Privacy Impact Assessment (PIA): FDA - PPSS - QTR2 - 2024 - FDA2129522

Created Date: 5/22/2024 4:02 PM Last Updated: 6/20/2024 2:42 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 - PPSS - QTR2 - 2024 - FDA2129522	**PIA ID:**	1832894
Name of Component:	FDA - OC Physical and Personnel Security Systems	**Name of ATO Boundary:**	CBER Office of Regulatory Operations
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	30
Submission Status:	Submitted	**Submit Date:**	5/22/2024
Next Assessment Date:	N/A	**Expiration Date:**	6/20/2027
Office:		**OPDIV:**	FDA
Security Categorization:		**OpDiv PIA ID:**	FDA2129522
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?	No
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
4:	ATO Date or Planned ATO Date.	10/12/2022
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.	The following changes have occurred since the last approval of this PTA/PIA: (1) the Visitor Management System (VMS) has been decommissioned; (2) Computer Coordinated Universal Retrieval Entry (CCure) is awaiting contractual agreements; (3) AlertFDA is no longer a Food and Drug Administration (FDA) system. It is now a Department of Health and Human Services (HHS) owned and operated system; and (4) ReadyOP is no longer used as an emergency notification system. ReadyOP is now used to store information about foreign national visitors. Due to these changes, VMS, CCure, and AlertFDA are no longer a part of the OC Physical and Personnel Security Systems (PPSS)
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 Food and Drug Administration's (FDA) Office of the Commissioner Consolidated Infrastructure (OC CI) consists of five General Support Systems (GSS 1-5). Each GSS consists of several tools, applications, and components. This assessment addresses OC CI Physical and Personnel Security

System (PPSS), a GSS 4 subset of applications that provides physical security to FDA employees, Direct contractors, and visitors at FDA facilities (mainly at FDA's White Oak campus in Silver Spring, Maryland). The following OC CI PPSS applications are covered collectively under this assessment: (1) Building Access System (BAS)/Monitor Dynamics (MDI) upgrade; (2) PremiSys ID; (3) Closed Circuit Television (CCTV); (4) ReadyOp; and (5) Emergency Call Stations.

The BAS/MDI component of PPSS is a major application and is implemented using MDI Commercial-Off-The-Shelf (COTS) software. BAS reads information off Personal Identity Verification (PIV) cards of individual FDA employees and Direct Contractors when they place cards atop a card reader present at FDA owned facility entry points. This card reading results in a logical decision made in the software to grant or deny access to physical entry points, including gates at parking facilities and barriers, and card access readers at the entrances of office buildings and areas within the buildings. This system includes intrusion alarm points, maps, and a central monitoring station located at FDA's White Oak Campus, which is monitored at all times. BAS production servers reside in the secure FDA Physical Security White Oak Command Center.
FDA uses PremiSys ID software, a minor application of the PPSS, to create and print photo ID badges only for FDA food inspectors and employees of Federal and State health departments. Per terms of agreement, state and local public health counterpart offices conduct inspections on behalf of FDA. The PremiSys ID production server resides in the secure FDA White Oak Data Center.

CCTV and Emergency Call stations are PPSS subcomponents that operate on an independent network isolated from the FDA network. The purpose of CCTV is to monitor and record activity on campus in real time to support emergency safety and security measures.

The Emergency Call Stations are telephones mounted on walls, light posts, and other fixtures located throughout the White Oak, College Park 1 and 2 campuses. In an emergency, an individual may use the callbox to signal and send a notification message (i.e., phone call) to FDA's White Oak Security Command Center.
ReadyOp is a web-based, encrypted platform requiring no hardware or software (ReadyOp was included in prior PIAs under PPSS as an emergency communication platform). ReadyOp is no longer used in this capacity. The FDA now utilizes ReadyOp to store information about foreign nationals who have an interest in visiting the FDA. PII is collected once a foreign national initiate a request to visit an FDA facility and gets approved.

		AlertFDA is now an HHS owned system that interfaces with FDA's Enterprise Administrative Support Environment system (EASE, the subject of a separate assessment) whichprovides the personally identifiable information (PII) of employees and contractors to be used for emergency communications.
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.	OC CI PPSS collects information about permanent FDA employees, Direct Contractors, authorized visitors to FDA facilities, including foreign nationals, and other individuals affiliated with FDA as described in this assessment. Individuals visiting FDA facilities are required to present proof of identification consisting of state/government issued identification. All PPSS applications require a user ID and password to log on. PPSS collects the following PII from and about FDA employees, Direct Contractors, non-Direct Contractors, and members of the public (United States (US) and non-US visitors): (a) full name; (b) phone number; (c) photographic identifiers (face); (d) passport number; (e) signature; and (f) user ID, and password. The PII data collected for purposes of the different PPSS subcomponents (BAS/MDI and PremiSys ID) are maintained at the White Oak Data Center (WODC). FDA also maintains CCTV recordings captured by cameras at different locations inside and outside FDA facilities. These cameras capture video of individuals and objects within each camera's viewer, such as a building entry location. When individuals are within the recording field for a camera, their face, hair color, clothing and other characteristics may be discernible in the recording as well as characteristics of any vehicle the images of which may be recorded. No voice or other sound data is captured by the cameras. FDA maintains CCTV recordings for thirty days or as long as required for FDA use in accordance with applicable records schedule. The Emergency Call Stations store only the date and time the box was triggered and a recording of the caller's voice. FDA uses PII to facilitate physical access to FDA facilities for authorized individuals. For most applications, such as BAS/MDI, the information used for this purpose includes name, photo, issue and expiration dates of the badge and a unique user number. Aggregate data from BAS is used by the FDA parking program to estimate the number of parking spaces necessary to accommodate employee demand. When an FDA employee or Direct Contractor enters an FDA building, they use their PIV card at the security checkpoint to authenticate access. Such individuals who present an FDA PIV card when entering a facility do not need to provide other proof of identity.

		FDA has processes in place to allow access to FDA facilities for foreign visitors. A valid passport is the only accepted form of identification for foreign visitors. Prior to a foreign visitor's arrival, the FDA sponsor is responsible for completing a brief host and escort registration form and quiz via ReadyOp. Sponsors can find the form on the FDA intranet. Sponsors must completely fill out a form for each visitor and provide the form to FDA's Office of Security Operations for review and approval prior to the visit. For their foreign visitors, upon approval of the submitted form, the sponsor will receive a personal link to the Foreign Visitor request form via ReadyOp. Passport information is captured for all foreign visitors that initiated a request and received approval to visit an FDA facility. The host and escort are responsible for monitoring the foreign visitor's activities during the visit. In regard to the PremiSys ID system , each Federal and/or State food inspector who visits an FDA facility must provide a valid photo ID such as a driver's license or passport. CCTV allows FDA guards and law enforcement to view live and recorded videos from specific FDA sites within the United States (U.S.). FDA maintains recordings for thirty days (or longer for business needs) as per the record retention requirement.
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.	
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.	OC CI PPSS collects and maintains federal employee and Direct Contractor PII. The system applications, BAS/MDI and PremiSys ID, use PII (name) to retrieve records about individuals. BAS/MDI manages physical access and monitoring for FDA buildings. It also monitors for alarms that may require police response. PremiSys ID is a comprehensive photo ID solution that helps create professional ID badges and cards for Federal and State Investigators. Foreign Visitors provide information to FDA employees to enter in ReadyOp which includes Passport information. FDA does not use PII to retrieve records from the CCTV and the Emergency Call Station applications and therefore these applications are not subject to the Privacy Act. The information collected and maintained by the CCTV and the Emergency Call Station applications may be shared with other FDA systems only where an authorized law enforcement purpose exists.
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.	ReadyOp's website is utilized to fill out, store and manage a series of forms for FDA personnel to request approval for foreign national visitors to visit the FDA and who have been pre-approved. This system contains selective Passport information on foreign national visitors. Hosts, escorts, and requestors can fill out a series of forms to gain approval on the behalf of their foreign national visitors. Hosts, escorts, and requestors must be U.S. citizens who are badged FDA employees or FDA Direct contractor s. This system is only accessible to users who are FDA personnel (employee or contractor) and is solely managed by the FDA Foreign National Team. The Foreign National Team shares an internal FDA URL with Hosts, escorts, and requestors to use the system. Members of the Foreign National Team serving in system administrator (Admin) roles manage ReadyOp's back-end capabilities using a unique web-based login and password. Additionally, once the host, escort, or requester enters information into ReadyOp, they no longer have access to the submitted information.
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 Phone numbers Date of Birth Photographic Identifiers Mailing Address Passport Number User Credentials Other - Free text Field - Voice recorded at Emergency Call Stations (Potential PII)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors Members of the public 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?	The primary purpose of the PII in these applications is to identify and record staff and visitors who seek to access an FDA facility.
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.	5 U.S.C. 301; Federal Property and Administrative Services Act of 1949 (codified as amended in scattered sections of 40 U.S.C. and 41 U.S.C.); Information Technology Management Reform Act of 1996 (Clinger-Cohen Act, Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104-347, sec. 203); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004.
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.	For MDI and PremiSys ID: Name of Federal employees and contractors. For ReadyOp: PII elements displayed in government issued identification (e.g., Passport information).
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 System of Records Notice(s) (SORN(s)) used to cover the system is 09-90-0777 Facility and Resource Access Control https://www.hhs.gov/foia/privacy/sorns/09900777/index.html
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Email Online Government Sources Within the OPDIV Other HHS OPDIV Non-Government Sources Members of the Public Private Sector
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.	Because the Foreign Visitor forms do not collect PII from members of the general public, an Office of Management and Budget information collection approval number is not applicable. Note: The PII is only collected once a Foreign Visitor initiates a request to visit an FDA facility and gets approved.
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 Within HHS
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Within HHS: PII may be shared with offices that have access to employee data to ensure consistency with HHS access lists and policies. Other Federal Agency/Agencies: In rare cases, FDA will receive requests for information, such as footage from CCTV of accidents that have happened on campus. Minimum necessary principles are adhered to for any such disclosures/sharing with other federal entities.
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)).	None

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.	FDA does not share PII in a Privacy Act PPSS application outside the Agency. Internally it is shared only with personnel who have an authorized need to know. The Privacy Act does not require an accounting of disclosures in these circumstances. If this changes in the future, officials accountable for operation of the applications within PPSS that are subject to the Privacy Act are responsible for ensuring their office maintains an accurate and current accounting of disclosures as required by the statute, HHS and FDA regulations, and FDA's internal privacy policies and procedures. FDA's Privacy Office provides guidance on the accounting requirement.
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.	BAS/MDI and PremiSys ID applications require the use of PII about federal employees and Direct Contactors to retrieve records about individuals maintained in each application. Foreign Visitors (a person not a citizen or national of the United States) are required to fill out the internal Foreign Visitors Data Request form in ReadyOp. There is no option to opt-out of the collection of their PII if they desire to enter an FDA facility. The individual must understand that they must be identified, and their information validated in order to gain access to a federal building. Individuals will have awareness of how their information will be used. In the event an individual decides to opt-out of providing PII for any reason, they will not be granted access to FDA.
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.	In the event of a major change, FDA will notify individuals via one or more of several available avenues of communication. Agency personnel would be notified using one or more methods, e.g., via updated HHS/FDA forms; new or updated Privacy Act Statements and Notices published in the Federal Register and on FDA.gov (e.g., System of Records Notice(s)); an updated PIA; and/or internal e-mail. The system does not provide the capability for automated notification of individuals. To the extent, use of visitor data changes between the time of collection and deletion, visitors (all data subjects other than FDA permanent employees and Direct Contractors) would be notified via published notices and assessments (SORN, PIA, web-posted notices and policies). FDA personnel area advised at the time of hire of the creation, collection, and use of PII about them. All users view a warning message at log in advising of the lack of privacy in the course of using government systems and resources.

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.	Personnel may initiate corrections to PII by submitting an information update form to his or her supervisor or the FDA Badging Office. Federal employees and Direct Contractors may address their privacy concerns through supervisors, managers, and team leaders, and they may also seek assistance using FDA's Employee Resource and Information Center (ERIC), reporting potential loss or misuse of their PII to FDA's Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) and/or by contacting FDA's Privacy Office directly. Visitors may contact FDA's Privacy Office or other appropriate officials using contact information provided on FDA.gov. All system users are required to rapidly report suspected incidents and breaches.
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.	Updated information is provided to BAS/MDI by the source (HHS) systems. Other system data is transactional and short-term and reviewing it and changing it in any way would render it inaccurate and not useful. FDA validates authenticity of the identification to support reliance on the accuracy of the information content. Individuals are prompted to review and confirm the accuracy of information they provide at building entry. Individuals are also encouraged and reminded to verify the accuracy and validate their contact information (PII) while configuring or updating their contact preferences. Relevancy is ensured by the design of the system which limits the type of PII collected to PII necessary for identity document authenticity and individual identity verification. Applied access settings and other security controls support PII integrity, availability, and accuracy. Maintenance of cameras, scanners, servers, and applications provide additional security.
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: For authorizing access to the building. Administrators: System maintenance or the role of a Direct Contractor. Developers: System maintenance, development, or the role of a Direct Contractor. Contractors: Direct Contractors who perform the role of Developers or Administrators.

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 information system must obtain supervisor approval and sign off before access is granted. Access to each of the applications in PPSS is granted separately using a person-specific role-based standard. Users (All FDA badge-holders) must log in to each application separately with a user ID and password.
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.	Each user's supervisor will specify on the account creation form the minimum information system access that is required for the user to complete his/her job. The access list for the information system is reviewed on a regular basis to adjust users' access permissions and purge unnecessary user accounts 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.	Annual security awareness training is provided to all FDA staff and Direct Contractors. Privacy is specifically addressed within this training. This training includes guidance of Federal laws, policies, and regulations relating to privacy and data confidentiality, integrity, and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA verifies that training has been successfully completed.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	A technical contractor trains FDA System Administrators and provides FDA-specific training materials to include electronic manuals and videos for FDA badged population (includes security guards) to register visitors and cancel registrations. Additional privacy training is available from the FDA’s Privacy Office.
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).	Records in the system are maintained under the following FDA file codes and associated records retention schedules: FDA file code 9647a and National Archives and Records Administration (NARA) General Records Schedule (GRS) 18-17a for areas under maximum security. Disposition: TEMPORARY. Destroy 5 years after final entry or 5 years after date of document, as appropriate. File code 9647b and GRS 18-17b for other areas. Disposition: TEMPORARY. Destroy 2 years after final entry or 2 years after date of document, as appropriate. Records Description: Visitor processing records. Registers or logs recording names of outside contractors, service personnel, foreign national and other visitors, employees admitted to areas, and reports on vehicles and passengers. Disposition Instruction: TEMPORARY. Destroy when 30 days, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS¬2017-0006¬0015. GRS 5.6, Item Number 111-Visitor Processing Records.

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 information contained within the system is protected by several layers of administrative, physical, and technical controls in accordance with policies and regulations from the FDA, NIST, and OMB. Administrative controls include review of security controls on an ongoing/continuous basis to ensure effectiveness, and supervisor review of individual access requests. Physical controls include locked guarded facilities and enclosures, and that system hardware devices are in a limited access computer room, with access restricted to physical security staff. Technical controls include that logical access is controlled through two factor authentications at the domain level as well as separate authentication mechanisms at the application level. Additional controls include encryption, virtual private network (VPN), intrusion detection, and guarded facilities with closed circuit TV. Users who require access to the information system are restricted to the minimum information system access necessary for the user to complete his/her job. FDA has a comprehensive monitoring and incident response plan designed to accommodate various situations and escalate privacy and security incidents as necessary.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	5/22/2024
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:		**SOP Review Date:**	5/22/2024
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	5/23/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 5/23/2024 This PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature_Bridget Guenther.docx
SAOP Comments:	Update to include drivers license in the next iteration of this PIA, see below. The Emergency Call Stations store only the date and time the box was triggered and a recording of the caller's voice. FDA uses PII to facilitate physical access to FDA facilities for authorized individuals. For most applications, such as BAS/MDI, the information used for this purpose includes name, photo, issue and expiration dates of the badge and a unique user number. In regard to the PremiSys ID system , each Federal and/or State food inspector who visits an FDA facility must provide a **valid photo ID such as a driver's license** or passport.	**SAOP Review Date:**	6/20/2024
		SAOP Days Open:	28

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

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:	6/20/2024 2:42 PM	**History Log:**	View History Log