Privacy Impact Assessment (PIA): FDA - OCI Kbox - QTR1 - 2023 - FDA2084356

Date Signed: 2/21/2023

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

Status:	Approved	**PIA ID:**	1617304
PIA Name:	FDA - OCI Kbox - QTR1 - 2023 - FDA2084356	**Title:**	ORA OCI Kbox Helpdesk System
OpDiv:	FDA		

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	Significant System Management Change
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Since this Privacy Threshold Analysis/Privacy Impact Assessment was last approved, FDA made the following changes to the KBOX system: The system now receives (handles but does not maintain) additional Personally Identifiable Information (PII) relating to the targets of active criminal investigations.
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.	KBOX is a Help Desk ticketing system used internally by several teams within the Office of Criminal Investigations (OCI) including the IT Support Team and Investigative Analysis Branch (IAB). Users (FDA Special Agents and other authorized FDA personnel) may submit internal

		information requests in two ways. First, by sending an email from their FDA email account to the queue-specific email address which will auto generate a help ticket. Or, second, by using a web browser and navigating to the system portal available on FDA's intranet. Only OCI employees are able to use the system portal as it is an internal-only Single Sign-On (SSO) configured system that requires users from the IAB office to authenticate their identity using their agency-issued computers and Personal Identity Verification (PIV) certificate (aka badge). KBOX is also setup to receive suspected criminal activity tips that have been processed by the agency after they are reported to the agency through a publicly available FDA webpage which is not part of KBOX (https://www.accessdata.fda.gov/scripts/email/oc/oci/contact.cfm). Once a reporter has submitted a tip to the FDA-managed site, the information is passed to KBOX via FDA email. OCI does not manage or interact with the public-facing FDA tip site. The tip reporting page provides limited fields for information submission. The fields consist of submitter email address (optional), a "related activity" selection from a drop-down menu (required field), a location selection from a drop-down menu (state or US territory, "foreign" or "other"; required field) and an open text field for comments (required field). Only OCI Staff are permitted to access KBOX. Individual level access permissions and controls are applied to enforce access restrictions.
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.	FDA's use of the KBOX system is limited to facilitating the request from the Special Agent assigned to a case to the IAB Staff member who will assist with the investigation. No information found by IAB through their research in response to an Agent's information request is stored in or communicated through this system. KBOX simply functions as a Help

Desk queue and collects or handles PII necessary for that function.

Separate from the research by IAB, the system receives but does maintain information about targets of investigation received via the public tip reporting portal. This information may include PII about investigative targets; members of the public who submit tips control what PII or other information they include in a submitted tip. Targets of investigations can include Employees, Public Citizens, Business Partners/Contacts, Vendors/Suppliers/Contractors, Patients, and non-US persons.

The IAB handles internal information requests about entities associated with criminal investigative matters and now employs a queue in the system to receive information requests. All requests are internal, as placed by Special Agents (FDA personnel). As part of their duties, IAB Staff have access to and may use Law Enforcement Agency- (LEA) and Finance-specific tools (software, applications) including commercial and open-source tools to gather information in response to requests from Special Agents.

The only PII elements maintained by the system are related to the OCI staff's user account which include first name, last name, and email address. Non-PII data such as non-identifying details contained in the results of IAB research or in tips are not stored in the system.

There is the potential for all manner of PII and potential PII to be received or handled by the system although not stored or maintained there. Given the investigative nature of the work of OCI, this is likely to include sensitive and other PII such as SSN, date of birth, driver's license information, passport information, photographs/images, criminal and employment history, professional license information, FDA establishment inspection data and banking and financial information.

FDA does not share data from the KBOX system. OCI teams receive requests in the form of tickets and the requested actions are fulfilled and communicated through other systems.

PTA - 5A:	Are user credentials used to access the system?	Yes
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.	OCI staff user account information which includes first name, last name, and email address are collected and maintained in the system to provision the system and ensure correct access is granted. PII about other FDA personnel is entered by OCI Staff to place tickets with specialized units and the Investigative Analysis Branch (IAB) staff who assist with the criminal investigations. No data is shared from the system. OCI teams receive requests in the form of tickets and the requested actions are fulfilled and communicated through other systems.
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.	The purpose of the website is to provide a web interface for users to submit tickets and ticket owners to receive and updated the placed tickets. Only OCI Staff has access to the website. OCI Staff access the website via SSO internally on the FDA network.
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 - 12:	Does the website use web measurement and customization technology?	No
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 14:	Does the system have a mobile application?	No
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 - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Email Address Name Other - Free text Field - The selected PII elements are data expected to be collected and/or stored. Other PII may be collected and/or stored as necessary for authorized investigative needs, such as Alien Registration Number, FBI number, National Crime Information Center (NCIC) criminal history information including photos/tattoo/scars/identifying marks, arrest information and FDA Regulatory records.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies)
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	FDA employee PII is used only to maintain the user's system account for placing tickets and access to the portal. All other types of PII (e.g., relating to members of the public) is used for criminal investigations.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	No secondary usage of the PII.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID	SSNs are submitted by Special Agents working on active criminal investigations for Investigative Analysts to reference during the course of their research and investigation.
PIA - 6A:	Cite the legal authority to use the SSN.	Federal Food, Drug and Cosmetic Act (e.g., 21 U.S.C. 371, establishing authority to conduct examinations and investigations; 21 U.S.C. 331 listing prohibited acts) and the crimes and criminal procedure provisions of Title 18 of the U.S. code. This system is not used to collect SSNs directly from the individuals identified by the SSN. The use of the SSN as an identifier for Federal employees is permissible per Executive Order 9397, as amended by Executive Order 13478 issued November 18, 2018.
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Legal authorities governing use and disclosure include provisions of the Federal Food, Drug, and Cosmetic Act (e.g., 21 U.S.C. 372, establishing authority to conduct examinations and investigations; 21 U.S.C. 331

		listing prohibited acts) and the crimes and criminal procedure provisions of Title 18 of the U.S. Code. The OCI collects and handles information in accordance with the U.S. Constitution, federal rules of procedure, court orders and other authorities applicable to criminal law enforcement organizations. The administrative functions of KBOX are authorized by 44 U.S.C. 3101, and a number of sections of 5 U.S.C. including sections 301, 1302, 2951, and 4118 and Executive Order 10561. These statutory provisions authorize agency heads to create the infrastructure and maintain the information necessary for the organization to accomplish its purposes and mission. E-Government Act of 2002, Title III: Information Security (Federal Information Security Modernization Act of 2002 (FISMA)), December 2014 as amended.
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
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 Other Federal Entities Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to 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 individualized opt-out for collection of investigative information because it is obtained for federal criminal investigative purposes and providing an opt-out option would risk compromising open investigations.
PIA - 14:	Describe the process to notify and obtain	There is no individualized prior notice for collection of investigative

	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.	information because it is obtained for federal criminal investigative purposes and providing notice would risk compromising open investigations. There is no notification and consent process regarding major changes affecting the investigative aspects of the system because information is obtained and used for federal investigative purposes and notification could compromise ongoing investigations. In the event of major changes impacting FDA employee data, any necessary notice or consent would be addressed in email, system notifications, text boxes or other communications to the individuals.
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.	For subjects of investigative records, individuals may resolve these concerns as part of the legal proceedings related to the relevant criminal investigation. FDA regulations provide a process by which these individuals may seek access to a record about themselves in certain circumstances (See 21 CFR 21.65). Employees may contact their management or administrative offices to correct inaccurate information. Employees and external individuals may contact the FDA Privacy Office for assistance. All FDA personnel are required to rapidly report suspected or confirmed instances of unauthorized access or use of PII.
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.	Individuals are responsible for providing accurate information. Accuracy is ensured by individual review at the time of submission. FDA personnel may correct/update the information. FDA user 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). PII about other individuals is obtained from other

		source systems that are separately responsible for PII accuracy, integrity and availability. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an authority to operate (ATO). PII relevancy is ensured by system design and user needs; investigative actions often require a variety of PII. Controls are selected based on 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. OCI (Office of Criminal Investigations) performs annual reviews to evaluate user access. One of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information. Data discrepancies identified during system use are addressed when discovered.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: Investigative Analysis Branch (IAB) Staff have access to PII for authorized work on criminal investigative matters. Administrators: Administrators have access in the course of working to monitor and ensure the system functions operate properly.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access (RBA) is used for supervisors to approve and limit access at the individual level and administrators to control permissions. Permissions are assigned based on responsibility and position within the organization. Ticket Owners are only able to view PII that is directly associated with the Help Desk queue associated with their work.
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.	Permissions are assigned based on responsibility and position within the organization. Users only have access to information needed to perform duties related to their specific roles.

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.	FDA requires employees to complete annual security and privacy awareness training. The Office of Digital Transformation (ODT) tracks completion of annual training.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Intensive system-specific user training is provided for all new employees during a Special Agent Training Program.
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).	FDA maintains records in KBOX in accordance the FDA Records Schedule 8900, Reference Materials, National Archives and Records Administration (NARA) Citation N1-088-05-1, which indicates that materials are destroyed or deleted when no longer needed for reference purposes. OCI has a need to maintain KBOX records continuously due to the nature of the law enforcement data.
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; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.