PTA / PIA: FDA - OII FMS - QTR2 - 2026 - FDA5270677

Created Date: 6/2/2026 2:00 PM Last Updated: 6/4/2026 6:00 PM

General Information

PTA / PIA Name:	FDA - OII FMS - QTR2 - 2026 - FDA5270677	**PTA / PIA ID:**	4541528
Component Name:	FDA - OII Firm Management Services	**ATO Boundary Name:**	CDRH Scientific and Research General Support Systems
Overall Status:	Complete	**# of Days - Open:**	13
Submitter:		**Submit Date:**	6/2/2026
Next Assessment Date:	06/03/2029	**Expiration Date:**	6/3/2029
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.	Food and Drug Administration (FDA) has made no changes to Firm Management Services (FMS) 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.	Firm Management Services (FMS) is an internal-facing Single Sign-On (SSO) component of the broader Office of Inspections and Investigations (OII) Case and Workload Management (OCWM) system. It functions as a web service used by other OII system components and applications to search and manage data on firms regulated by the Food and Drug Administration (FDA). FMS provides reliable, comprehensive, and uniform data about the firms, establishments, and facilities regulated by FDA, serving as a centralized repository for firm-related information that is critical to OII's regulatory mission. In addition to OII staff, users from across FDA and its various centers access FMS — primarily through integrated applications such as the Field Accomplishments and Compliance Tracking System (FACTS) and the Operational and Administrative System for Import Support (OASIS) — to search and manage firm information in support of their respective regulatory activities. These integrated applications, along with any other interfacing systems, are each subject to their own separate privacy and security assessments. FMS underpins OII's core field activities, including inspections, investigations, recalls, and other compliance and enforcement operations, by ensuring that accurate and up-to-date firm information is available to authorized users across the agency, thereby directly supporting the Department of Health and Human Services' (HHS) broader public health and safety mission. FMS is an intranet web application accessible only to internal FDA users. Users are required to complete an account access form to request system access, and each user is assigned a role that determines their permissions within the system. FMS implements SSO, meaning users do not need to manually log into the system separately — they are automatically authenticated when they log on to the agency's secure network. Users then navigate to the intranet uniform resource locator (URL) to access the system. User credentials are maintained in a separate system, specifically Active Directory (AD), and are not collected or stored within FMS itself.

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.	FMS collects and manages two categories of information: personally identifiable information (PII) and non-PII. With respect to PII, FMS collects point of contact (POC) information for regulated firms, including the full name, work email address, and work telephone number and job title of the firm's point of contact, as well as the firm's business email address, physical and mailing address, and business telephone number. The system also collects the FDA Establishment Identifier (FEI) number, which is considered a form of PII or potential PII. It is worth noting that while a firm's name and physical address are not typically considered PII, they would be treated as such in instances where they can be used to identify a specific individual. In addition to PII, FMS collects non-PII related to firm operations and regulatory activities. This includes firm operational status, workload obligation, establishment and activity type, and industry type. This information is necessary for OII to manage its firm inventory and carry out its regulatory mission effectively. FMS maintains both current and historical firm data. Records fall under the National Archives and Records Administration (NARA) approved citation N-1-088-09-003, which is a Record Control Schedule (RCS). This schedule calls for the deletion of records 10 years after the final action, or when the records are no longer needed for operational, trend analysis, legal, or reference purposes, whichever is latest. There is no plan to delete historical data prior to meeting these criteria. In the event that data is migrated to another system, it would be deleted from FMS after verification of successful migration. FMS shares firm data with other OII applications, including FACTS and OASIS, to enable OII business users to perform their regulatory work. Any sharing of information is conducted within the Department of Health and Human Services (HHS) and is restricted to a need-to-know basis for authorized agency activities. FDA does not expect or plan to disclose records in FMS to any individuals or entities outside of FDA. PII in the system is not shared directly with organizations outside the system's Operating Division.
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.	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.	FMS provides a centralized application for OII to manage its firm inventory and related information, which is critical for OII to perform its regulatory mission. The system is integrated and shares firm data with other OII applications such as the Field Accomplishments and Compliance Tracking System (FACTS) and the Operational and Administrative System for Import Support (OASIS), as well as other interfacing applications, all of which are subject to separate assessments. With respect to the categories of individuals about whom information is collected, FMS collects PII and non-PII about two primary groups. The first group consists of employees and Direct Contractors, as well as members of the public who serve as points of contact (POC) for FDA-regulated firms. For these individuals, FMS collects full name, work email address, work telephone number, business email address, physical location and mailing address, business telephone number, and the FDA Establishment Identifier (FEI). This PII is collected because it is necessary to communicate with firms and their points of contact and to track and manage OII activities. It is worth noting that while a firm's name and physical address are not typically considered PII, they would be treated as such in instances where they can be used to identify a specific individual. The non-PII collected — including firm operational status, workload obligation, and establishment, activity, and industry type — is maintained because it is essential for OII to effectively manage its firm inventory and carry out its broader regulatory and compliance enforcement mission in support of the Department of Health and Human Services (HHS).
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://oii.fda.gov/fms/firmservices/welcome.do
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.	FMS is an intranet web application used internally by FDA users to search and manage firm information. This includes the ability to add and update firm information within the system. The application serves as a centralized tool for OII staff and other authorized FDA users to access reliable and up-to-date data on FDA-regulated firms, establishments, and facilities in support of OII's regulatory and compliance enforcement mission. FMS is accessible only to internal FDA users and is not available to the general public. Access to the system is not open to all FDA staff by default — users are required to complete an account access form to formally request access to FMS. Each user is assigned a role within the system, and their permissions are determined based on that assigned role, ensuring that access is granted on a need-to-know basis consistent with the user's duties. The groups that have access to the system include users, administrators, developers, and contractors, the latter referring specifically to Department of Health and Human Services (HHS) and Operating Division (OpDiv) Direct Contractors. FMS implements SSO, meaning users do not need to manually log into the system separately. Instead, they are automatically authenticated when they log on to the agency's secure network. Once authenticated, users navigate to the intranet URL — https://oii.fda.gov/fms/firmservices/welcome.do — to access the system. User credentials are maintained in Active Directory (AD), a separate system (covered in separate assessment), and are not collected or stored within FMS itself.
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 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.	FDA Establishment Identifier (FEI) number Job Title Physical Address (Business)
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Members of the public
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	500 – 4,999
PIA 25:	For what primary purpose is the PII used?	The primary purpose for which PII is used in FMS is to correspond with individuals at the firm who can respond to FDA questions and requests. In other words, the PII collected including contact information such as name, business email address, business mailing address, and business phone number is used to facilitate communication between FDA and the designated points of contact (POC) at FDA-regulated firms. This ensures that OII can effectively reach the appropriate individuals at regulated firms in support of its inspections, investigations, recalls, and other compliance and enforcement activities.
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.	FMS information collection and use is conducted in accordance with, and to satisfy the requirements of, numerous provisions of the Federal Food, Drug and Cosmetic Act (FD&C Act), 21 U.S.C. 301, as amended by the Food Safety Modernization Act (FSMA), 21 U.S.C. 220. The relevant provisions can be found in 21 U.S.C. 331 and 350-387. These legal authorities collectively establish FDA's mandate to regulate firms, establishments, and facilities, and provide the statutory basis for the collection, maintenance, and use of firm-related information — including PII — within FMS. The information collected is necessary for OII to fulfill its regulatory obligations under these provisions, which govern matters such as prohibited acts, inspections, registration of food facilities, and other compliance and enforcement activities central to OII's mission of protecting public health and safety.
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 Non-Government Sources Private Sector
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 FMS because the system does not collect any information from the general public. FMS is an internal-facing intranet web application accessible only to authorized FDA users, and its collection of firm-related information — including PII — is limited to points of contact at FDA-regulated firms who provide their information as a practical requirement in order to communicate with FDA. Since the Paperwork Reduction Act (PRA), which governs OMB information collection approvals, applies to information collections directed at the general public, FMS falls outside the scope of that requirement.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary
PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	There are no formal notification and consent procedures specific to FMS. Individuals provide their contact information as a practical requirement in order to communicate with FDA. While FDA requires that regulated entities provide the PII of a point of contact (POC), that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity. In this sense, the submission of PII is voluntary in that the regulated entity has discretion over which individual they designate as their point of contact, though the provision of a point of contact's information is itself a practical necessity for maintaining communication with FDA.

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 are no formal notification and consent procedures specific to FMS for instances when major changes occur to the system. As noted previously, individuals provide their contact information as a practical requirement in order to communicate with FDA, rather than through a formal consent process. As such, there is no established mechanism to proactively notify individuals of changes to the system's data uses or disclosure practices at the time those changes occur. However, FDA has established a general framework for addressing such situations should they arise. If FDA practices change with regard to the collection or use of PII in FMS, the agency will provide required notice and obtain consent from individuals through the most efficient and effective means available. FDA website and privacy policies are publicly accessible on FDA.gov and the FDA intranet, providing a baseline level of transparency regarding the agency's privacy practices. Additionally, the completion and public availability of Privacy Threshold Analyses (PTA) and Privacy Impact Assessments (PIA) — serves as a further mechanism for providing notice to individuals about how their information is collected, used, and disclosed within FMS.
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.	Individuals who suspect their PII has been inappropriately obtained, used, or disclosed in any FDA system have multiple avenues available for assistance. These individuals may contact FDA and OII offices, including the Privacy Office and other agency offices, via email, phone, and standard mail avenues, all of which are listed on FDA.gov and the FDA intranet. All FDA personnel are also required to rapidly report any suspected or confirmed unauthorized access or use of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), ensuring that any potential breach or misuse of PII is escalated and addressed promptly in accordance with FDA's broader privacy and security protocols.

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.	Firms voluntarily provide the PII of their designated POC, and the firm itself is responsible for ensuring that the information provided is accurate at the time of submission. Accuracy is further supported by review at the time of reporting. Firms may update their POC information as needed to reflect changes in personnel or contact details, ensuring that the PII maintained in FMS remains current and relevant to ongoing communication with the FDA. PII relevancy is supported through the design of the system, which is configured to collect only the PII elements necessary to administer the system and enable its intended use — specifically, to facilitate communication between FDA and regulated firms. Access to PII within FMS is granted and restricted at the individual level based on each user's assigned role, ensuring that only authorized personnel with a need to know can view or manage firm-related PII. Integrity and availability are protected through the privacy and security controls selected and implemented as part of the system's Authorization to Operate (ATO) process. Controls are selected in accordance with National Institute of Standards and Technology (NIST) guidance and are calibrated to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. FDA performs annual reviews to evaluate user access and ensure that access roles and permissions remain appropriate to each user's current duties.
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: Review and manage submissions, work planning. Administrators: Monitor the system, manage the workflow and system access. Developers: Access data for system development and maintenance. Contractors: Access data for system development and maintenance. “Contractors” here refers to FDA Direct Contractors.

PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users and Direct Contractors with valid network accounts who require access to the system must obtain supervisory approval and signature before access is granted. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from 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 relevant supervisor will indicate on the user account creation form the minimum access that is required in order for the user to complete his/her job. The scope of access is restricted based on role-based criteria. Network and system settings are applied to enforce access restrictions.
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 FDA take annual mandatory computer security and privacy awareness training. This training includes guidance on federal laws, policies, and regulations relating to privacy and data confidentiality, integrity and availability, as well as the handling of data (including any special restrictions on data use and/or disclosure). The FDA Office of Digital Transformation (ODT) verifies that individuals successfully complete the training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Additionally, personnel are trained on the use of the system and review the Rules of Behavior. Additional role-based training on privacy is available via FDA's privacy office.
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).	FMS records fall under National Archives and Records Administration (NARA) approved citation N-1-088-09-003 (a Record Control Schedule (RCS)) which calls for deletion of records 10 years after the final action or when no longer needed for operational, trend analysis, legal, or reference purposes, whichever is latest.
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 include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools. Physical controls include that all system servers are located at facilities protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology’s (NIST’s) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	6/2/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	6/2/2026
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:**	6/4/2026
Agency Privacy Analyst Review Comments:	Reviewer: Godisgreat Peters 6/4/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	2

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/4/2026
SAOP Review Comments:		**# of Days - SAOP Review:**	0

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/4/2026 4:20 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
No Records Found				