Privacy Impact Assessment (PIA): CDC - eFSAP Cloud - QTR3 - 2023 - CDC6795171

Created Date: 7/28/2023 2:09 PM Last Updated: 10/2/2024 12:02 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:	CDC - eFSAP Cloud - QTR3 - 2023 - CDC6795171	**PIA ID:**	1683505
Name of Component:	CDC - electronic Federal Select Agent Program - Cloud	**Name of ATO Boundary:**	electronic Federal Select Agent Program - Cloud
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	440
Submission Status:	Re-Submitted	**Submit Date:**	9/20/2024
Next Assessment Date:	10/01/2027	**Expiration Date:**	10/1/2027
Office:		**OPDIV:**	CDC
Security Categorization:	High	**OpDiv PIA ID:**	CDC6795171
Legacy PIA ID:		**Make PIA available to Public?:**	Yes

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)?	Yes
4:	ATO Date or Planned ATO Date.	11/9/2024
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.	No changes to system; annual assessment.
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.	eFSAP is a joint Centers for Disease Control and Prevention (CDC) and United States Department of Agriculture (USDA) Agriculture Select Agent Services (AgSAS) system is designed to control, protect, and store the use, possession and transfer of Select Agents and Toxins. eFSAP maintains information regarding an entity's Select Agent registration. It replaced the Select Agents and Toxins Regulatory Network (SATRN) system. The system allows entities to enter information regarding implementing, and enforcing the Select Agent Regulations Data is a national databased that documents, identifies, manages, and inspects entities that possess, use, or transfer select agents.

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.	eFSAP collects information regarding an entity's Select registration: facility information; a list of select agents or toxins to be possessed, used, or transferred by the entity; individual(s) who will have access to select agents and toxins; It also tracks assessments and inspections results of each entities compliance to regulations. For staff that will accessing select agents there is a clearance process that is required to ensure safety. This process collects the individuals name, their DOB, email addresses, phone numbers and what they will have access to. This PII data is provided to Criminal Justice Information Service (CJIS) to have them verify if a person is cleared to access information and agents. Users will access the system using a user name/password or a Health and Human Services (HHS) Personal Identity Verification (PIV) Card; these credentialings will be stored via the CDC Secure Access Management System (SAMS), a separate access control system with its own Privacy Impact Assessment (PIA). SAMS Authenticates all users and validates they are approved to access eFSAP Activity. User accounts and passwords are therefore not stored in the system.
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.	eFSAP collects information regarding an entity's Select registration: facility information; a list of select agents or toxins to be possessed, used, or transferred by the entity; individual(s) who will have access to select agents and toxins; It also tracks assessments and inspections results of each entities compliance to regulations. The information collected includes name, date of birth, email address, phone number, and entity (business) address. Name - Used for background check by individuals that will have access to select agents and toxins. Date of birth - Used for background check by individuals that will have access to select agents and toxins. Email address - Communicate with individuals requesting access and for SAMS access. Phone number - Communicate with individuals requesting access and that have access to select agents and toxins. Business (entity) address - Physical address is required for facility inspections of entities that have access to select agents and toxins.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	
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.	Users will access the system using a user name/password or a Health and Human Services (HHS) Personal Identity Verification (PIV) Card; these credentialings will be stored via the CDC Secure Access Management System (SAMS), a separate access control system with its own Privacy Impact Assessment (PIA). SAMS Authenticates all users and validates they are approved to access eFSAP Activity. User accounts and passwords are therefore not stored in the system.
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?	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.	
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 Date of Birth
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The PII is used to assist in identifying an individual for the Federal Bureau of Investigations (FBI) to conduct background checks and to contact the facility.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	N/A
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	N/A
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	N/A

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and The Agricultural Bioterrorism Protection Act of 2002 (Pub. L. 107-188).
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 and email address
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.	09-20-0170 Electronic Federal Select Agent Program Portal (eFSAP Portal)
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Other Federal Entities Non-Government Sources Private Sector Other
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB NO. 0920-0576. OMB is currently reviewing our forms. New expiration date will be given once process has completed.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	1/31/2024
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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.	Other Federal Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Animal and Plant Health Inspection Service (APHIS) and Criminal Justice Information Services (CJIS) for compliance with federal mandates.
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)).	Interconnection Security Agreement, between USDA/APHIS; and HHS/CDC MOU among CDC, APHIS, and CJIS.
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.	Disclosure of any eFSAP records is processed through managerial written/approved procedures. Requests for disclosures are processed and maintained using a SharePoint WorkFlow. An accounting of disclosures is produced by a review of signed transmittal documents.
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.	Submission of PII is required. A Security Risk Assessment is necessary for those individuals identified as a Responsible Official (RO), Alternative Responsible Official (ARO), owners of non-governmental entities, and individuals who want to have access to select agents or toxins. Access to the system may be denied if there is insufficient information to conduct a Security Risk Assessment.
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.	Notification of any major changes to the system are posted on the Select Agents Web Site as "Select Agent (SA) Grams".
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 process to be followed in the event an individual has concerns regarding the use/accuracy/disclosure of his/her PII is as follows: The user may contact the Business Steward in writing via the following address: Director, Division of Regulatory Science and Compliance (DRSC), Office of Readiness and Response, CDC, 1600 Clifton Rd. NE, Atlanta, GA 30329, (404) 718-2000, lrsat@cdc.gov. Individuals must reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons that the PII is inaccurate for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.
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.	There is an established quality control check of eFSAP. The individual's information is checked/rechecked at one of the various points below: 1. Individuals access and data are verified through SAMS and their renewal process. 2. Entity information is reviewed at the registration(1st year), major Amendments (as submitted), and renewals (3 year) 3. Entity Responsible Officials (ROs) have their Admin dashboard allowing them direct ability to see who has access to their information and can request changes as need 4. We also perform a quarterly review of our users by comparing SAMS access list to User List within eFSAP to validate accounts/users.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv 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.	Users - Initial Data Entry Administrators - Production Operation and Maintenance to fix/update logic. Developers/Contractors - These are direct contractors with access to Production Operation and Maintenance to fix/update logic that cannot be resolved locally.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	There is an established Standard Operating Procedure (SOP) in place that provides instructions for all users to complete. This SOP requires an access request form to be completed and approved along with a completed Rules Of Behavior (ROB). The form and ROB must then go through a review, validation and approval process prior to a user ever obtaining access. A user completes the Access request form request access to eFSAP, role(s) being requested, and their justification as to why they believe access is needed. Role-Based Access (RBAC) is used to determine who may access the system and its PII. The form is is then provided to a Full-Time Equivalent (FTE) within the eFSAP program who can validate the need and justification for access to the role(s) selected. Validated forms are then provided to the System Security steward who will review the form to ensure it is completed correctly. Once reviewed for completeness, the security steward contacts the Office of Safety, Security, and Asset Management (OSSAM) to ensure the proper clearance levels based on roles the user has been approved for. If the form is complete and all required clearances are in place, a request is submitted to the System team to have the account and access granted. If not, the forms are returned to the requester and the FTE validator noting the reason(s) why access can not be granted.

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 established SOP defines roles and they are assigned based on approval and justification of access. The least privilege model is used to determine who may access the system and PII. The system is designed to have role based restrictions to include System Administrator, Agency User, Entity User, Read only, etc. Each role has restrictions. Ex. Entity User is only able to see their individual information. Read-only allows for viewing only. Agency User is an internal CDC or USDA partner user who requires set clearances in order to gain access.
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.	All individuals are required to show a certificate of completion for and mandatory Security and Privacy Awareness Training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	System stewards (Business, Security & Designated Approval Authority(DAA)) must undergo additional Role Based Training. Users must be verified by the DRSC process and sign the eFSAP Rules of Behavior.
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).	Data will be maintained in accordance with the National Archives and Records Administration (NARA) complainant file retention and destructive plans. The Division of Select Agents and Toxins Records retention schedule DAA-0442-2019-0001-0003. The PII will be retained for 10 years.

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 -- eFSAP stores data in password protected databases hosted in Azure Fed Ramp Government Cloud. Additional Administrative controls are in place to protect PII with Rules of Behavior, training, notifications, and disclosures. All individuals are required to show a certificate of completion for mandatory Security and Privacy Awareness Training. System stewards (Business, Security & Designated Approval Authority(DAA)) must undergo additional Role Based Training. Users must be verified by the DSAT process and sign the eFSAP Rules of Behavior. Technical -- Technical Controls are in place with the Cybersecurity Program Office (CSPO) and Digital Services Office (DSO), Logical access barres include Access Control Lists, Active Directory Federation Services (ADFS) Accounts/groups, and Intrusion detection. Physical -- Physical controls for CDC are in place through the Office of Safety, Security, and Asset Management (OSSAM) including guards, smart-card, and Closed Circuit TV. Microsoft Azure facilities server locations also maintain Guards, Access card controls, and Closed Circuit TV. Microsoft also designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where data is stored. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	9/20/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker	**SOP Review Date:**	9/20/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	9/24/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 9/24/2024 Per CDC email (see Supporting Documentation) the current ATO Planned date is 11/9/2024 and PTA-7 is "Yes." All comment have been addressed. This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	4

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	9/24/2024 Per CDC email (see Supporting Documentation) the current ATO Planned date is 11/9/2024 and PTA-7 is "Yes." All comment have been addressed.	**SAOP Review Date:**	10/1/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
Re_ CDC - eFSAP Cloud - QTR3 - 2023 - CDC6795171.pdf	247765	.pdf	9/24/2024 1:31 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 21	Data Feed Service, piafrmcdc	9/20/2024	How often is the training required?	
PIA - 21	Data Feed Service, piafrmcdc	9/20/2024	The annual Security Awareness Training by OCIO. I've updated the original response to reflect.	
PIA - 1	VILLAFUERTE, NESTOR	9/23/2024	Reviewer notes PTA-7A failed to sync Please remove response to PTA-14A as the system does not have a mobile 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:	10/2/2024 12:02 AM	**History Log:**	View History Log