PTA / PIA: FDA - eSAF - QTR2 - 2026 - FDA5270619

Created Date: 5/28/2026 10:47 AM Last Updated: 6/18/2026 2:18 PM

General Information

PTA / PIA Name:	FDA - eSAF - QTR2 - 2026 - FDA5270619	**PTA / PIA ID:**	4528660
Component Name:	FDA - OII Electronic State Access to FACTS	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	29
Submitter:		**Submit Date:**	5/26/2026
Next Assessment Date:	06/17/2029	**Expiration Date:**	6/17/2029
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?	No
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
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.	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) has made no changes to Office of Inspections and Investigations (OII) Electronic State Access to the Field Accomplishments & Compliance Tracking System (eSAF) 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.	The Electronic State Access to the Field Accomplishments & Compliance Tracking System (eSAF) is an external-facing, publicly accessible platform operated by the Office of Inspections and Investigations (OII) within the Food and Drug Administration (FDA). The system serves as a critical bridge between the FDA and state contractors, enabling the agency to automate and streamline the management of inspection work performed by state contractors under cooperative agreements. Specifically, eSAF automates the issuance of work requests to state contractors and allows those contractors to electronically enter and update inspection results. The system also supports business processes for capturing and tracking inspection data performed by states and provides state contractors with access to limited firm data maintained in the Field Accomplishments & Compliance Tracking System (FACTS). The subject of a separate PIA. This access enables state contractors to identify firms considered to be "high-risk" and to obtain information about past inspections and violations for firms within their jurisdiction, thereby supporting the broader Health and Human Services (HHS) mission of ensuring public health and safety through effective regulatory oversight. There are two primary categories of users who access eSAF: state contractor personnel and FDA personnel. Both user groups access the system through a secure, multi-factor authentication (MFA) process via the publicly accessible uniform resource locator (URL) at https://esaf.fda.gov/eSAF. Users must first provide a unique username and password, after which they are required to complete a second authentication step by entering a one-time password (OTP) that is sent to their registered email address. The system maintains role-based access controls, ensuring that different user roles are granted permissions appropriate to their specific responsibilities within the eSAF workflow.

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.	eSAF collects and maintains work request and assignment information to facilitate the automation of work requests to state contractors. This includes assignment details such as status, background information, and target completion dates. The system also maintains contract numbers and state agency assignments, work descriptions and operation details, request dates and completion tracking information. Program Assignment Codes (PAC) and product codes are tracked along with remarks and follow-up information to ensure proper categorization and monitoring of all work activities. The system also collects and maintains inspection-related data, including inspection dates, inspection conclusions and classifications, and hours spent on inspections. Additionally, eSAF tracks refusal codes and reasons when inspections cannot be completed, sample indicators and descriptions, and investigation-specific data including investigation identification (ID)s and reasons for investigations. eSAF maintains firm and establishment data sourced from FACTS. This includes Firm Establishment Identifier (FEI) numbers, physical addresses (including address lines, city, state, zip code, and country), and separate mailing addresses (an alternative location where a business or firm receives mail, packages, and official correspondence, distinct from its physical street location). Contact information for firms, such as phone numbers and email addresses, are also stored for communication purposes. Finally, the system collects and maintains personnel information for both FDA employees and state contractors. This includes first names, last names, middle initials or names, person IDs, and Workforce Administration and Management (WAAM) user IDs for system integration, as well as contact details such as email addresses and phone numbers with area codes and extensions. eSAF database records are maintained in accordance with National Archives and Records Administration (NARA) approved citation N1-088-09-3, which designates records as temporary and requires that they be deleted or destroyed 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, with retention and destruction periods generally ranging from 10 to 30 years after an action closes or when a record is no longer needed.
PTA 05A:	Are user credentials used to access the system?	Yes

PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Password Email Address
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.	Work request and assignment information, including assignment details, contract numbers, state agency assignments, work descriptions, PAC and product codes, request dates, and completion tracking information, is collected and maintained in order to facilitate the automation and management of inspection work requests issued to state contractors. This information ensures proper categorization, monitoring, and follow-up of all work activities conducted on behalf of the FDA under cooperative agreements with state partners. Inspection data, including inspection dates, conclusions, classifications, hours spent, refusal codes, sample indicators, and investigation IDs, is collected and maintained in order to document and track the results of inspections and investigations performed by state contractors. This information supports the FDA's regulatory oversight responsibilities and ensures accountability for inspection findings and regulatory decisions, even when inspections are carried out by state contractors rather than FDA personnel directly. Firm and establishment data sourced from FACTS, including FEI numbers, physical and mailing addresses, and contact information such as phone numbers and email addresses, is collected and maintained in order to enable communication with establishments subject to FDA oversight, identify responsible parties at inspected facilities, coordinate inspection scheduling and logistics, provide inspection findings and follow-up requirements, and ensure that regulatory notifications reach the appropriate individuals within regulated firms. Information collected about state contractor inspectors and lead investigators includes first names, last names, middle initials or names, person IDs, WAAM user IDs, email addresses, and phone numbers with area codes and extensions. This information is collected and maintained in order to track who performs inspections on behalf of the FDA, ensure proper credentialing and qualifications, facilitate communication regarding inspection assignments and results, maintain accountability for inspection activities, and document the chain of custody for inspection findings and regulatory decisions. This information is also shared with FDA district offices and program managers in order to coordinate inspection assignments, review inspection results, and ensure quality oversight of state contractor work, given that the FDA maintains ultimate responsibility for

		regulatory oversight even when inspections are performed by state contractors under cooperative agreements. Information collected about FDA employees and personnel includes first names, last names, middle initials or names, person IDs, WAAM user IDs, email addresses, and phone numbers with area codes and extensions. This information is collected and maintained in order to manage work assignments and operations, track organizational responsibilities and reporting structures, control system access and permissions, maintain accountability for regulatory decisions and actions, document supervisory reviews and approvals, and support workforce management and resource allocation. Information collected about firm employees and points of contact includes contact details such as phone numbers and email addresses. This information is collected and maintained in order to enable communication with establishments subject to FDA oversight, identify responsible parties at inspected facilities, coordinate inspection scheduling and logistics, provide inspection findings and follow-up requirements, and ensure that regulatory notifications reach the appropriate individuals within regulated firms. It is important to note that the submission of this information by firm personnel is voluntary, and individuals may object to or discuss inspection observations with the FDA representative during or after the inspection.
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://esaf.fda.gov/eSAF
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 eSAF website serves as an external-facing, publicly accessible platform that enables the FDA to automate and streamline the management of inspection work performed by state contractors under cooperative agreements. The website supports the full lifecycle of inspection work request management, allowing the FDA to issue work requests to state contractors electronically, and enabling state contractors to enter and update inspection results in return. Additionally, the website provides state contractors with access to limited firm data maintained in FACTS, which allows them to identify firms considered to be "high-risk" and to obtain information about past inspections and violations for firms within their jurisdiction. Access to the eSAF website is provided to two primary categories of users: state contractor personnel and FDA personnel. The system maintains role-based access controls, with different user roles having different permissions and access to specific functionality based on their responsibilities within the eSAF workflow. The approximate number of individuals whose personally identifiable information (PII) is maintained in the system falls within the range of 100 to 499 individuals, reflecting the relatively limited and specific user base of the platform. Users access the eSAF website through the publicly accessible URL at https://esaf.fda.gov/eSAF. Although the login page is publicly accessible, access to the system's functionality is restricted to authorized users through a secure MFA process. Users must first provide their unique username and password credentials. Upon successfully entering those credentials, users must then complete a second authentication factor by receiving and entering an OTP that is emailed to their registered email address. This email-based OTP provides an additional layer of security beyond the static password, helping to ensure that only authorized individuals are able to access the system and its data. FDA personnel may also use HHS Personal Identity Verification (PIV) cards as a credential type, while non-HHS users, such as state contractors, authenticate using their email address and password in conjunction with the emailed OTP.
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?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
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.	Biographical Information Name User Credentials Contact Information Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Other Other
PIA 22A:	Identify the “other” type(s) of personally identifiable information (PII) not mentioned in the above list.	Person IDs WAAM user IDs
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
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100 – 499
PIA 25:	For what primary purpose is the PII used?	The PII maintained in eSAF is used primarily to facilitate communication between the FDA and state inspectors operating under FDA contract. Specifically, the FDA uses the PII in eSAF to provide work requests to state inspectors, and state inspectors in turn use the system to report inspection results and recall audit check information back to the FDA. This exchange of information is essential to ensuring the effective coordination and oversight of inspection activities conducted by state contractors on behalf of the FDA under cooperative agreements.
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 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	The legal authorities governing the use and disclosure of information in eSAF are rooted in two foundational pieces of federal legislation. The first is the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374, which provides the FDA with the authority to conduct inspections of regulated establishments and governs the collection and use of information gathered in the course of those inspections. The second is the Public Health Service Act, 42 U.S.C. 262-264, which further establishes the legal framework under which the FDA collects, maintains, and shares information in support of its public health and regulatory mission. Together, these statutes provide the legal basis under which all PII in eSAF is collected voluntarily and shared with state partners to assist with contracted inspections.
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.	Government Sources Within the OPDIV State/Local/Tribal
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 eSAF because the system does not collect any information directly from the general public. While the eSAF login page is accessible via a public URL, access to the system and its data collection functions is strictly restricted to authorized users — specifically, FDA personnel and state contractors operating under cooperative agreements with the FDA. Members of the general public are unable to access the system's functionality or submit any information through the platform. The Paperwork Reduction Act, which governs the requirement for OMB information collection approval numbers, applies to federal agencies when they collect information from members of the public. Since all information collected through eSAF is limited to authorized FDA personnel and state contractors, and no information is collected from the general public, the system falls outside the scope of this requirement and therefore does not require an OMB information collection approval number.
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.	State or Local Agency/Agencies
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The PII is shared and disclosed with State partners to assist with contracted inspections.

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)).	The information sharing and disclosure activities conducted through eSAF are governed by a series of Information Sharing Agreements (ISAs) established between the FDA and various state partner agencies. The following ISAs are currently in place: The "2024 Maryland DH 3 Year Renewal ISA_Final" is an ISA with the State of Maryland that expires on November 1, 2027. The "2024 Iowa DIAL Lab 3 Year" is an ISA with the Iowa Department of Inspections that expires on November 1, 2027. The "2024 Kansas DA_3 Year Renewal ISA" is an ISA with the Kansas Department of Agriculture that expires on November 1, 2027. The "2024 Illinois DPH 3 Year Renewal ISA_Final" is an ISA with the Illinois Department of Public Health that expires on November 1, 2027. The "2024 Alaska DEC_3 Year Renewal ISA" is an ISA with the Alaska Department of Environmental Conservation that expires on November 1, 2027. The "2023 Jul 28 Texas DSHS 3 Year ISA_Final Signed" is an ISA with the Texas Department of State Health Services that expires on November 1, 2027. The "Minnesota DA ISA Renewal Final Signed" is an ISA with the Minnesota Department of Agriculture that expires on June 30, 2029.
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.	All PII is given voluntarily and gathered under the authority of the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. 374; Public Health Service Act, 42 U.S.C. 262-264 as part of a regulated inspection or investigation. Before PII can be shared, non-disclosure agreements, memorandum of understanding, and information sharing agreements must be documented.
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.	The method for notifying individuals and obtaining consent for the collection of their PII in eSAF varies depending on the category of individual involved, as described below. Firm Personnel and Establishment Points of Contact Establishment personnel provide their PII voluntarily. As such, the act of voluntarily providing their information serves as the primary means of consent for its collection. Firm personnel retain the right to object to or discuss inspection observations with the FDA representative during the course of the inspection itself. Additionally, individuals may contact the FDA after the inspection has been completed through various communication channels, all of which are listed on FDA.gov, including email, phone, and standard mail. Furthermore, there is a review process during the inspection that allows a firm point of contact to review the final inspection reports and identify anything that they believe to be inaccurate, providing an additional opportunity for individuals to engage with and respond to the information collected about them. FDA Personnel FDA employees are required to provide their name and work contact information as a condition of obtaining authorization to access the eSAF system. In this context, the provision of PII is a mandatory requirement for system access, and consent is obtained as part of the system access authorization process. FDA personnel are made aware of this requirement as part of the system onboarding process, and all system users are required to review and adhere to the Rules of Behavior governing the use of the system and the handling of PII contained within it.

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.	If FDA practices change regarding the collection or use of PII in eSAF, the agency will provide any required notice and obtain consent from individuals whose PII is maintained in the system. The FDA has identified several methods through which such notification and consent may be carried out, depending on the nature of the change and the individuals affected. These notification procedures may include any of the following: Federal Register notices, which provide formal public notification of changes to the system's data collection or use practices in accordance with federal requirements. Hard copy mail sent directly to affected individuals, ensuring that those who may not have regular access to digital communications are still properly notified. Online notices and disclaimers, including the addition of new notices or the updating of existing notices on the eSAF website, to ensure that users are informed of any changes at the point of system access. Other available technological means for notification and consent, providing flexibility to adapt to evolving communication technologies and methods as appropriate. It is worth noting that the specific method or combination of methods used for notification and consent will likely depend on the nature and scope of the changes made to the system, as well as the categories of individuals affected. The FDA's commitment to providing required notice and obtaining consent reflects its broader obligation to protect the privacy rights of individuals whose PII is maintained within eSAF.

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 FDA has established several processes for resolving concerns raised by individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII maintained in eSAF is inaccurate. These processes vary depending on the category of individual involved. FDA Personnel FDA employees who have concerns regarding the inappropriate obtaining, use, or disclosure of their PII, or who believe their PII is inaccurate, may raise concerns and/or submit data corrections through two primary channels. First, individuals may address their concerns through supervisory channels, escalating the matter to their supervisor or appropriate management official. Second, individuals may submit their concerns through the FDA's Employee Resource and Information Center (ERIC), which provides a dedicated resource for employees to address personnel-related matters, including concerns about the handling of their PII. Additionally, all FDA personnel are required to rapidly report any potential or suspected unauthorized access or use of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), ensuring that potential breaches or misuse of PII are promptly identified and addressed. Firm Personnel and Establishment Points of Contact Individuals who are members of an inspected establishment or firm and have concerns regarding their PII may contact the FDA through numerous communication channels, including email, phone, and standard mail, all of which are listed on FDA.gov. Additionally, there is a review process during the inspection itself that allows a firm point of contact to review the final inspection reports and identify anything that they believe to be inaccurate, providing an opportunity to address concerns about the accuracy of collected information at the time of the inspection. This multi-channel approach ensures that firm personnel have accessible and flexible means of raising and resolving concerns about their PII regardless of their preferred method of communication.
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 relevancy of PII maintained in eSAF is ensured by the nature of the information itself. All PII maintained in the system is considered relevant because point of contact information is necessary to facilitate communication with vendors and state contractors involved in the inspection process. The system only maintains PII that is directly tied to the operational needs of the inspection workflow, ensuring that no extraneous or unnecessary personal information is collected or retained. The accuracy of PII maintained in eSAF is ensured through individual review of purchase orders and work requests. Additionally, PII such as names and work contact data is provided directly by the

		vendors and contractors themselves, meaning that the individuals whose information is maintained in the system are the primary source of that information. This direct sourcing of PII from the individuals concerned helps to ensure that the information maintained in the system is accurate and up to date. Furthermore, the inspection review process allows firm points of contact to review final inspection reports and identify any inaccuracies, providing an additional layer of accuracy assurance at the point of data collection. The integrity of PII maintained in eSAF is protected through the implementation of security controls selected and implemented as part of the system's Authority to Operate (ATO) process. These 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. Specific technical safeguards implemented to protect the integrity of PII include the use of firewalls, access controls such as usernames, passwords, and MFA, and regular testing of information technology systems. Administrative safeguards such as user training, system documentation advising on proper use, and the implementation of Need to Know and Minimum Necessary principles when awarding access further support the integrity of PII in the system. The availability of PII maintained in eSAF is similarly protected through the security controls implemented as part of the ATO process, in accordance with NIST guidance and FIPS 199. Physical controls also contribute to the availability of the system and its data, as all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. These physical safeguards help to ensure that the system and its data remain available to authorized users by protecting the underlying infrastructure from physical threats that could disrupt system operations. Together, the administrative, technical, and physical controls implemented for eSAF provide a comprehensive framework for ensuring the ongoing availability of PII maintained in the system.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators 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.	Users require access to PII in eSAF for the purpose of performing and documenting FDA inspections. This includes both FDA personnel and state contractor personnel who are directly involved in the inspection workflow and must be able to access PII related to firm contacts, inspection assignments, and personnel information in order to effectively carry out their assigned inspection responsibilities and document their findings accurately. Administrators require access to PII in the course of performing analysis of historical activities and to review work in process. This access is necessary to support the operational management and oversight of the system and its associated inspection activities, ensuring that the system is functioning as intended and that inspection workflows are being carried out appropriately. Developers require access to PII in order to perform level 3 helpdesk support. This represents the highest tier of technical support and involves diagnosing and resolving complex technical issues that cannot be addressed at lower levels of helpdesk support. Access to PII at this level is limited to what is necessary to identify and resolve such technical issues within the system. Contractors, specifically HHS/OpDiv Direct Contractors, require access to PII in order to perform level 1 and level 2 helpdesk support activities. These represent the first and second tiers of technical support respectively, involving the handling of routine support requests and issues escalated from the first tier. As with all contractor access to PII, this access is governed by FAR and other appropriate clauses included in their contracts, ensuring adherence to privacy provisions and practices in the handling of any PII accessed in the course of their support duties.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The FDA has established a structured set of administrative procedures to govern and control which system users are granted access to PII maintained in eSAF. These procedures are designed to ensure that access to PII is granted only to individuals who have a legitimate need for such access in the performance of their duties, and that access is regularly reviewed and adjusted as circumstances change. System access requests are reviewed and approved by the system and business owner, along with the eSAF management team. This multi-party review process ensures that access decisions are made thoughtfully and with appropriate oversight, and that no individual is granted access to PII without the explicit approval of the relevant system and business stakeholders. Access to PII in eSAF is granted and restricted at the individual level, based on the principle of role-based access control. This means that each user's access permissions are tailored to their specific duties and responsibilities within the eSAF workflow, ensuring that individuals are only granted access to the minimum amount of PII necessary to perform their assigned functions. Supervisors indicate the minimum information system access required for each user at the time accounts are created, further reinforcing the application of the Need to Know and Minimum Necessary principles in the granting of access to PII. System accounts are reviewed on a regular basis to determine whether access is still required for each user. Specifically, the access list for the information system is reviewed on a quarterly basis, at which time users' access permissions are reviewed and adjusted as appropriate, and unneeded accounts are deactivated from the system. This regular review process helps to ensure that access to PII is promptly revoked when it is no longer needed, reducing the risk of unauthorized or unnecessary access to sensitive information.

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 FDA has implemented a series of technical methods to ensure that individuals with access to PII in eSAF are limited to accessing only the minimum amount of information necessary to perform their assigned duties. These methods work in conjunction with the administrative procedures described previously to provide a comprehensive framework for controlling access to PII at the technical level. At the time system accounts are created, supervisors indicate the minimum information system access that is required for each user to complete their job responsibilities. This ensures that access permissions are appropriately scoped from the outset, and that users are not granted broader access to PII than is necessary for the performance of their duties. This process directly supports the application of the Minimum Necessary principle in the technical configuration of user accounts within eSAF. The access list for the information system is reviewed on a quarterly basis, at which time users' access permissions are reviewed and adjusted as appropriate to ensure that they remain aligned with each user's current duties and responsibilities. Accounts that are no longer needed are deactivated from the system during these quarterly reviews, ensuring that access to PII is promptly revoked when it is no longer required. This regular review and adjustment process helps to ensure that the technical access controls in place remain current and effective over time, and that the principle of Minimum Necessary access is maintained on an ongoing basis rather than only at the time of initial account creation. The system implements role-based access controls that restrict each user's access to the specific functionality and data required for their assigned role within the eSAF workflow. This technical control ensures that users are only able to access the PII that is directly relevant to their duties, and that they are prevented from accessing PII associated with functions or workflows outside the scope of their assigned responsibilities. Together with the account creation and quarterly review processes described above, these role-based access controls provide a robust technical framework for ensuring that access to PII in eSAF is limited to the minimum amount necessary for each user to perform their job effectively.

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 system users at the FDA, including system owners, managers, operators, contractors, and program managers, are required to complete annual mandatory computer security and privacy awareness training. This training is comprehensive in scope and is designed to ensure that all individuals with access to eSAF and the PII maintained within it are fully aware of their responsibilities for protecting that information. The annual mandatory training covers the following key areas: Federal laws, policies, and regulations relating to privacy and data confidentiality, ensuring that all system users are aware of the legal framework governing the collection, maintenance, and use of PII within eSAF and other FDA systems. Data integrity and availability, providing system users with guidance on their responsibilities for maintaining the accuracy and accessibility of information maintained in the system. Data handling practices, including any special restrictions on data use and/or disclosure that apply to the information maintained in eSAF, ensuring that system users understand how to handle PII appropriately in the course of their duties. Compliance with this mandatory training requirement is verified by the FDA Office of Digital Transformation (ODT), which confirms that all individuals with access to eSAF successfully complete the required training on an annual basis. This verification process helps to ensure that the training requirement is consistently enforced across all user categories and that no individual retains access to the system without having completed the necessary security and privacy awareness training.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the annual mandatory computer security and privacy awareness training required of all FDA system users, eSAF system users receive supplemental training and guidance specifically tailored to their responsibilities within the system. This additional training is designed to ensure that system users have a thorough understanding of the specific requirements and expectations associated with their use of eSAF and the PII maintained within it. The additional training and guidance provided to eSAF system users includes the following elements: System-specific training, which provides users with detailed guidance on the proper use of eSAF and its associated functionality. This training ensures that users understand how to interact with the system in a manner that is consistent with applicable privacy and security requirements, and that they are equipped to carry out their assigned duties effectively and responsibly. Rules of Behavior, which all system users are required to review and adhere to as a condition of their access to eSAF. The Rules of Behavior establish clear expectations for the appropriate use of the system and the handling of PII maintained within it, providing a formal framework for user conduct that complements the broader guidance provided through the annual mandatory training. Additional privacy guidance, which users may obtain from the agency's privacy officials as needed. This resource ensures that system users have access to expert guidance on privacy-related matters that may arise in the course of their use of eSAF, and that they are able to seek clarification or assistance when needed to ensure that their handling of PII remains consistent with applicable requirements and best practices.

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 in eSAF are governed by a variety of records schedules specific to the nature of the records maintained within the system. The retention and destruction of PII in eSAF is carried out in accordance with National Archives and Records Administration (NARA)-approved records retention schedules, which establish clear guidelines for how long records must be maintained and when they must be deleted or destroyed. The applicable NARA records retention schedules and their associated retention periods are described below. NARA Approved Citation N1-088-09-3 eSAF database records are maintained in accordance with NARA approved citation N1-088-09-3. Under this schedule, records disposition is designated as temporary, meaning that records are not retained permanently but are instead deleted or destroyed after a specified period of time. Specifically, records governed by this citation are deleted or destroyed 10 years after the end of the fiscal year in which the subject regulatory action is final. This retention period ensures that inspection-related records are maintained for a sufficient period of time to support ongoing regulatory oversight and accountability, while also ensuring that records are not retained indefinitely beyond the point at which they are needed. NARA Approved Citation N1-088-07-2 Program management files maintained in eSAF fall under NARA approved citation N1-088-07-2. The retention and destruction periods applicable to records governed by this citation generally range from 10 to 30 years after an action closes or when a record is no longer needed. This broader retention range reflects the varying nature of program management records and the differing periods of time for which such records may be needed to support the FDA's regulatory mission and administrative functions. Together, these two NARA-approved records retention schedules provide a comprehensive framework for the retention and destruction of PII maintained in eSAF, ensuring that records are kept for as long as they are needed to support the FDA's regulatory and administrative functions, and that they are appropriately disposed of once they are no longer required.
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 FDA has implemented a comprehensive set of administrative, technical, and physical controls to ensure the security of PII maintained in eSAF. These controls are selected from National Institute of Standards and Technology (NIST's) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, as determined using Federal Information Processing Standards (FIPS) 199, and are designed to work together to provide a robust and layered security framework for the protection of PII within the

system.

Administrative safeguards implemented to protect PII in eSAF include the following measures:

User training, including the annual mandatory computer security and privacy awareness training required of all system users, as well as system-specific training and the review and adherence to the Rules of Behavior, ensures that all individuals with access to PII are aware of their responsibilities for protecting that information.

System documentation that advises on the proper use of the system provides users with clear guidance on how to interact with eSAF in a manner that is consistent with applicable privacy and security requirements.

Need to Know and Minimum Necessary principles are implemented when awarding access to the system, ensuring that individuals are only granted access to the PII that is directly relevant to their assigned duties and responsibilities. System access requests are reviewed and approved by the system and business owner along with the eSAF management team, and accounts are reviewed on a quarterly basis to ensure that access remains appropriate and that unneeded accounts are promptly deactivated.

Contractual safeguards, including FAR and other appropriate clauses in contracts with HHS/OpDiv Direct Contractors, ensure that contractor personnel who have access to PII in the course of performing helpdesk support activities adhere to applicable privacy provisions and practices.

Technical safeguards implemented to protect PII in eSAF include the following measures:

Firewalls are used to control and monitor network traffic, helping to prevent unauthorized access to the system and its data from external sources.

Access controls, including usernames, passwords, and MFA via an emailed OTP, are implemented to ensure that only authorized individuals are able to access the system and the PII maintained within it. Role-based access controls further restrict each user's access to the specific functionality and data required for their assigned role within the eSAF workflow.

Regular testing of information technology systems is conducted to identify and address potential vulnerabilities that could compromise the security of PII maintained in eSAF. This includes static code analysis completed via SonarQube.

Session management controls, including automatic session timeouts, help to prevent unauthorized

access to the system in the event that an authorized user leaves their workstation unattended.

Audit logging is maintained to track user access and activity within the system, providing a record of who has accessed PII and what actions they have taken, supporting accountability and the detection of potential unauthorized access or misuse of PII.

Physical safeguards implemented to protect PII in eSAF include the following measures:

Secure facility access controls, including guards and locked facility doors at all FDA facilities where system servers are located, help to prevent unauthorized physical access to the underlying infrastructure supporting eSAF and the PII maintained within it.

Climate controls are implemented at all FDA facilities where system servers are located, helping to ensure the ongoing availability and integrity of the system and its data by protecting the underlying infrastructure from environmental threats such as temperature fluctuations and humidity that could damage or destroy server hardware.

Together, these administrative, technical, and physical controls provide a comprehensive and layered security framework for the protection of PII maintained in eSAF, ensuring that the information is safeguarded against both internal and external threats in a manner consistent with applicable federal requirements and best practices.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/26/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/28/2026
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:**	2

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/15/2026
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 6/15/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	18

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/18/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	3

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/18/2026 1:35 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	5/28/2026	5/28/2026 Per FDA's email a copy of the PIA and email are attached.	FW_ PTA _ PIA 5270619 is ready for APA Review.pdf OII Electronic State Access to FACTS eSAF_SOP approved.pdf