-SRS - QTR1 - 2024 - CDC8049210

Created Date: 3/21/2024 4:02 PM Last Updated: 9/30/2024 8:01 PM

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:	CDC - SEAD3-SRS - QTR1 - 2024 - CDC8049210	**PIA ID:**	1788411
Name of Component:	CDC - SEAD 3 Self Reporting System	**Name of ATO Boundary:**	SEAD 3 Self Reporting System
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	64
Submission Status:	Re-Submitted	**Submit Date:**	3/26/2024
Next Assessment Date:	N/A	**Expiration Date:**	5/23/2027
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8049210
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

1:	Identify the Enterprise Performance Lifecycle Phase of the system.	Disposition
2:	Is this a FISMA-Reportable system?	Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	4/30/2024
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	None
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.	Security Executive Agent Directive 3 (SecEA) establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. This system, the Security Executive Agent Directive 3 Self Reporting System (SEAD3-SRS), enables covered CDC and HHS personnel to self-report required travel, financial, and other activities required by the United States' Security Executive Agent Directive 3.

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.	SEAD3 will include travel itinerary, passport information, planned contacts and their personal contact information, description of foreign activities (i.e., business involvement, financial, passport, political involvement, citizenship, and foreign owned property information), adoption of non-U.S. citizen children, reports on suspicious contacts who may be attempting to obtain classified information, media contact, arrests, personal financial anomalies, co-habitation, marriage, alcohol/drug related treatment. The PII elements collected and maintained are: Name Email Address Phone Number Medical Notes Foreign Activities Date of Birth Mailing Address Medical Records Number Financial Account Information Employment Status Passport Number Spouse/Partner/Children Information Foreign travel/passports/property/roommates/communication with non-US citizens Interactions with the media Criminal Activity Alcohol/drug related information
PTA - 5A:	Are user credentials used to access the system?	
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.	HHS employees that maintain a position that is deemed 'sensitive' are mandated to self-report foreign activities, personal contact information such as address, phone number and emails, passport, financial information to include foreign bank accounts, adoption of non-U.S. citizen children, reporting of suspicious contracts with who may be attempting to obtain classified information and various self-reporting requirements. There are a total of nineteen (19) self-reporting requirements. This information is to be used as part of Security Executive Agent Directive 3 mandate to self-report clearance activities and changes. No individuals outside of the CDC and HHS are able to access and use the system. The PII elements collected and maintained are: Name Email Address Phone Number Medical Notes Foreign Activities Date of Birth Mailing Address Medical Records Number Financial Account Information Employment Status Passport Number Spouse/Partner/Children Information Foreign travel/passports/property/roommates/communication with non-US citizens Interactions with the media Criminal Activity Alcohol/drug related information
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No

PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	SEAD3-SRS allows CDC personnel with security clearances to report required travel, financial, and other activities required by the United States' Security Executive Agent Directive 3. Users access the website via **https://sead3-srs.cdc.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?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Foreign Activities Date of Birth Mailing Address Medical Records Number Financial Account Info Employment Status Passport Number Other - Free text Field - Medical Notes. Spouse/partner/children information. Interactions with the media. Criminal Activity. Alcohol/drug related information
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 Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	PII is used to fulfill reporting requirements pursuant to Security Executive Agent Directive 3.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	None
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	NA, SSNs are not used by this system
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	NA, SSNs are not used by this system
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Executive Orders 10450 and 12356
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.	Name Date of Birth
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.	09-90-0002, Investigatory Material Compiled for Security and Suitability Purposes
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Online Government Sources Within the OPDIV Other HHS OPDIV

PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	NA, this system does not collect information from the public
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	NA, this system does not collect information from the public
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Available data will be used to create a report to send to HHS who will use the report to create an aggregate of their reporting agencies to meet National level reporting requirements.
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)).	There are currently no agreements in place. This system is under Security Executive Agent Directive 3. HHS OPDIVs will coordinate the service level agreements between the various Physical Security departments to identify points of contacts and establish MOUs.
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.	HHS OPDIVs will coordinate the service level agreements between the various Physical Security departments to identify points of contacts and establish MOUs. In addition, HHS OPDIVs will establish agency specific procedures and disclosures.
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 PII contained within this system is required as a condition of employment as well as for those holding a security clearance, therefore there is no option to opt-out. The purpose of the system to report information for anyone with elevated security clearance. Opting out would violate the SEAD-3 directive. To opt-out the individual would have to opt out of the data collection of each individual system that SEAD-3 relies on. Opting out would mean the individual would no longer be able to perform the duties associated with their position.
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.	Individuals and users can be notified of significant changes to SEAD3-SRS via a warning banner upon login.

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.	A large portion of the PII is collected via other systems as part of the individual's in-processing with the CDC, travel planning, and background investigation. Redress will be covered under those systems if that data is found to be inaccurate. However, the reporting portion of the information is collected via the individual as a requirement for holding a security clearance and can be updated by them as needed. Additionally, Individuals may contact the Application Services branch (ASB) Help-desk or the Cybersecurity Program Office (CSPO) 770-488-8660, if they believe their PII has been inappropriately obtained. Individuals can contact the Help Desk via phone or email for additional assistance.
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.	A large portion of the PII is collected via other systems as part of the individual's in-processing with the CDC, travel planning, and background investigation. Reviews will be covered under those systems to ensure data integrity, availability, accuracy, and relevancy. However, the reporting portion of the information is collected via the individual as a requirement for holding a security clearance and can be updated by them as needed. Administrators will review the data every 365 days to ensure integrity, availability, accuracy and relevancy. The user is likewise asked to update and correct their information as well.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers
PIA - 17A:	Select the type of contractor.	
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Updating reportable information within their own records Administrators: Reviewing and creating reports to be sent to HHS as a response to SEAD3. Developers: Support application development and resolve issues.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	SEAD3-SRS uses the Active Directory to authenticate users. SEAD3-SRS will have a SEAD3 Role Based Access Control (RBAC) database that will authorize all users' privileges and access in the application. There will be a Security Specialist (system application administrator) role implemented by the SEAD3-SRS RBAC database. Only those assigned to this role will be authorized to see PII data within there assigned OPDIV.
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.	SEAD3-SRS uses a dedicated RBAC to restrict a user's ability to view PII to only that level required to perform their job function, least privilege. The roles are assigned to Security Specialist (system application administrator) and implemented by the SEAD3-SRS RBAC database. Only those assigned to this role will be authorized to see PII data within their assigned OPDIV.
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.	CDC users must undergo annual security and Privacy Awareness training. Other HHS OPDIVs are responsible for the security awareness training for their respective agencies in order to maintain their network accounts and access to SEAD3-SRS.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	In addition to annual Security Awareness Training, specific clearance training requirements, and role-based training, cleared personnel will undergo an initial clearance briefing on what is required for system use.
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).	All officials' records are transferred or destroyed based on CDC record management policies and practices. The following records schedules apply to the system: GRS 5.2 Input/Source Records - uncalibrated or unvalidated observational data. When verified in new final record. GRS 5.2 Input/Source Records - uncalibrated or unvalidated from another agency When verified in new final record.

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.	Administrative: Records will be maintained according with CDC's record control schedule and record control policy. In addition, the application will follow GRS 3.1 specifically. The PII is secured using the CDC/IS Active Directory authentication process and RBAC. Technical: Monitored by the Network and IT security controls which is administered by Cybersecurity Personnel Office (CSPO) and Digital Services Office (DSO). Information is exchanged with HHS across an encrypted Secure File Transfer Protocol (SFTP) connection. Physical: Controls are managed by guards, ID badges and key card restrictions.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	4/1/2024
Privacy Analyst Comments:	OpDiv Privacy Analyst: Joshua Mosios Status: Approved Date: April 1, 2024	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	4/30/2024
		SOP Days Open:	35

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/2/2024
Agency Privacy Analyst Review Comments:	Reviewer: James Laskowski 5-2-2024 Confirm responses for PTA-5A, PTA-5-B see exported PIA in Supporting Doc. Will need to include note about URL. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Confirm responses for PTA-5A, PTA-5-B see exported PIA in Supporting Doc. The reviewer notes that the URL in PTA9 was not accessible.	**SAOP Review Date:**	5/23/2024
		SAOP Days Open:	21

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Copy_of_SEAD3-SRS Privacy_Impact_Assessment_PIA_bl (7).rtf	211379	.rtf	5/2/2024 8:46 AM	1

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 24	Data Feed Service, piafrmcdc	3/21/2024	GRS 20 has been superseded Old GRS 20 Superseded (archives.gov)	
PIA - 8A	Data Feed Service, piafrmcdc	3/21/2024	Please confirm that all these elements are used to **retrieve information about an individual**. Per the SORN "Retrievability: The records are alphabetically indexed by name and date of birth of the individual subject of the file or by cross reference to another file. Access within HHS is limited to the Secretary, and on a need-to-know basis to other Department officials having program management responsibility."	
PIA - 1	LASKOWSKI, JAMES	5/1/2024	Please respond to PTA 5A/5B. The reviewer notes that the URL in PTA9 was not accessible.	
PIA - 1	Data Feed Service, piafrmcdc	9/30/2024	This System has been migrated within the OCIO ISB Infrastructure Services authorization boundary. All future updates should be made via the new Sub- Component application.	

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:	9/30/2024 8:01 PM	**History Log:**	**View History Log**