PTA / PIA: FDA - TSS - QTR2 - 2026 - FDA5269936

Created Date: 5/12/2026 2:19 PM Last Updated: 5/29/2026 6:17 PM

General Information

PTA / PIA Name:	FDA - TSS - QTR2 - 2026 - FDA5269936	**PTA / PIA ID:**	4477405
Component Name:	FDA - OII Threat Screening Service	**ATO Boundary Name:**	OII Case and Workload Management
Overall Status:	Complete	**# of Days - Open:**	29
Submitter:		**Submit Date:**	5/14/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
Office:		**OpDiv:**	FDA
Security Categorization:	High		
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?	No
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.	1/13/2025
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	Sabrina Mosley
PTA 01A:	POC Title and Organization	Information System Owner Office of Inspections and Investigations (OII)
PTA 01B:	POC Email Address	sabrina.mosley@fda.hhs.gov
PTA 01C:	POC Phone Number	240-731-8624
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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	The Office of Inspections and Investigations (OII)

	what the functions of the system are and how the system carries out those functions in support of HHS.	Threat Screening Service (TSS) is a mission-critical backend system designed to enhance the security of the U.S. food supply by enabling the Food and Drug Administration (FDA) to screen individuals associated with imported food shipments against federal threat databases. The system operates entirely as a backend data ingestion and processing pipeline with no frontend user interface, functioning as a Representational State Transfer (REST)-based service with no publicly accessible Uniform Resource Locator (URL). TSS accomplishes its mission by ingesting threat screening data from the Federal Bureau of Investigation (FBI) Threat Screening Center (TSC) into the FDA Extranet. This data transfer is facilitated through the Threat Screening Service Interface (TSSI), a Spring Boot-based REST service that securely accepts files from the FBI's TSC over the extranet. Once received, the Threat Screening System Data Processor (TSSDP) processes the incoming extensible markup language (XML) files and stores the data into an Oracle database for use by downstream applications. A third sub-component, the Threat Screening System Targeting (TSST), then screens the watchlist data against incoming Prior Notices (PNs) — advance notifications submitted by importers for food shipments entering the United States — and generates matching flags based on rule criteria defined by the FDA's Division of Food Defense Targeting (DFDT). The TSS supports the broader Prior Notice Manager (PNM) application ecosystem in several important ways. It enables the implementation of automatic rules to identify and target potentially high-risk food shipments, notifies reviewers of data irregularities, allows users to review Prior Notices against threat screening data from within the PNM application, and supports the development of Matrix rules based on TSS data. The results generated by the TSS are also shared with the Division of Targeting and Analysis (DTA), which relies on this data to fulfill its core mission of protecting the U.S. food supply through proactive, risk-based analysis and targeting. This sharing is authorized by an Interconnection Security Agreement (ISA) between the FDA and FBI, which was renewed on July 29, 2024, and is valid for three years. TSS is a backend service only and does not have a direct user-facing interface through which individuals log in or interact with the system. Direct access to the TSS is limited to developers and contractors — specifically Department of Health and Human Services (HHS) and OII Direct Contractors — who require access for purposes of troubleshooting, system administration, and development activities. All authorized system users, including both FDA employees serving in developer roles and Direct Contractors with valid network accounts, must obtain formal supervisor approval and signature before access is granted.

		Authentication is managed through the FDA Enterprise Active Directory, which maintains user credentials independently of the TSS and verifies user identity before granting access to the system. The agency reviews the system access list on a quarterly basis to adjust authorized users' access roles and permissions and to delete unneeded accounts. Access to personally identifiable information (PII) within the system is further restricted through role-based access controls, whereby the supervisor of each authorized system user indicates on database access forms the minimum level of access required to complete their job responsibilities. All FDA personnel are also required to complete mandatory security and privacy awareness training at least once per year, with additional system-specific training provided to those who interact directly with the TSS.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	TSS collects, maintains, and shares ten broad categories of information. The first category is biographical data, which captures fundamental identifying information about individuals, including their full names (with various forms and attributes), dates of birth (with accuracy indicators), sex, physical disabilities, and occupations. It also records whether the person is deceased or alive. The second category is document information, which encompasses all official identification documents associated with individuals, primarily passports but also other government-issued credentials. Specific data points include unique document numbers, issuing authorities and countries, issue and expiration dates, and any names or addresses recorded on those documents. The system tracks document-specific details with accuracy indicators and maintains references to multiple identification types per person. The third category is location data, which includes both physical addresses (street addresses, localities, states/provinces, postal codes, and countries) and precise geographic coordinates (latitude and longitude) associated with individuals. Location information is tracked with usage indicators and form attributes, and can represent current residences, historical addresses, or locations specified on identification documents. The fourth category is physical descriptors, which captures detailed information about an individual's physical appearance and identifying features, including apparent physical characteristics such as scars, marks, and tattoos, as well as biometric data such as facial images. The system records both the type and detailed descriptions of these characteristics, along with profile codes indicating the conditions under which biometric data was captured. The fifth category is asset information, which

tracks vehicles, vessels, aircraft, and other transportation assets associated with individuals. Specific data points include Vehicle Identification Numbers (VINs), registration numbers, make/model/style/year, colors, and boat identification numbers for vessels. It also maintains registration details such as the registering state/province and country, registration types, and expiration dates with accuracy indicators.

The sixth category is security classifications, which encompasses threat assessment and screening information, including Threat Screening Center (TSC) identifiers, threat names and populations, subject categories and types, handling codes and instructions, and caution information for law enforcement or security personnel. This category also tracks which government agencies have expressed interest in or issued warnings about specific individuals, along with watchlist posting indicators.

The seventh category is organizational connections, which documents an individual's affiliations with organizations, employers, or other entities, including the names of those organizations, the types of affiliations (such as employment or membership), and the countries where those organizations are located. These connections help establish patterns of association and potential security concerns.

The eighth category is criminal records, which encompasses information related to an individual's criminal history as maintained within the FBI Threat Screening Center (TSC) data ingested by the system. This information supports the threat screening mission by providing additional context for assessing the risk level associated with individuals connected to imported food shipments.

The ninth category is foreign activities, which captures information related to an individual's activities, associations, or connections in foreign countries as reflected in the FBI TSC data. This information assists in identifying individuals who may pose a heightened security risk based on their involvement in activities of concern outside the United States.

The tenth category is citizenship, which records the citizenship status and nationality of individuals as contained in the FBI TSC data ingested by the system. This information supports identity verification and threat screening by providing additional identifying context for individuals associated with food shipments entering the United States.

Records handled within TSS and the broader OII Case and Workload Management (OCWM) system are governed by National Archives and Records Administration (NARA)-approved records

		schedules, with retention and destruction periods generally ranging from 10 to 30 years after an action closes or when a record is no longer needed. More specifically, import program database records are maintained in accordance with NARA-approved citation N1-088-09-3, which designates records as temporary and requires deletion or destruction 10 years after the end of the fiscal year in which the subject regulatory action is final. Program management files fall under NARA-approved citation N1-088-07-2, which designates these records as temporary and requires deletion or destruction 10 years after the end of the fiscal year in which the subject regulatory action is final, or when the records are no longer needed for agency business, whichever comes first.
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 Enterprise 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.	The following describes why each type of information is collected, maintained, and/or shared within the Threat Screening Service (TSS), including what information is collected about each category of individuals. All information is collected from FBI TSC and pertains to members of the public — specifically individuals associated with food shipments entering the United States. Biographical data is collected from the FBI TSC to enable the FDA to identify individuals associated with food shipments and match them against known threat profiles, allowing the system to automatically flag shipments handled by persons of security concern. This information is essential for implementing automatic rules that target potentially high-risk food shipments and for enabling Prior Notice Manager (PNM) application users to review Prior Notices (PNs) against threat screening data to assess whether individuals involved in food imports pose security risks. Document information is collected to verify the authenticity of identification credentials used by individuals involved in food shipments and to cross-reference passport numbers and other official identifiers against threat databases. This enables the development of Matrix rules that can automatically screen shipment documentation for individuals using fraudulent or flagged identification documents, helping reviewers identify data irregularities that may indicate security threats. Location data is collected to identify geographic patterns and high-risk regions associated with food shipments, allowing the system to flag shipments originating from, transiting through, or destined for locations linked to known threats or suspicious activities. This information supports automatic

rules that assess risk based on the addresses and geographic coordinates of shippers, manufacturers, growers, and other parties involved in the food supply chain.

Physical descriptors are collected to enable positive identification of individuals who may attempt to use aliases or fraudulent documents when involved in food shipments, providing additional verification points beyond names and document numbers. This biometric and characteristic data allows PNM application users to confirm identities when reviewing Prior Notices and helps prevent threat actors from evading detection through identity manipulation.

Asset information is collected to track vehicles, vessels, aircraft, and other transportation assets associated with known threats, enabling the system to automatically flag food shipments transported by or associated with these assets. This data supports the development of Matrix rules that identify high-risk shipments based on transportation methods and allows reviewers to detect patterns where the same suspicious vehicles or vessels are repeatedly used for food imports.

Security classifications are collected to provide critical threat assessment information — including TSC identifiers, threat levels, subject categories, handling instructions, and watchlist status — that directly informs risk-based screening of food shipments. This information enables automatic rules to prioritize review of shipments associated with individuals or entities on watchlists and ensures that reviewers are notified of specific caution information and handling protocols when examining Prior Notices linked to security concerns.

Organizational connections are collected to document an individual's affiliations with organizations, employers, or other entities, including the names of those organizations, the types of affiliations, and the countries where those organizations are located. These connections help establish patterns of association and potential security concerns, supporting the broader mission of identifying and targeting high-risk food shipments before they enter the U.S. food supply.

Criminal records are collected from the FBI TSC to provide the FDA with additional context for assessing the risk level associated with individuals connected to imported food shipments entering the United States. An individual's criminal history may indicate a pattern of behavior relevant to food safety or national security concerns, enabling the TSS to more accurately flag shipments associated with persons who pose a heightened risk. This information supports the development of Matrix rules and automatic targeting criteria that account for the criminal backgrounds of individuals involved in the food supply chain, thereby

		strengthening the FDA's ability to identify and prioritize high-risk shipments for enhanced review. Foreign activities are collected from the FBI TSC to identify individuals whose activities, associations, or connections in foreign countries may indicate a heightened security risk to the U.S. food supply. Information about an individual's foreign activities allows the TSS to flag shipments associated with persons who may have ties to foreign organizations, governments, or activities of concern, supporting the FDA's proactive, risk-based approach to screening imported food shipments. This data enables reviewers within the PNM application to assess whether the foreign activities of individuals involved in food imports are consistent with known threat profiles maintained in federal threat databases. Citizenship is collected from the FBI TSC to support identity verification and to provide additional identifying context for individuals associated with food shipments entering the United States. An individual's citizenship status and nationality can serve as a supplementary data point when matching Prior Notice submissions against federal threat databases, helping to distinguish between individuals with similar biographical information and reducing the likelihood of false positives or missed matches. This information also supports the development of Matrix rules that incorporate nationality as a factor in risk-based targeting of imported food shipments. TSS shares its results with the FDA Division of Targeting and Analysis (DTA) through the PNM application. DTA requires access to TSS-generated results to fulfill its core mission of protecting the U.S. food supply through proactive, risk-based analysis and targeting. This sharing is authorized by an Interconnection Security Agreement (ISA) between the FDA and FBI, which was renewed on July 29, 2024, and is valid for three years. All data sharing is conducted through the PNM application, which maintains extensive auditing capabilities that track who accessed what data and when.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	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 Passport Number Vehicle Identifiers (e.g., VIN, license plate number) Biographical Information Name Date of Birth Criminal Records Foreign Activities Contact Information Mailing Address (Personal) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Sex Facial Biometric Data Citizenship Physical Characteristics (e.g., tattoos, scars, marks) Disability Information Occupation Geographic Coordinates (latitude and longitude) Organizational Affiliations
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	1,000,000 or more

PIA 25:	For what primary purpose is the PII used?	The PII collected by TSS is primarily used to identify and verify individuals associated with food shipments entering the United States, enabling the FDA to assess whether these individuals pose potential security threats to the food supply chain. More specifically, the PII allows the TSS to automatically match names, dates of birth, passport numbers, and other identifying details from PN submissions against the FBI threat databases, flagging shipments that involve persons of concern for enhanced review. The biographical and identification data enables PNM application users to conduct thorough reviews of flagged shipments by comparing the identities of shippers, manufacturers, growers, and other parties against comprehensive threat profiles that include aliases, physical characteristics, and known affiliations. By leveraging this PII, the system can implement Matrix rules that automatically target high-risk shipments based on the involvement of specific individuals, their locations, their organizational connections, or their use of particular transportation assets, thereby prioritizing FDA resources toward the most significant security concerns. The PII also supports the work of the Division of Targeting and Analysis (DTA), which relies on TSS-generated results to conduct proactive, risk-based analysis and targeting in fulfillment of its core food safety mission. Ultimately, the PII serves to protect public health and national security by ensuring that food imports associated with known or suspected threat actors receive appropriate scrutiny before entering the U.S. food supply.
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 — the information is used solely for the primary threat screening and food safety purposes.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The primary legal authority governing the TSS is the Federal Food, Drug, and Cosmetic Act (FD&C Act), codified at 21 U.S.C. 301, as amended by the Food Safety Modernization Act (FSMA), 21 U.S.C. 220. Relevant provisions of this authority can be found at 21 U.S.C. 331 and 350–387, which establish the FDA's broad regulatory authority over food safety and the admissibility of imported food products into the United States. The second key legal authority is the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, commonly referred to as the Bioterrorism Act, Public Law 107-188. This authority specifically underpins the FDA's ability to collect and share information related to the security of the U.S. food supply, including the review of Prior Notices (PNs) for imported food shipments and the assessment of risks associated with those shipments. Relevant provisions include those codified at 21 U.S.C. 350c and 21 U.S.C. 381, which govern the FDA's authority to require advance notice of imported food and to refuse admission of food shipments that pose a security risk. It is under this authority, in particular, that the FDA's requirement to screen all parties involved in the food supply chain — without exception or opt-out — is grounded. Together, these legal authorities establish the statutory foundation for the TSS's collection, use, maintenance, and sharing of PII in support of the FDA's mission to protect public health and national security through risk-based screening of imported food shipments.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	The PII data elements used to retrieve records in the system include name, date of birth, passport number, and other biographical and document identifiers ingested from the FBI TSC. These elements correspond to individuals associated with food shipments entering the United States, who may be members of the public, and are used to match Prior Notice (PN) submissions against federal threat databases for screening purposes.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-10-0002 - Regulated Industry Employee Enforcement
PIA 30:	Identify the sources of PII in the system.	Government Sources Other Federal Entities
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.	TSS ingests its data exclusively from the FBI TSC, which is a federal government entity. Because the information flowing into the TSS originates from another federal agency rather than being collected directly from members of the public, the TSS does not trigger the Paperwork Reduction Act (PRA) requirements that would otherwise necessitate an OMB information collection approval number. The PRA generally applies to federal agencies when they collect information directly from ten or more members of the public, and since the TSS operates entirely as a backend data ingestion system that receives information from the FBI rather than soliciting it from individuals, this requirement does not apply.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	DTA requires access to the results generated by the TSS application to fulfill its core mission of protecting the U.S. food supply through proactive, risk-based analysis and targeting. The TSS application's function of identifying and verifying individuals associated with food shipments is a critical data source that directly supports DTA's analytical and operational responsibilities. Without this access, DTA's targeting efforts would be significantly hindered, creating a critical gap in the FDA's defensive posture.

PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	Two agreements are currently in place to authorize the information sharing and disclosure described in this PIA. The first is an Interconnection Security Agreement (ISA) between the FDA and the FBI, which governs the secure exchange of threat screening data between the two agencies. This agreement was renewed on July 29, 2024, and is valid for a period of three years, meaning it is currently active through approximately July 2027. The ISA covers the connection between the FBI's Threat Screening Center (TSC) and the FDA's Threat Screening Service (TSS) and establishes the terms and conditions under which the FBI TSC transmits threat screening data to the FDA for ingestion into the TSS. The second is the data sharing arrangement governing the disclosure of TSS-generated results to the FDA's Division of Targeting and Analysis (DTA) within HHS. Because both the TSS and DTA operate within the same Operating Division and the sharing occurs entirely through the Prior Notice Manager (PNM) application — which maintains extensive auditing capabilities that track who accessed what data and when — this internal sharing is governed by the access control and auditing framework established within the PNM application environment. DTA personnel access TSS-generated results exclusively through the PNM application, and all such access is subject to the role-based access controls, supervisory approval requirements, and quarterly access reviews that govern the broader OII Case and Workload Management (OCWM) system of which the TSS is a component.

PIA 32D:	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.	The process for logging, tracking, and accounting for the sharing and disclosure of PII within TSS is handled indirectly through the PNM application rather than through TSS itself. Because the TSS is a backend system only — functioning solely as a data ingestion and processing pipeline with no frontend user interface — there is no direct mechanism within the TSS to track or log the sharing and disclosure of PII. All data that is shared from TSS is done through the PNM application, which serves as the primary interface through which TSS-generated results are accessed and used by authorized personnel such as those in DTA. The PNM application, however, does maintain extensive auditing capabilities that compensate for the TSS's lack of direct tracking functionality. Specifically, the PNM application tracks who accessed what data and when they accessed it, providing a comprehensive audit trail for all interactions with the PII that flows through the TSS into the PNM environment. This audit trail capability ensures that the sharing and disclosure of PII can be accounted for at the application level, even though the TSS itself does not have the technical capability to perform this tracking function independently. It is worth noting that while these auditing capabilities within PNM provide a meaningful compensating control, the reliance on a downstream application for logging and tracking purposes represents a limitation of the current system architecture. FDA employees or other authorized personnel seeking to review audit logs related to PII access and disclosure would need to do so through the PNM application's auditing interface rather than through any direct TSS logging mechanism.
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 opt-out method or consent mechanism in place for the collection of PII within TSS. The PII maintained by TSS is not collected directly from the individuals to whom it pertains. Rather, it is ingested exclusively from the FBI TSC, meaning that the individuals whose PII is maintained in the system do not themselves submit that information to the FDA. The voluntary classification therefore reflects the fact that no individual is legally compelled under the Privacy Act to directly provide their PII to the TSS. However, it is worth noting that this voluntary classification exists alongside the practical reality that there is no opt-out mechanism available for individuals whose PII appears in the FBI's threat databases and is subsequently ingested into the TSS. TSS serves a critical national security and public health protection function that requires screening of all individuals associated with food shipments entering the United States. Allowing individuals to opt out of threat screening would create dangerous security vulnerabilities by enabling threat actors to evade detection and potentially introduce contaminated, or otherwise harmful food products into the U.S. food supply. The PII is collected from the FBI Threat Screening Center rather than directly from individuals, meaning it represents intelligence and law enforcement data about persons who pose potential security threats, and such individuals cannot be permitted to decline screening that protects the American public. The FDA has a statutory obligation under the Public Health Security and Bioterrorism Preparedness and Response Act and other food safety laws to review Prior Notices and assess risks associated with imported food, which necessitates the ability to screen all parties involved in the food supply chain without exception. Furthermore, participation in importing food into the United States is a voluntary commercial activity subject to regulatory requirements, and entities choosing to engage in this activity must accept that all associated individuals will be screened against threat databases as a condition of doing business, making opt-out incompatible with the government's responsibility to safeguard the nation's food supply.
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 can be no process to notify individuals and obtain their consent when major changes occur to the TSS system because doing so would compromise the effectiveness of threat screening operations and potentially alert threat actors to law enforcement and intelligence capabilities. Notifying individuals that they are included in threat databases or that screening methodologies have changed would provide adversaries with intelligence about what triggers enhanced scrutiny, allowing them to evade detection or circumvent security measures.

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.	Several avenues are available to individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII maintained about them is inaccurate. The first avenue is available to FDA personnel specifically. FDA personnel have the Employee Resource and Information Center (ERIC), which provides a resource through which internal FDA employees can raise concerns about the handling of their PII in general. The second avenue available exclusively to FDA personnel is the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), which serves as another internal resource for addressing concerns related to PII handling and potential security incidents involving personal information. For individuals who are not FDA personnel — including members of the public whose PII may be maintained within TSS — the primary avenue for resolving concerns is through the FDA Privacy Office. The FDA Privacy Office is accessible through multiple contact methods, all of which are publicly listed on the FDA's official website at fda.gov. These contact methods include email, phone, and standard mail, ensuring that individuals have multiple options for reaching the appropriate office to raise their concerns regardless of their preferred mode of communication. It is worth noting an important practical limitation in the context of TSS specifically. Because the PII maintained by the TSS originates from the FBI TSC rather than being collected directly from individuals, the FDA's ability to correct or amend inaccurate PII within the system may be limited. The FBI TSC is identified in the PIA as the entity responsible for providing accurate information to the FDA, meaning that concerns about the accuracy of specific PII data points may ultimately need to be directed to or coordinated with the FBI TSC rather than resolved solely through FDA channels. Individuals with concerns about the accuracy of their information in federal threat databases may therefore need to engage with both the FDA Privacy Office and the appropriate FBI channels to fully resolve their concerns.
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 FBI TSC is the entity responsible for providing accurate information to the FDA. Because TSS ingests its data exclusively from the FBI TSC rather than collecting it directly from individuals, the responsibility for ensuring the accuracy of the underlying PII data rests primarily with the FBI TSC as the originating source. The FDA's role in this regard is therefore dependent on the FBI TSC's own processes and procedures for maintaining accurate threat screening data, and individuals with concerns about the accuracy of their PII, as noted in PIA 36, may need to engage with both the FDA Privacy Office and appropriate FBI channels to fully resolve those concerns.

		Regarding integrity and availability, these two elements are protected through the security and privacy controls selected and implemented as part of the system's Authority to Operate (ATO) process. Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process and are appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. The TSS has been categorized as a high impact information system, meaning that the security controls implemented to protect the integrity and availability of its data are commensurate with the elevated risk level associated with the sensitive nature of the PII and threat screening data it maintains. Technical safeguards such as firewalls, encryption, and network monitoring and intrusion detection tools further support the integrity and availability of the PII maintained in the system, as do physical controls including system servers located at facilities protected by guards, locked facility doors, and climate controls. The broader OCWM system's administrative procedures provide some relevant compensating mechanisms. Specifically, the agency reviews the system access list on a quarterly basis to adjust authorized users' access roles and permissions and to delete unneeded accounts, which helps ensure that only personnel with a current and legitimate need to access the PII are able to do so. Additionally, all FDA personnel are required to complete mandatory security and privacy awareness training at least once per year, which reinforces awareness of the importance of maintaining only relevant and necessary PII within agency systems. The retention and destruction schedule governing the TSS also contributes indirectly to ensuring the ongoing relevancy of PII maintained in the system. As governed by National Archives and Records Administration (NARA)-approved citation N1-088-09-3, import program database records are designated as temporary and must be deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final, ensuring that PII is not retained indefinitely beyond its useful and relevant period. Program management files fall under NARA-approved citation N1-088-07-2, which similarly governs the retention and destruction of those records in accordance with established federal records management requirements.
PIA 38:	Identify who will have access to the PII in the system.	Developers Contractors
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors

PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Developers require access to PII within TSS for the purposes of troubleshooting issues with the system and monitoring system performance. Because the TSS is a backend data ingestion and processing pipeline that handles sensitive threat screening data sourced from the FBI TSC, developers must be able to access the underlying data in order to diagnose and resolve technical issues that may arise in the system's operation, ensure that data is being ingested, processed, and stored correctly, and maintain the overall performance and reliability of the system in support of its mission-critical functions. Contractors require access to PII within the TSS to support the information technology (IT) team in the areas of administration, troubleshooting, and development of the system. More specifically, the contractors identified in this PIA are Department of Health and Human Services (HHS) and Office of Inspections and Investigations (OII) Direct Contractors, who may serve as users, administrators, and developers with respect to the TSS system. In these capacities, Direct Contractors require access to PII to perform the same types of administrative, troubleshooting, and development functions as FDA developers, ensuring the continued operation, maintenance, and improvement of the TSS in support of the FDA's food safety and national security mission. It is important to note that access to PII for both groups is governed by strict administrative and technical controls designed to ensure that individuals access only the minimum amount of information necessary to perform their job functions. The supervisors of all authorized system users indicate on user database access forms the minimum access required to complete their jobs, and access is restricted based on role-based criteria. Additionally, the agency reviews the system access list on a quarterly basis to adjust authorized users' access roles and permissions and to delete unneeded accounts, ensuring that access to PII remains limited to those with a current and legitimate need. All personnel with access to PII are also required to complete mandatory security and privacy awareness training at least once per year, with additional system-specific training provided to those who interact directly with the TSS.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The primary administrative procedure governing access to PII requires that all authorized system users, including both FDA employees serving in developer roles and Direct Contractors with valid network accounts, obtain formal supervisor approval and signature before access to TSS is granted. This approval process ensures that access to PII is authorized at the supervisory level and is granted only to individuals with a demonstrated and legitimate need to access the system in support of their job responsibilities. Once access has been granted, the agency conducts periodic reviews of the system access list on a quarterly basis. These quarterly reviews serve to adjust authorized users' access roles and permissions as needed to reflect changes in job responsibilities or organizational requirements, and to delete unneeded accounts from the system to ensure that access to PII remains limited to those with a current and active need. This regular review process helps prevent unauthorized or unnecessary access to PII by ensuring that the system access list remains accurate and up to date. In terms of the technical implementation of these administrative procedures, the supervisors of all authorized system users indicate on user database access forms the minimum level of access required to complete their job responsibilities. The scope of access is then restricted based on role-based criteria, ensuring that individuals access only the minimum amount of PII necessary to perform their assigned functions in accordance with the principles of Need to Know and Minimum Necessary access. This role-based approach to access control provides an additional layer of protection for the sensitive PII maintained within the TSS by limiting the potential impact of unauthorized access or misuse of the system.

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 primary technical method in place is a role-based access control system. Under this approach, a user's supervisor indicates on user database access forms the minimum level of access required for that user to complete their job responsibilities within the Threat Screening Service (TSS). The scope of access is then technically restricted based on these role-based criteria, meaning that the system itself enforces the access limitations specified by the supervisor rather than relying solely on individual users to self-limit their access to Personally Identifiable Information (PII). This ensures that even if a user were inclined to access more information than necessary, the technical controls built into the system would prevent them from doing so. This role-based access control approach is further supported by the broader Oracle-based security architecture for the OII Case and Workload Management (OCWM) system, of which the TSS is a component. Specifically, the OCWM system implements two primary Oracle database roles that govern the scope of data access available to different categories of users. The first role, Operational and Administrative System for Import Support (OASIS)READ, grants select-only privileges on all OCWM tables, limiting users assigned to this role to read-only access to the data. The second role, OASISUSER, grants select, update, delete, and insert privileges on all OCWM tables, providing a broader but still defined and controlled scope of access for users who require the ability to modify data in the performance of their job responsibilities. Additional technical safeguards that support the minimum necessary access principle include the use of Single Sign-On (SSO) functionality, which integrates with Oracle's SSO feature to authenticate users through the Food and Drug Administration (FDA) Enterprise Active Directory before granting access to the appropriate applications. The system also implements an application-level security procedure that runs each time a user logs in, which determines whether the user is running a valid program and sets the user's application roles as global variables that control which modules, menus, and application functions are available to that user throughout their session. This ensures that role-based access restrictions are consistently enforced across all components of the system for the duration of each user session. Furthermore, technical safeguards such as firewalls, encryption, and network monitoring and intrusion detection tools provide additional layers of protection for the PII maintained within the TSS, helping to prevent unauthorized access to sensitive data by both internal and external actors.

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.	All FDA personnel are required to complete mandatory security and privacy awareness training at a minimum of once per year. This annual training requirement applies universally to all personnel who interact with TSS, regardless of their specific role or level of access, ensuring that everyone with access to the sensitive PII and threat screening data maintained by the TSS is regularly reminded of their responsibilities for protecting that information. Completion of the annual security and privacy awareness training course is tracked by the Office of Digital Transformation (ODT), which maintains records of training completion to ensure that all personnel remain current with their training requirements.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	System users of TSS receive the following training above and beyond the mandatory annual general security and privacy awareness training required of all FDA personnel. System users receive system-specific training tailored to the particular functions, responsibilities, and requirements associated with their use of the TSS. This system-specific training is designed to ensure that users understand the unique characteristics of the TSS, including the sensitive nature of the threat screening data and Personally Identifiable Information (PII) it maintains, and the specific procedures and protocols that govern the appropriate handling, use, and protection of that information within the system. System users are required to review and adhere to the Rules of Behavior governing the use of the TSS. The Rules of Behavior establish the specific expectations and responsibilities for all users of the system with respect to the protection of the sensitive information it collects and maintains, and users must acknowledge their understanding of and commitment to these rules as a condition of being granted access to the system. System users may obtain additional privacy guidance from the agency's privacy officials as needed. This provision ensures that users have access to expert guidance and support when they encounter specific questions or concerns related to the handling of PII within the TSS that may not be fully addressed by the system-specific training or the Rules of Behavior, providing an additional layer of assurance that the sensitive information maintained by the system is handled appropriately at all times.

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).	The records handled within TSS and the broader OCWM system are governed by a variety of National Archives and Records Administration (NARA)-approved records schedules specific to the nature of the records being maintained. The retention and destruction periods for these records generally range from 10 to 30 years after an action closes or when a record is no longer needed, reflecting the long-term regulatory and enforcement responsibilities associated with the FDA's import surveillance and food safety mission. More specifically, import program database records — which represent the primary category of records maintained within the TSS — are governed by NARA-approved citation N1-088-09-3. Under this records schedule, import program database records are designated as temporary records, meaning they are not intended for permanent retention. These records must be deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final, ensuring that PII is not retained indefinitely beyond its useful and relevant period while still allowing sufficient time for the records to support ongoing regulatory and enforcement activities. Program management files associated with the TSS and the broader OCWM system are governed by a separate NARA-approved citation, N1-088-07-2. Under this records schedule, program management files are designated as temporary records. These records must be deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final, or when the records are no longer needed for agency business, whichever comes first, ensuring that program management records are not retained beyond their useful period while still supporting the FDA's ongoing regulatory and administrative responsibilities.

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.	Administrative safeguards governing the protection of PII within the TSS include mandatory annual security and privacy awareness training for all FDA personnel, system-specific training for those who interact directly with the TSS, and system documentation that advises on proper use. Access is awarded in accordance with the principles of Need to Know and Minimum Necessary, with supervisors required to indicate on user database access forms the minimum level of access required for each user to complete their job responsibilities. The agency also conducts quarterly reviews of the system access list to adjust access roles and permissions and to delete unneeded accounts, ensuring that access to PII remains limited to those with a current and legitimate need. Technical safeguards include the use of firewalls, encryption, and network monitoring and intrusion detection tools to protect the integrity and availability of PII maintained within the system. Role-based access controls, implemented through Oracle database roles and enforced through SSO authentication via the FDA Enterprise Active Directory, ensure that users can access only the minimum amount of information necessary to perform their assigned functions. An application-level security procedure further enforces role-based restrictions each time a user logs in, controlling which modules, menus, and application functions are available throughout each user session. Physical controls include that all system servers are located at facilities protected by security guards, locked facility doors, and climate controls, ensuring that the physical infrastructure supporting the TSS is secured against unauthorized access and environmental hazards. Additional controls have been selected from National Institute of Standards and Technology (NIST) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199, and are commensurate with the TSS's High impact security categorization.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/14/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/14/2026
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:**	5/21/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 5/21/2026 All comment(s) addressed, this PIA is ready for SAOP review and approval. 5/14/2026 Please see comment(s) and update accordingly. **PTA-5:** Per PIA-22 and PIA-22A: please include "criminal records, foreign activities, and citizenship" in your response.	**# of Days - APA Review:**	7

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	5/29/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	8

SAOP Signature

Date	User	Type	Name	Original Value	New Value
5/29/2026 3:00 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	5/13/2026	5/13/2026 Per FDA's Email: The attached PIA (OII Threat Screening Service) is SOP approved and should be in your queue for review. I have attached an exported a copy for you if you are unable to view in the HHS instance of Archer. 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 1/13/2025. At this time, we are unable to update Archer to reflect the correct answer “Yes.”	5-12-2026 EMAIL_FW_ PTA _ PIA 5269936 is ready for APA Review.pdf OII Threat Screening Service SOP approved.pdf
PTA 05	BLAND, CRYSTAL	5/14/2026	Per PIA-22 and PIA-22A: please include "criminal records, foreign activities, and citizenship" in your response.	