Privacy Impact Assessment (PIA): FDA - FSMA108 - QTR4 - 2024 - FDA4563755

Created Date: 10/30/2024 8:27 AM Last Updated: 11/13/2024 1:48 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:	FDA - FSMA108 - QTR4 - 2024 - FDA4563755	**PIA ID:**	2386096
Name of Component:	FDA - HFP Food Safety Modernization Act 108	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	15
Submission Status:	Submitted	**Submit Date:**	11/5/2024
Next Assessment Date:	N/A	**Expiration Date:**	11/13/2027
Office:		**OPDIV:**	FDA
Security Categorization:	Moderate	**OpDiv PIA ID:**	FDA4563755
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
4:	ATO Date or Planned ATO Date.	12/23/2022
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.	FDA has made no changes to this component since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
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.	In support of ongoing modernization efforts, the Food and Drug Administration (FDA) recently launched the Human Foods Program (HFP), an integrated and unified approach to food safety operations across FDA. The Center for Food Safety and Applied Nutrition (CFSAN) is one of three offices now aligned under the HFP. For purposes of this assessment, HFP and CFSAN are used interchangeable. The CFSAN Food Safety Modernization Act 108 Survey Collection Tool (FSMA108) is a data collection and reporting tool used to administer the National Agriculture and Food Defense Strategy (NAFDS) Survey. This is a voluntary survey of state governments (external users) intended to gauge government activities in food and agriculture defense from intentional contamination and emerging threats. The collected information will be included in the mandatory NAFDS follow-up Report to Congress. Protecting the nation's food and agriculture supply against intentional contamination and other emerging threats is an important responsibility shared by federal, state, local, tribal, and territorial governments as well as private sector partners. To access the system, state government users must first establish an account through the FSMA108 system request user account function. Survey participants are provided access to the survey via a web linked portal included via an email invitation. Once access is granted, external users are provided access to the survey only (not to FSMA 108 directly). All FSMA108 data is protected by 21 U.S.C. 301 (Federal Food, Drug and Cosmetic Act, of which the Food Safety Modernization Act of 2011 is part). CFSAN FSMA108 includes two user modules. Users of the external module include members of state governments who require a user account (username and password as well as token factor authentication) to access the system. Users of the internal module is limited to a very small group of FDA employees (permanent and Direct Contractors) serving in the role of System Administrators (Admins).

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.	CFSAN/HFP FSMA 108 collects and maintains the following personally identifiable information (PII) about FDA employees (permanent and Direct Contractors): first and last name. Non-PII data collected from internal users include job title and center name. Non-PII can become PII when combined with PII. The FDA system providing employee data is the Enterprise Administrative Support Environment (EASE) system (the subject of a separate assessment). Employee data is used to log on authorized users automatically and securely. CFSAN/HFP FSMA 108 also collects PII about external users of the system (members of state governments). PII may include: (a) first and last name; (b) work e-mail address; (c) work phone number; (d) employment status; and (e) user credentials. Non-PII data collected from external users include organization affiliation and state/province. Non-PII data collected and maintained in the system includes program evaluation, Congressional Liaison Operations and Policy and Guidance Development data. PII collected and maintained by CFSAN/HFP FSMA 108 is used primarily for communication purposes. CFSAN/FHP FSMA 108 Admins (internal users) use PII to contact FDA affiliated state agency leads regarding status of responses of their activities and activity assignments. The Admins can also contact state users if the pilot survey has not been completed. External users of the system (state government officials) require a user account (username and password as well as token factor authentication) to access the system. Users of the internal system module (FDA System Admins) access the system via system is Single Sign On (SSO) and Personal Identity Verification (PIV) enabled for internal users. The system has implemented multifactor authentication via alternate PIV cards for network access to privileged accounts. FDA employees and Direct Contractors who access or use the FSMA108 application do not use any PII to retrieve records held within the system. All records are maintained temporarily and destroyed when no longer needed or after a period of 3 or 20 years, depending on the file system, per NARA guidelines.
PTA - 5A:	Are user credentials used to access the system?	Yes
PTA - 5B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password

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.	CFSAN/HFP FSMA108 is a voluntary survey of state governments, intended to gauge government activities in food and agriculture defense from intentional contamination and emerging threats. The collected information is included in the mandatory NAFDS follow-up Report to Congress. CFSAN/HFP FISMA 108 collects the following information about FDA employees (permanent and Direct Contractors) as internal users of the system: first and last name. Non-PII data collected from internal users include job title and center name. Employee data is used to log on authorized users automatically and securely. CFSAN/HFP FSMA 108 Admins (internal users) use PII to contact FDA affiliated state agency leads regarding status of responses of their activities, activity assignments and to inquire about completion of pilot surveys. CFSAN/HFP FISMA 108 may also collect the following information about external users of the system (state government officials): (a) first and last name; (b) work e-mail address; (c) work phone number; and (d) user credentials. Non-PII data collected from external users include organization affiliation and state/province. The FSMA108 system is Single Sign On (SSO), and Personal Identity Verification (PIV) enabled for internal users. The system has implemented a multifactor authentication via alternate PIV cards for network access to privileged accounts. The FDA uniquely identifies and authenticates organizational users. For PIV authenticated system, PIV credentials are based on user's certification which are also unique. Users of the external module include members of state governments who only require a user account (username/email address and password) to access the system/survey. Users of the internal module serve as Admins and investigators (FDA permanent employees) and developers (FDA Direct Contractors). Users of the external module include members of state governments who require a user account (username/email address and password as well as token factor authentication) to access the system.
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.	The purpose of the website is to allow the state governments to report activities in food and agriculture defense from intentional contamination and emerging threats. The Food Defense and Emergency Coordination Staff then document responses as progress toward a coordinated, risk-based, and mission-critical federal food safety research strategy. The CFSAN/HFP FSMA-108 system includes a website or online application that is accessible to the general public. External users access the website via public URL. Internal users access the website via an internal URL.
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?	Yes
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies - Does Not Collect PII Persistent Cookies - Does Not 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 Employment Status Other - Free text Field
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
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Below 50
PIA - 4:	For what primary purpose is the PII used?	The FDA uses the PII for communication purposes: CFSAN/HFP FSMA Admins (internal users) use PII to contact the FDA affiliated state government agency leads to provide status of responses of their activities and assign activities to the leads. The admins can also contact state users if the pilot survey has not been completed.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The FDA makes no secondary use of the PII.
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.	The legal authorities that govern information use and disclosures specific to the system and program are 21 U.S.C. 301 (Federal Food, Drug and Cosmetic Act, of which the Food Safety Modernization Act of 2011 in part), and Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60 Rev. 1, Volumes I and II.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
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.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Online Government Sources Within the OPDIV State/Local/Tribal Other Federal Entities

PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	The OMB information collection approval number is OMB 0910-0855
PIA - 10B:	Identify the OMB information collection approval number expiration date.	8/31/2028
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
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.	There is no option to object to or opt-out of the information collection because all Federal employees and Direct Contractors with access to the system provide their PII for contact purposes. This is required through a FSMA directive. If an FDA employee or Direct Contractor chooses not to disclose their PII they will not be able to access or login to the FDA network and access CFSAN FSMA 108. External users are survey participants that are provided access to the survey (not to FSMA 108 directly) through a web linked portal included via an email invitation. The PII collected will not be shared outside of FDA and HHS and is used for contact purposes only.
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.	If FDA changes its practices with regard to the collection or handling of PII related to the website, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

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.	Individuals who suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have many avenues available for assistance. These individuals may contact FDA offices, including the Privacy Office, the Employee Resource and Information Center (ERIC-permanent employees or Direct Contractors only), the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and other agency offices, via e-mail, phone and standard mail avenues (all listed on fda.gov and the FDA intranet). In the event of a suspected incident or data breach, FDA personnel must report without delay to FDA's Cybersecurity and Infrastructure Operations and Coordination Center (CIOCC).
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.	Accuracy of PII is ensured by individual review of information provided at time of reporting. The PII is provided voluntarily by the individual. The individual is responsible for providing accurate information. FDA personnel may correct/update their information themselves and their PII is relevant and necessary to be granted access to the system. Access is granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authorization to operate (ATO). Controls are selected based on National Institute of Standards & Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. Data availability is ensured by annual reviews of users of CFSAN FSMA 108 to evaluate user access. Other controls include information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data relevancy is ensured by identifying data discrepancies during system use and addressing these discrepancies when discovered.
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: Users require access to provide response data for their respective activities. Some users are Direct Contractors. Administrators: For development, testing, and account management purposes. Some of the administrators are Direct Contractors. Developers: For development, testing, and maintenance purpose. Some of the developers are Direct Contractors. Contractors: Direct contractors who perform administrative, development, testing, and maintenance purpose.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users who require access to the PII in the system need to obtain supervisory approval before access is granted. There are two ways to request access to the applications: the user emails the business owner/IT Technical Lead or submits a request online through the 'Request Access' application option.
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.	Role based security controls ensure that each user role is appropriately assigned at the individual level in accordance with an individual user's need-to-know and least-access-privileges in regard to official duties such that each user sees/accesses only the data that is essential to complete his/her job. The agency reviews the access list for the information system on a quarterly basis. During this process users' access permissions are reviewed/adjusted, and unneeded accounts are purged from the system.
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 users of CFSAN/HFP FSMA 108 with access to PII in the system are required to complete mandatory FDA security and privacy awareness training annually. Completion is tracked by the Office of Digital Transformation (ODT).
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	No additional system-specific training is received by users; however, users are provided with user guides and manuals, and privacy guidance is available on the FDA intranet and from Privacy staff.
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).	FSMA108 adheres to General Records Schedule (GRS) 5.2 Transitory and Intermediary Records, Item 20: Temporary. Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule. Therefore, PII records are reviewed during the periodic User Access Review process and retained or destroyed when no longer needed for business use.

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 safeguards include user training on PII, system documentation that advises on proper use, and implementation of Need to Know and Minimum Necessary principles when awarding access. Technical Safeguards include the use of two-factor access authentication, device disk encryption, firewalls, virtual private network (VPN) and network monitoring and intrusion detection tools. Physical controls include the location of all system servers located at FDA facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the NIST's Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	11/5/2024
Privacy Analyst Comments:	HHS comment addressed.	**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls. HHS comments (PIA-23) were addressed.	**SOP Review Date:**	11/5/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	11/6/2024
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 11/6/2024 All comments have been addressed. This PIA is ready for SAOP review and approval. 11/1/2024 For PIA-23 Please be advise that GRS 20 no longer exist and was superseded by GRS 5.1 and 5.2. Please review the GRS 5.1 and 5.2 and update accordingly.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:		**SAOP Review Date:**	11/13/2024
		SAOP Days Open:	7

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
(11-4-2024) EMAIL_FDA - FSMA108 - QTR4 - 2024 - FDA4563755 (2386096).pdf	241482	.pdf	11/4/2024 4:48 PM	0
(11-6-2024) Revised PIA_HFP Food Safety Modernization Act 108_SOP Approved.rtf	808523	.rtf	11/6/2024 1:37 PM	0
10-31-2024 EMAIL_PIA in Queue (HFP Food Safety Modernization Act 108).pdf	384815	.pdf	10/31/2024 9:23 AM	0
HFP Food Safety Modernization Act 108_SOP Approved.pdf	176381	.pdf	10/31/2024 9:23 AM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 23	BLAND, CRYSTAL	11/1/2024	Please be advise that GRS 20 no longer exist and was superseded by GRS 5.1 and 5.2. Please review the GRS 5.1 and 5.2 and update accordingly.	

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:	11/13/2024 1:48 PM	**History Log:**	View History Log