PTA / PIA: FDA - OCI_Kbox - QTR2 - 2026 - FDA5271678

Created Date: 7/8/2026 2:01 PM Last Updated: 7/16/2026 2:18 PM

General Information

PTA / PIA Name:	FDA - OCI_Kbox - QTR2 - 2026 - FDA5271678	**PTA / PIA ID:**	4623491
Component Name:	FDA - OII OCI Kbox Helpdesk System	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	21
Submitter:		**Submit Date:**	7/8/2026
Next Assessment Date:	07/15/2029	**Expiration Date:**	7/15/2029
Office:		**OpDiv:**	FDA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	3/9/2026
General 05:	Is the system or electronic information collection, agency or contractor operated?	Agency
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Jordan Hessman
PTA 01A:	POC Title and Organization	Lead Information Technology FDA/OII/OCI
PTA 01B:	POC Email Address	Jordan.Hessman@fda.hhs.gov
PTA 01C:	POC Phone Number	240-276-9432
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Food and Drug Administration (FDA) have made no changes to this system/component/ since the last Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) was approved.
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	KBOX is a Help Desk ticketing system used internally by several teams within the Office of Criminal Investigations (OCI), which operates under the Food and Drug Administration (FDA), a component of the Department of Health and Human Services (HHS). The system supports HHS's law enforcement mission by providing a structured, secure platform for managing internal information requests and tracking suspected criminal activity tips related to FDA-regulated products and activities. The system carries out its functions through two primary mechanisms. First, authorized users may submit internal information requests by sending an email from their FDA email account to a queue-specific email address, which automatically generates a help desk ticket. Second, users may access the system through a web browser by navigating to the system portal available on FDA's intranet. In addition to internal ticketing, KBOX is configured to receive suspected criminal activity tips that members of the public submit through a publicly available FDA webpage. It is important to note that OCI does not manage or interact with this public-facing FDA tip site. The tip reporting page provides limited fields for information submission, consisting of the submitter's email address (optional), a "related activity" selection from a drop-down menu (required), a location selection from a drop-down menu — which includes options for state or U.S. territory, "foreign," or "other" (required) — and an open text field for comments (required). Once a tip is submitted to that external site, the information is forwarded to KBOX via FDA email, where it is received and reviewed by OCI staff. If a tip is deemed worthwhile following OCI review, a case is opened in the Agency Investigative Management System (AIMS), which is a separate case management system. KBOX functions solely as the intake and triage platform; all case records and associated investigative PII are maintained in AIMS, which is covered under a separate PIA/PTA. The users of the system are FDA Special Agents and other authorized OCI personnel, including staff from the Investigative Analysis Branch (IAB). The IAB uses the system to receive and manage internal information requests placed by Special Agents working on active criminal investigative matters. Access to the system is strictly controlled: the web portal is an internal-only, Single Sign-On (SSO) configured system that requires users to authenticate their identity through SSO authentication integrated with FDA's Active Directory (AD) system (covered in a separate PIA), using a Health and Human Services (HHS) Personal Identity Verification (PIV) card for multi-factor authentication. No external or public access to the portal is permitted. Individual-level access permissions and role-based access controls are applied to enforce these restrictions, ensuring that ticket owners can only view information directly associated with the Help Desk queue relevant to their specific duties.
PTA 05:	List and/or describe all the types of information that are collected,	FDA's use of the KBOX system is limited to

	maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	facilitating requests from the Special Agent assigned to a case to the IAB staff member who will assist with the investigation, and to receiving and triaging suspected criminal activity tips submitted by the public. KBOX functions as a Help Desk queue and ticket management platform. Ticket data — including any PII submitted in the body of a ticket — is stored locally within the system's MariaDB database instance, hosted at the OCI Data Center, for the duration of the ticket lifecycle and in accordance with the applicable records retention schedule. The only PII elements actively maintained by the system on a persistent basis are those related to OCI staff user accounts, which include first name, last name, and email address. These are required to provision the system and ensure correct access is granted to authorized personnel. Separate from user account data, the system receives information about targets of investigation via the public tip reporting portal, as well as PII submitted by Special Agents in the body of investigative help desk tickets. This information is received and handled by the system but is not maintained as a case record within KBOX. If a tip is deemed worthwhile following OCI review, a case is opened in the Agency Investigative Management System (AIMS), which is a separate case management system covered under its own PIA/PTA. All investigative case records and associated PII are maintained in AIMS, not in KBOX. Targets of investigations can include employees, members of the public, business partners/contacts, vendors/suppliers/contractors, patients, and non-U.S. persons. Given the investigative nature of OCI's work, information received by the system may include sensitive PII such as Social Security Numbers (SSNs), 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. Additionally, the system may receive or handle other sensitive PII as necessary for authorized investigative needs, including but not limited to Alien Registration Numbers, Federal Bureau of Investigation (FBI) numbers, National Crime Information Center (NCIC) criminal history information (including photos, tattoos, scars, and other identifying marks), arrest information, and FDA regulatory records. This sensitive PII is received transiently as part of ticket submissions and is not stored as a persistent investigative record within KBOX. FDA does not share data from the KBOX system to external organizations. Internally, when a tip or request is acted upon, the relevant information is transferred to AIMS for case management purposes. Regarding retention, FDA maintains records in KBOX in accordance with 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 it handles.
PTA 05A:	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.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	FDA's Active Directory
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	OCI staff user account information, which includes first name, last name, and email address, is collected and maintained in the system to provision the system and ensure correct access is granted to authorized personnel. This information is necessary to manage user accounts and enforce individual-level access permissions and role-based access controls within the system. PII about other FDA personnel is entered by OCI staff to place tickets with specialized units and IAB staff who assist with criminal investigations. This information is used solely to facilitate the internal request process between Special Agents and the IAB staff members who support their investigative work. All requests of this nature are internal, as placed by Special Agents who are FDA personnel. Regarding members of the public who submit tips, the system receives information that tipsters voluntarily provide through the public-facing FDA tip reporting page. The tip reporting page provides limited fields for submission, and members of the public determine what PII or other information they choose to include when submitting a tip. Once submitted, that information is forwarded to KBOX via FDA email, where it is received and reviewed by OCI staff. Targets of investigations — which can include employees, members of the public, business partners/contacts, vendors/suppliers/contractors, patients, and non-U.S. persons — may have PII received or handled by the system either through the tip submission process or in connection with an active criminal investigation. This information may include sensitive PII such as SSNs, 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. Additionally, the system may receive or handle other sensitive PII as necessary for authorized investigative needs, including but not limited to Alien Registration Numbers, Federal Bureau of Investigation (FBI) numbers, National Crime Information Center (NCIC) criminal history information (including photos, tattoos, scars, and other identifying marks), arrest information, and FDA regulatory records. No data is shared from the KBOX system to another system. OCI teams receive requests in the form of tickets, and the requested actions are fulfilled and communicated through other systems external to KBOX. The collection and handling of all information within the system is authorized under provisions of the Federal Food, Drug, and Cosmetic Act (FD&C Act), the crimes and criminal procedure provisions of Title 18 of the U.S. Code, and other

		applicable legal authorities governing federal criminal law enforcement organizations. When a tip or investigative request is deemed worthy of further action following OCI review, the relevant information is transferred internally to the Agency Investigative Management System (AIMS), a separate FDA/OCI case management system covered under its own PIA/PTA, where the formal case record is opened and maintained.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://oci-helpdesk.fda.gov/ — This Uniform Resource Locator (URL) is only accessible within FDA's internal network and is not publicly accessible.
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	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 KBOX website is to provide a web interface for users to submit tickets and for ticket owners to receive and update the placed tickets. The portal supports the internal operational needs of OCI, including Information Technology (IT) support requests, management of suspected criminal activity tips received from the public-facing FDA tip site, and other specialized queue-based requests for groups within OCI. Access to the website is restricted exclusively to authorized OCI staff. No external or public access to the portal is permitted. Individual-level access permissions and role-based access controls are applied to enforce these restrictions, ensuring that ticket owners can only view information directly associated with the Help Desk queue relevant to their specific duties. OCI staff access the website internally on the FDA network via SSO authentication integrated with FDA's AD system, using an HHS PIV card for multi-factor authentication. The production Uniform Resource Locator (URL) for the system is <a>https://oci-helpdesk.fda.gov/, which is only accessible within FDA's internal network and is not publicly accessible. The system is not accessible outside of FDA's network, which serves as an additional compensating control to protect the sensitive law enforcement data handled by 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 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:	Are any third-party websites or applications (TPWA) associated with the system?	No

PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Biographical Information Name Contact Information Email Address (Business) Other Other

PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Additional PII may be collected and/or stored as necessary for authorized investigative needs. This includes, but is not limited to, Alien Registration Numbers, Federal Bureau of Investigation (FBI) numbers, National Crime Information Center (NCIC) criminal history information including photos, tattoos, scars, and other identifying marks, arrest information, and FDA regulatory records. Other sensitive PII such as 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 may also be received or handled by the system as needed for investigative purposes. The PII elements listed — including Social Security Number — reflect the full range of PII that the KBOX system may receive, handle, or process in the course of its operations. It is important to note, as described in PTA-05, that the KBOX system functions primarily as a Help Desk ticketing platform. The only PII elements actively maintained (i.e., stored) by the system on a persistent basis are those associated with OCI staff user accounts: first name, last name, and email address. Sensitive PII elements — including, but not limited to, Social Security Numbers, 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 — may be received or handled by the system as part of investigative ticket submissions but are not stored or maintained within KBOX itself. This information is submitted by Special Agents in the body of help desk tickets and passes through the system as transient content. The system does not serve as a repository for investigative records, and no such records are retained in KBOX beyond the ticket lifecycle governed by FDA Records Schedule 8900. The inclusion of Social Security Number and other sensitive PII in PIA-22 reflects the system's potential exposure to this information during normal operations, not an indication that these elements are maintained as persistent records within the system.
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)

PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The PII collected and maintained within the KBOX system serves two primary purposes depending on the category of individual to whom the information pertains. FDA employee PII, which consists of first name, last name, and email address, is used solely to maintain the user's system account for placing tickets and for access to the portal. This information is necessary to provision the system and ensure that correct access is granted to authorized OCI personnel. All other types of PII — such as that relating to members of the public, targets of investigations, business partners/contacts, vendors/suppliers/contractors, patients, and non-U.S. persons — is used exclusively for criminal investigations conducted by OCI. This includes PII submitted by Special Agents working on active criminal investigations for IAB Investigative Analysts to reference during the course of their research and investigation. There is no secondary usage of PII within the system.
PIA 26:	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 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	SSNs may be submitted by Special Agents working on active criminal investigations for IAB Investigative Analysts to reference during the course of their research and investigation. It is important to note that the KBOX system is not used to collect SSNs directly from the individuals identified by the SSN. Rather, SSNs may be submitted internally by OCI Special Agents as part of the investigative request process and are received transiently within ticket submissions. If the associated tip or investigative matter is acted upon, the relevant information — including any SSN — is transferred to the Agency Investigative Management System (AIMS), where it is maintained as part of the case record. The use of the SSN as an identifier for Federal employees is permissible per Executive Order (EO) 9397, as amended by EO 13478, issued November 18, 2008.

PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	The following legal authorities govern the use of SSNs within the KBOX system: Federal Food, Drug, and Cosmetic Act (FD&C Act): Specifically, 21 U.S.C. § 372, establishing FDA's authority to conduct examinations and investigations, and 21 U.S.C. § 331, listing prohibited acts. Title 18 of the U.S. Code: The crimes and criminal procedure provisions of Title 18 of the U.S. Code provide additional legal authority for the use of SSNs within the system in the context of criminal investigations. Executive Order (EO) 9397, as amended by EO 13478 (issued November 18, 2008): The use of the SSN as an identifier for Federal employees is permissible under this authority.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The following legal authorities govern the use and disclosure of information within the KBOX system: Federal Food, Drug, and Cosmetic Act (FD&C Act): Specifically, 21 U.S.C. § 372, establishing authority to conduct examinations and investigations, and 21 U.S.C. § 331, listing prohibited acts. 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. Title 18 of the U.S. Code: The crimes and criminal procedure provisions of Title 18 of the U.S. Code provide legal authority governing the use and disclosure of information within the system in the context of criminal investigations. 44 U.S.C. § 3101 and Sections of 5 U.S.C.: 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, as well as Executive Order (EO) 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. Data Flow to AIMS: When a tip or investigative request received in KBOX is deemed worthy of further action, the relevant information is transferred to the Agency Investigative Management System (AIMS), a separate FDA case management system covered under its own PIA/PTA. The use and disclosure of information within AIMS is governed by the legal authorities applicable to that system. The transfer of information from KBOX to AIMS is an internal agency function conducted within FDA/OCI and is subject to the same legal authorities listed above.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No

PIA 30:	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 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	An Office of Management and Budget (OMB) information collection approval number is not required for the KBOX system because the system does not collect information directly from members of the public in a manner that would trigger the requirements of the Paperwork Reduction Act (PRA). The system is an internal-only Help Desk ticketing system used exclusively by authorized OCI staff, including Special Agents and IAB personnel. While the system does receive tips submitted by members of the public through the public-facing FDA tip reporting page, OCI does not manage or interact with that public-facing site, and the tip information is simply forwarded to KBOX via FDA email after submission. The collection of information from the public occurs through the separate, publicly accessible FDA tip reporting page, which is not part of the KBOX system. Therefore, the KBOX system itself does not directly collect information from the public in a way that would require OMB information collection approval.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	There is no individualized prior notice or consent process in place for the collection of investigative information within the KBOX system. This is because the information is obtained for federal criminal investigative purposes, and providing prior notice or an opt-out option would risk compromising open investigations. Given the sensitive law enforcement nature of OCI's work, notifying individuals that their information is being collected could undermine the integrity of active criminal investigations and jeopardize the agency's ability to fulfill its law enforcement mission. In the event of major changes impacting FDA employee data, any necessary notice or consent would be addressed through email, system notifications, text boxes, or other communications directed to the affected individuals. However, no such notification and consent process exists regarding major changes affecting the investigative aspects of the system, again due to the risk that such notification could compromise ongoing investigations. For members of the public who voluntarily submit tips through the public-facing FDA tip reporting page, the submission of PII is voluntary, and individuals control what PII or other information they choose to include in their submission. The tip reporting page includes a posted privacy notice to inform users of how their information may be used. It should be noted that OCI does not manage or interact with the public-facing FDA tip site, and therefore any notice provided to tip submitters is managed separately through that external site.
PIA 35:	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). If they cannot be notified or have their consent obtained, explain why.	There is no individualized prior notice for collection of investigative 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 36:	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 KBOX system has several processes in place to address concerns raised by individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that their PII is inaccurate. These processes vary depending on the category of individual raising the concern. Subjects of Investigative Records: For individuals who are subjects of investigative records, concerns regarding the inappropriate obtaining, use, or disclosure of their PII may be resolved as part of the legal proceedings related to the relevant criminal investigation. Additionally, FDA regulations provide a process by which these individuals may seek access to a record about themselves in certain circumstances, as outlined in 21 Code of Federal Regulations (CFR) 21.65. FDA Employees: Employees who believe their PII is inaccurate may contact their management or administrative offices to correct the inaccurate information. Employees are also responsible for providing accurate information at the time of submission, and FDA personnel may correct or update information as needed. Employees and External Individuals: Both employees and external individuals may contact the FDA Privacy Office for assistance in resolving concerns related to the inappropriate obtaining, use, or disclosure of their PII, or regarding the accuracy of their PII within the system. Reporting Unauthorized Access or Use: All FDA personnel are required to rapidly report suspected or confirmed instances of unauthorized access or use of PII, ensuring that any potential privacy incidents are promptly identified and addressed in accordance with FDA policy.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The KBOX system has several processes in place to ensure the integrity, availability, accuracy, and relevancy of PII contained within the system. Each element is addressed as follows: Accuracy: Individuals are responsible for providing accurate information at the time of submission, and accuracy is ensured by individual review at the time of submission. FDA personnel may correct or update information as needed. PII about other individuals is obtained from other source systems that are separately responsible for PII accuracy. Data discrepancies identified during system use are addressed when discovered. Integrity and Availability: 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 and 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. Additionally, one of the controls includes information system backups reflecting the requirements in contingency plans as well as other agency requirements for backing up information, further ensuring the availability of data in the event of a system failure. Relevancy: PII relevancy is ensured by system design and user needs. FDA user PII is relevant and necessary to be granted access to the system, and access is granted and restricted at the individual level as appropriate to the individual's duties through role-based access controls. Investigative actions often require a variety of PII, and the system is designed to handle only the PII necessary for authorized investigative and administrative purposes. Access Reviews: OCI performs annual reviews to evaluate user access, ensuring that access permissions remain appropriate to each individual's role and responsibilities within the organization. Permissions are assigned based on responsibility and position within the organization, and supervisors approve and limit access at the individual level while administrators control permissions.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users: IAB staff require access to PII for authorized work on criminal investigative matters. As part of their duties, IAB staff have access to and may use Law Enforcement Agency (LEA) and finance-specific tools, including commercial and open-source tools, to gather information in response to requests from Special Agents. Ticket owners are only able to view PII that is directly associated with the Help Desk queue associated with their work, ensuring that access is limited to the minimum amount of information necessary to perform their job duties. Administrators: Administrators require access to PII in the course of working to monitor and ensure that the system functions operate properly. This access is necessary to maintain the integrity, availability, and security of the system and the information it contains. Administrator access is governed by role-based access controls, and permissions are assigned based on responsibility and position within the organization, ensuring that administrators only have access to the minimum amount of information necessary to perform their system management and oversight duties.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The following administrative procedures are in place to determine which system users may access PII within the KBOX system: Role-Based Access (RBA): RBA is the primary mechanism used to control access to PII within the KBOX system. Permissions are assigned based on responsibility and position within the organization, ensuring that users only have access to information needed to perform duties related to their specific roles. Supervisors are responsible for approving and limiting access at the individual level, while administrators control permissions within the system. Individual-Level Access Controls: Access permissions and controls are applied at the individual level to enforce access restrictions. Ticket owners are only able to view PII that is directly associated with the Help Desk queue associated with their work, ensuring that access is limited to the minimum amount of information necessary to perform their job duties. Annual Access Reviews: OCI performs annual reviews to evaluate user access, ensuring that access permissions remain appropriate to each individual's role and responsibilities within the organization. This process helps to identify and address any instances where access permissions may need to be updated or revoked due to changes in an individual's role or responsibilities. Need to Know and Minimum Necessary Principles: The system implements Need to Know and Minimum Necessary principles when awarding access, ensuring that individuals are only granted access to the PII that is directly relevant to and necessary for the performance of their specific job duties.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	The following technical methods are in place to ensure that those with access to PII can only access the minimum amount of information necessary to perform their job duties within the KBOX system: Role-Based Access Controls: Permissions are assigned based on responsibility and position within the organization, ensuring that users only have access to information needed to perform duties related to their specific roles. This technical control ensures that no individual user has broader access to PII than is necessary for the performance of their specific job duties. Single Sign-On (SSO) Authentication Integrated with Active Directory (AD): Users access KBOX through SSO authentication integrated with FDA's AD system, using an HHS PIV card for multi-factor authentication. This technical control ensures that only authorized individuals are able to access the system and the PII contained within it. Queue-Specific Access Restrictions: Ticket owners are only able to view PII that is directly associated with the Help Desk queue associated with their work. This technical control ensures that users can only access PII that is directly relevant to and necessary for the performance of their specific job duties, preventing unauthorized access to PII contained in other queues within the system. Network Access Restrictions: The KBOX system is not accessible outside of FDA's internal network, serving as an additional technical control to prevent unauthorized access to the system and the PII it contains. This restriction ensures that access to PII is limited to authorized OCI staff operating within the FDA network environment. Firewalls and Network Monitoring: The system employs firewalls and network monitoring and intrusion detection tools as additional technical safeguards to protect against unauthorized access to PII. These controls help to detect and prevent any attempts to access the system or its data in an unauthorized manner.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	FDA requires all employees and Direct Contractors to complete annual security and privacy awareness training. This training is designed to make system users, including system owners, managers, operators, contractors, and program managers, aware of their responsibilities for protecting the information being collected and maintained within the system. The Office of Digital Transformation (ODT) is responsible for tracking the completion of this annual training requirement, ensuring that all personnel remain current in their understanding of their security and privacy responsibilities.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the general annual security and privacy awareness training, intensive system-specific user training is provided for all new employees during a Special Agent Training Program. This training goes above and beyond the general security and privacy awareness training and is designed to ensure that new personnel have a thorough understanding of the specific security and privacy requirements and responsibilities associated with their use of the KBOX system and the sensitive law enforcement information it contains. Together, these two training requirements ensure that all personnel using the KBOX system are adequately informed of their responsibilities for protecting the sensitive PII and law enforcement information collected and maintained within the system.
PIA 44:	Describe the process and guidelines in place for 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 with the FDA Records Schedule 8900, Reference Materials, National Archives and Records Administration (NARA) Citation N1-088-05-1. This records retention schedule indicates that materials are destroyed or deleted when no longer needed for reference purposes. While the FDA Records Schedule 8900 generally provides for the destruction or deletion of materials 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 contained within the system. The sensitive and ongoing nature of OCI's criminal investigative mission necessitates that records be retained on a continuous basis to support active and potential future investigations. In accordance with the FDA Records Schedule 8900 and NARA Citation N1-088-05-1, records are destroyed or deleted when they are no longer needed for reference purposes. However, given OCI's need to maintain records continuously due to the nature of the law enforcement data, the destruction of records is carefully managed to ensure that no records are destroyed prematurely or in a manner that could compromise active or potential future criminal investigations.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	The following administrative, technical, and physical controls are in place to secure PII within the KBOX system: Administrative Controls: User Training: FDA requires all employees and Direct Contractors to complete annual security and privacy awareness training, and new employees receive intensive system-specific user training as part of the Special Agent Training Program. These training requirements ensure that all personnel are aware of their responsibilities for protecting the

sensitive PII and law enforcement information collected and maintained within the system.

System Documentation: System documentation is in place that advises users on the proper use of the system and the information it contains, ensuring that all personnel understand and adhere to the appropriate policies and procedures for handling PII.

Need to Know and Minimum Necessary Principles: The system implements Need to Know and Minimum Necessary principles when awarding access, ensuring that individuals are only granted access to the PII that is directly relevant to and necessary for the performance of their specific job duties.

Role-Based Access Controls: Permissions are assigned based on responsibility and position within the organization, and supervisors are responsible for approving and limiting access at the individual level while administrators control permissions within the system. OCI performs annual reviews to evaluate user access, ensuring that access permissions remain appropriate to each individual's role and responsibilities.

Configuration Management: The system administrator has developed a configuration management plan to ensure that the system baseline is maintained or updated when new releases are provided by the vendor, helping to ensure the ongoing security and integrity of the system and the PII it contains.

Technical Controls:

Multi-Factor Authentication: Users access KBOX through SSO authentication integrated with FDA's AD system, using an HHS PIV card for multi-factor authentication. This technical control ensures that only authorized individuals are able to access the system and the PII contained within it.

Firewalls: The system employs firewalls as a technical safeguard to protect against unauthorized access to the system and the PII it contains.

Network Monitoring and Intrusion Detection: Network monitoring and intrusion detection tools are employed to detect and prevent any attempts to access the system or its data in an unauthorized manner. The system administrator reviews the system audit log weekly to look for any unusual or unauthorized activity and takes appropriate action to ensure any anomalies are addressed.

Network Access Restrictions: The KBOX system is not accessible outside of FDA's internal network, serving as an additional technical control to prevent unauthorized access to the system and the

PII it contains.

Data Backup: The KBOX system and user data are backed up regularly, and the system owner has an Information System Contingency Plan (ISCP) in place to support a timely restoration of service in the event of system failure, ensuring the availability and integrity of PII contained within the system.

NIST SP 800-53 Controls: Additional security controls have been selected from NIST's Special Publication (SP) 800-53, as determined using FIPS 199, to provide appropriate protection for the system based on its moderate security categorization.

Physical Controls:

Secure Facility: All system servers are located at facilities protected by security guards and locked facility doors, ensuring that physical access to the system's hardware is restricted to authorized personnel only.

Climate Controls: Climate controls are in place at the facilities where system servers are located, ensuring that the physical environment is maintained at appropriate conditions to protect the system's hardware and the PII it contains from damage or loss due to environmental factors.

OCI Data Center: The primary system component, OCI-helpdesk, is located at the OCI Data Center, which is subject to the physical security controls described above, ensuring that the system's hardware and the PII it contains are adequately protected from unauthorized physical access.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	7/8/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	7/8/2026
SOP Review 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.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	7/13/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 7/13/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	5

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	7/16/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
7/16/2026 2:18 PM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PTA 01	BLAND, CRYSTAL	7/9/2026	Per FDA Email: The PIA is experiencing an Archer error with Question #3 of the general information (Q-3 “Does the system have or is it covered by a Security Authorization to Operate (ATO)?” The FDA instance of Archer is automatically entering the answer “No,” which is incorrect. **The ATO date is 3/9/2026 .** At this time, we are unable to update Archer to reflect the correct answer “Yes.”	FW_ PTA _ PIA 5271678 is ready for APA Review.pdf OII OCI Kbox Help Desk System_SOP approved.pdf