PTA / PIA: FDA - ER - QTR2 - 2026 - FDA5270157

Created Date: 5/15/2026 2:22 PM Last Updated: 5/29/2026 6:17 PM

General Information

PTA / PIA Name:	FDA - ER - QTR2 - 2026 - FDA5270157	**PTA / PIA ID:**	4487856
Component Name:	FDA - OII Entry Review	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	22
Submitter:		**Submit Date:**	5/15/2026
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)?	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.	FDA has made no changes to Entry Review since the last Privacy Threshold Analysis/Privacy Impact Assessment 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.	Office of Inspections and Investigations (OII) Entry Review (ER) is an internal-facing component of the OII Case and Workload Management (OCWM) system. It is designed to assess the level of risk associated with products offered for import into the United States, directly supporting the Department of Health and Human Services (HHS) and the Food and Drug Administration's (FDA) regulatory mission. Specifically, ER supports Section 801 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), which directs the FDA to refuse admission into the nation of any import product or article that appears to be in violation of the Act. The system carries out its functions by presenting FDA staff with data submitted by importers to the U.S. Customs and Border Protection (CBP) Automated Commercial Environment (ACE) system, along with risk scores and indicators generated by the Predictive Risk-Based Evaluation for Dynamic Import Compliance Tracking (PREDICT) screening system. Based on their analysis of this data, FDA staff can take a range of actions, including accepting the import (May Proceed), requesting additional information, or arranging for FDA staff to physically examine and/or sample the import product. This enables the FDA to quickly make admissibility decisions on import products, with the agency screening more than 32 million import products per year. ER also includes a sub-component called Entry Query (EQ), which provides advanced query and search capabilities for product entries, further enabling FDA staff to efficiently analyze and act on import data. Access to ER is restricted exclusively to FDA personnel. The system utilizes FDA's Single Sign-On (SSO) infrastructure for authentication, with access limited to authorized FDA employees and staff who require the system to perform their official duties related to import review and regulatory decision-making. Users access the system via an internal URL (https://ora.fda.gov/entryreview/er) using their Personal Identity Verification (PIV) card credentials managed through Active Directory (AD). The system is not accessible via a public URL, and no third-party vendors or external partners have access to Personally Identifiable Information (PII) within the system. Access to PII is limited to authorized FDA employees and HHS/OpDiv Direct Contractors who support the system in an administrative, development, or troubleshooting capacity, and whose access is governed by role-based access controls, formal supervisor approval, and applicable Federal Acquisition Regulation (FAR) clauses ensuring adherence to privacy provisions and practices. FDA users must obtain formal supervisor approval and signature before access is granted, and the agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts.

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.	OII ER collects, maintains, and shares a variety of information types to support FDA's admissibility review and regulatory decision-making processes for imported products. The system handles both non-Personally Identifiable Information (non-PII) and PII in carrying out its mission. With respect to non-PII, the system collects and maintains entry and shipment information submitted by importers to U.S. Customs and Border Protection (CBP), including entry lines, availability dates, and location information for products under review. The system also handles product and commodity data, including risk scores and indicators generated by the Predictive Risk-Based Evaluation for Dynamic Import Compliance Tracking (PREDICT) screening system, which are used to support admissibility decisions and risk-based screening. Firm and establishment information, including Firm Establishment Identifiers (FEIs), is maintained to identify responsible parties and link to compliance history. Regulatory and compliance data documenting enforcement actions, compliance history, and regulatory decisions — including records of detentions, refusals, and other compliance activities — are also collected and maintained. Additionally, workflow and audit data are retained to ensure traceability and transparency throughout the import review process. ER also exchanges integration data with interconnected systems, including the Import Trade Auxiliary Communications System (ITACS), Entry Review Web Service (ERWS), Operational and Administrative System for Import Support (OASIS), and CBP. With respect to PII, the system collects and maintains user and personnel information, specifically names and Employee ID numbers of FDA personnel who access and use the system. It is important to note that sensitive PII as defined by HHS is not collected by this system. Contact information, including names and business email addresses associated with import transactions, is also maintained to facilitate communication and authenticate FDA users. PII subjects include both internal individuals, such as HHS employees and direct/badged contractors, as well as external individuals, including members of the public and regulated entity employees. The approximate number of individuals whose PII is maintained in the system is between 500 and 4,999. ER 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, 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.	ER collects, maintains, and shares information to support the FDA mission of evaluating imported products and ensuring compliance with applicable laws, including Section 801 of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Each category of information serves a specific and necessary purpose in carrying out the agency's import review and regulatory decision-making functions. Entry and product data, including risk scores and indicators generated by the Predictive Risk-Based Evaluation for Dynamic Import Compliance Tracking (PREDICT) screening system, are collected and maintained to support admissibility decisions and risk-based screening of imported products. This information enables FDA staff to quickly evaluate whether an import product should be accepted, examined, or sampled before entry into the nation, with the FDA screening more than 32 million import products per year. This data is shared with interconnected systems, including the Operational and Administrative System for Import Support (OASIS), Entry Review Web Service (ERWS), and U.S. Customs and Border Protection (CBP), to facilitate the seamless exchange of admissibility and compliance information across agencies. Firm and establishment information, including Firm Establishment Identifiers (FEIs), is collected and maintained to identify the responsible parties associated with import transactions and to link those parties to their compliance history. This information supports the FDA's ability to make informed, risk-based decisions about imported products and to track regulatory and enforcement actions against firms that have previously been found to be in violation of applicable laws and regulations. Regulatory and compliance data, including records of detentions, refusals, and other enforcement actions, are collected and maintained to document the FDA's regulatory decisions and to support the agency's enforcement activities. This information is shared with CBP via an Interconnection Security Agreement (ISA) to facilitate coordinated admissibility determinations and enforcement actions at the border. Workflow and audit data are collected and maintained to ensure traceability and transparency throughout the import review process, providing a complete record of the actions taken by FDA staff in reviewing and adjudicating

		import entries. With respect to Personally Identifiable Information (PII), the system collects and maintains different categories of information depending on the category of individual involved. For internal individuals, specifically HHS employees and direct/badged contractors who are FDA users of the system, the system collects and maintains names and Employee ID numbers. This information is collected to authenticate FDA users, support access control and accountability, and maintain audit logs of system activity. For external individuals, including members of the public and regulated entity employees associated with import transactions, the system collects and maintains names and contact information, such as business email addresses. This information is collected to identify individuals associated with import transactions and to facilitate communication between the FDA and regulated entities regarding admissibility decisions and compliance matters. In both cases, the submission of PII is voluntary, and the FDA makes no secondary use of the PII collected by the system.
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://ora.fda.gov/entryreview/er
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.	ER is an internal FDA application designed to support the agency's admissibility review and regulatory decision-making processes for imported products. The system enables FDA staff to evaluate imported products for compliance with applicable laws, conduct risk-based screening and admissibility decisions, track regulatory and compliance history, document enforcement actions, and ensure traceability and transparency in the import review process. Specifically, ER supports Section 801 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), which directs the FDA to refuse admission into the nation of any import product or article that appears to be in violation of the Act. Access to ER is restricted exclusively to FDA personnel. The system is not a public-facing application, and no members of the general public, third-party vendors, or external partners have access to the system or the PII it contains. Access is limited to authorized FDA employees and HHS/OpDiv Direct Contractors who support the system in an administrative, development, or troubleshooting capacity, and whose access is governed by role-based access controls, formal supervisor approval, and applicable Federal Acquisition Regulation (FAR) clauses ensuring adherence to privacy provisions and practices. FDA users must obtain formal supervisor approval and signature before access is granted, and 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. Access is further restricted based on role-based criteria, with supervisors indicating on user account creation forms the minimum access required for users to complete their jobs. Users access the system via an internal Uniform Resource Locator (URL) at https://ora.fda.gov/entryreview/er, which is accessible only within the FDA's internal network and is not reachable via a public URL. The system utilizes FDA's Single Sign-On (SSO) infrastructure for authentication, with users authenticating via their Personal Identity Verification (PIV) card credentials managed through Active Directory (AD). This ensures that only authorized FDA personnel can access the sensitive entry, product, firm, and compliance information contained within the system. The system also has a posted privacy notice and uses session cookies that do not collect PII as part of its web measurement and customization technology.
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.	Identifying Numbers Employee ID Number Biographical Information Name Contact Information Email 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 PII collected and maintained by the Entry Review (ER) system is used primarily to support the processing and admissibility determination of Food and Drug Administration (FDA)-regulated imports. More specifically, PII is used to identify individuals associated with import transactions, facilitate communication between the FDA and regulated entities regarding admissibility decisions and compliance matters, authenticate FDA users and ensure that only authorized personnel have access to the system, maintain audit logs that provide traceability and transparency in the import review process, and support risk-based screening and compliance activities related to the evaluation of imported products. Access to PII within the system is governed by role-based access controls, with supervisors indicating on user account creation forms the minimum access required for users to complete their jobs. The agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts, ensuring that PII is accessible only to those with a legitimate need to know. The FDA makes no secondary use of the PII collected by the system, and the submission of PII by individuals is voluntary. All FDA personnel who have access to PII in the system complete mandatory security and privacy awareness training at a minimum of once a year, and users receive system-specific training and review and adhere to the Rules of Behavior to ensure the proper handling and protection of PII.

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 primary legal authority governing information use and disclosure in ER is 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. Relevant provisions of the FD&C Act can be found at 21 U.S.C. 331 and 350-387, which establish the FDA's authority to regulate imported products and refuse admission of any import product or article that appears to be in violation of the Act. Additionally, the agency collects and shares information pursuant to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act), 42 U.S.C. 201, which provides authority for the FDA's food defense and import screening activities. Information sharing with U.S. Customs and Border Protection (CBP) is governed by an Interconnection Security Agreement (ISA) currently in place between the FDA and CBP, in accordance with the requirements of Office of Management and Budget (OMB) Circular A-130, which requires written management authorization prior to connecting with other systems and/or sharing sensitive data and information.
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 Members of the Public 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 the ER system because ER does not collect any information directly from the public. The system is an internal FDA application restricted exclusively to FDA personnel, and it is not accessible via a public URL. Rather than collecting information from members of the public, ER presents FDA staff with data submitted by importers to the U.S. CBP ACE system, along with risk scores and indicators generated by the PREDICT screening system. FDA staff then use this information to make admissibility decisions on imported products. Because the system does not independently solicit or collect information directly from the public, it does not trigger the Paperwork Reduction Act (PRA) requirement for an OMB information collection approval number. Any PII maintained in the system pertaining to external individuals is collected incidentally as part of the import transaction process rather than through a direct public-facing information collection effort conducted by the FDA. Information collected under OMB approval is not submitted directly to ER. However, ER employ FDA Form 3540 under OMB approval No. 0910-0520, expiring 09/30/2026.
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.	Other Federal Agency/Agencies
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	ER shares PII with the CBP ACE system. Specifically, imports information contained on Food and Drug Administration Form 3540 (FDA Form 3540) gathered by ER may be shared with CBP ACE. The purpose of this disclosure is to facilitate coordinated admissibility determinations and enforcement actions at the border, supporting the FDA's mission of evaluating imported products and ensuring compliance with applicable laws, including Section 801 of the Federal Food, Drug, and Cosmetic Act (FD&C Act). This sharing enables the FDA and CBP to work together in making timely and informed decisions about the admissibility of imported products into the United States. This information sharing arrangement is governed by an Interconnection Security Agreement (ISA) currently in place between the FDA and CBP, in accordance with the requirements of OMB Circular A-130, which requires written management authorization prior to connecting with other systems and/or sharing sensitive data and information. No other external organizations or systems are identified in the provided documents as recipients of PII from the ER system.

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)).	An Interconnection Security Agreement (ISA) between the Food and Drug Administration (FDA) and U.S. Customs and Border Protection (CBP) is currently in place to govern the sharing of imports information between the two agencies. This agreement authorizes the disclosure of imports information contained on FDA Form 3540 gathered by ER to the CBP Automated Commercial Environment (ACE) system, for the purpose of facilitating coordinated admissibility determinations and enforcement actions at the border. This ISA is consistent with the requirements of Office of Management and Budget (OMB) Circular A-130, which mandates that written management authorization be obtained prior to connecting with other systems and/or sharing sensitive data and information, and which requires that such written authorization detail the rules of behavior and controls that must be maintained by the interconnecting systems. No other agreements authorizing information sharing or disclosure, such as a Computer Matching Agreement (CMA) or Memorandum of Understanding (MOU), are identified in the provided documents as being in place for the ER system.
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 ER system is not a Privacy Act system of records subject to the disclosure accounting requirement of the Privacy Act of 1974. As such, a formal disclosure accounting process specific to ER is not required. The FDA Privacy Office makes available to agency programs guidance on how to create and maintain an accounting of disclosures in accordance with the Privacy Act of 1974. With respect to general logging and tracking of system activity, the ER system maintains audit logs that provide traceability and transparency throughout the import review process. These audit logs contain detailed information about user activity and access information, ensuring that any sharing or disclosure of information within the system can be traced back to the responsible user. Access to PII within the system is further governed by role-based access controls, with the agency reviewing the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts, providing an additional layer of accountability for the handling and disclosure of PII within the system. All system activity is subject to network monitoring and intrusion detection tools, which provide an additional mechanism for tracking and accounting for the sharing and disclosure of information within and from the system.
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 submission of PII by individuals in connection with the ER system is voluntary. Individuals provide their contact information as a practical requirement to communicate with the FDA and, where appropriate, to have system access. There are no opt-out procedures specific to the Imports program. While the FDA requires that regulated entities supply the PII of a point of contact, that person can be anyone who is authorized to send and receive communications on behalf of the regulated entity, providing a degree of flexibility in how regulated entities comply with this requirement. The ER system has a posted privacy notice accessible to users of the system, which serves as the primary mechanism for notifying individuals about the collection and use of their PII. This privacy notice is consistent with the requirements of the E-Government Act of 2002, the Privacy Act of 1974, and applicable OMB guidance governing the collection and use of PII by federal agencies. If the FDA changes its practices about the collection or handling of PII related to the Imports system, the agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and use of their PII. This may include email communications to individuals, adding or updating online notices or forms, revising the PIA or other available means to inform the individual of any material changes to the system's privacy practices.

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.	At the time of the submission of the current PIA, no major changes to the ER system are anticipated. The FDA has made no changes to ER since the last PTA/PIA was approved, and therefore no immediate need to notify individuals of changes to the system's privacy practices has been identified. However, in the event that the FDA does change its practices about the collection or handling of PII related to the Imports system, the agency has established a process to provide any required notice and obtain consent from individuals regarding the collection and use of their PII. This process may include sending email communications directly to affected individuals, adding or updating online notices or forms to reflect the changes, revising the PIA or other relevant privacy documentation to accurately describe the updated practices, or employing other available means to inform individuals of any material changes to the system's privacy practices. It is important to note that the submission of PII by individuals in connection with the ER system is voluntary, and the system is restricted exclusively to internal FDA personnel and regulated entities who provide contact information as a practical requirement to communicate with the FDA. As such, the FDA has established mechanisms to reach affected individuals through existing communication channels, including email and online notices, in the event that major changes to the system's privacy practices require individual notification and consent.

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 several avenues available to resolve the situation. For FDA personnel specifically, two primary internal resources are available. The first is the FDA's Employee Resource and Information Center (ERIC), which provides FDA employees with a point of contact for addressing concerns related to the handling of their PII. The second is the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), which is available exclusively to FDA personnel and provides a mechanism for reporting and resolving concerns related to the inappropriate handling or disclosure of PII within FDA systems. For all individuals, regardless of whether they are internal FDA personnel or external members of the public or regulated entities, the FDA Privacy Office is available as a resource for resolving concerns related to the inappropriate obtaining, use, or disclosure of PII. The FDA Privacy Office can be contacted via email, phone, and standard mail, with all relevant contact information listed on fda.gov. This ensures that all individuals whose PII is maintained in the ER system have access to a clear and accessible process for raising and resolving concerns about the handling of their PII, regardless of their affiliation with the FDA. The individual is responsible for providing accurate information, and accuracy is ensured by individual review at the time of reporting. FDA personnel may correct and update their own PII as needed, ensuring that the information maintained in the system remains relevant and accurate relative to the individual's current duties and access requirements. Access is granted and restricted at the individual level as appropriate to the individual's duties through role-based access controls, further ensuring that PII is maintained accurately and in accordance with the principle of minimum necessary access.
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 individual is responsible for providing accurate information at the time of reporting. FDA personnel may correct and update their own PII as needed, ensuring that the information maintained in the system remains accurate and reflective of the individual's current role and responsibilities. This approach places the primary responsibility for accuracy on the individual, who is best positioned to identify and correct any inaccuracies in their own PII. Additionally, the agency reviews the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts, ensuring that PII is maintained only for individuals with a current and legitimate need for system access. OII also performs separate annual reviews to evaluate user access at a program level, providing an additional layer of oversight to identify and correct any inaccuracies in the PII maintained in the system and to ensure that access remains appropriate to each user's

official duties.

Access to the ER system is granted and restricted at the individual level as appropriate to the individual's duties through role-based access controls. FDA users' supervisors indicate on user account creation forms the minimum access required for users to complete their jobs, ensuring that PII is collected and maintained only to the extent necessary to support the individual's official duties. 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, ensuring that PII is maintained only for individuals who have a current and legitimate need for access to the system. OII also performs separate annual reviews to evaluate user access at a program level, providing an additional layer of oversight to ensure that PII maintained in the system remains relevant to the agency's mission and operational needs. These two review processes are complementary and distinct: the quarterly reviews focus on account maintenance and access role adjustments, while the annual OII reviews provide broader program-level oversight to ensure that access to PII maintained in the system remains relevant and appropriate to the agency's mission and operational needs.

Integrity of PII and other information maintained in the ER system is protected by security and privacy controls selected and implemented as part of the system's Authorization to Operate (ATO) process. Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. These controls include technical safeguards such as multi-factor authentication, firewalls, and network monitoring and intrusion detection tools, as well as administrative safeguards such as user training and implementation of Need to Know and Minimum Necessary principles when awarding access. Together, these controls ensure that PII maintained in the system is protected from unauthorized modification, corruption, or destruction.

Availability of PII and other information maintained in the ER system is similarly protected by the security and privacy controls implemented as part of the system's ATO process. The OCWM system, of which ER is a component, has been categorized as a high impact information system in accordance with NIST FIPS 199, meaning that the loss of availability of the system would have a severe or catastrophic effect on the agency's mission and operations. As such, the system is subject to a comprehensive set of security controls designed to ensure the continued availability of PII and other information maintained in the system, including controls related to contingency planning,

		backup and recovery, and system maintenance. All FDA personnel who have access to PII in the system complete mandatory security and privacy awareness training at a minimum of once a year, ensuring that system users are aware of their responsibilities for protecting the 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: FDA users require access to PII in the ER system in order to review, process, and manage data submissions related to the admissibility review and regulatory decision-making processes for imported products. This includes access to names and contact information associated with import transactions, which is necessary to identify individuals associated with those transactions, facilitate communication between the FDA and regulated entities regarding admissibility decisions and compliance matters, and support risk-based screening and compliance activities related to the evaluation of imported products. Access to user and personnel information, including Employee ID numbers, is also necessary to support access control and accountability within the system. Administrators: System administrators require access to PII in the ER system in order to review, process, and administer the system, its files and data, and access control. This includes access to user and personnel information necessary to manage user accounts, assign and adjust role-based access controls, and ensure that PII is accessible only to those with a current and legitimate need for access. Administrators are responsible for reviewing the system access list on a quarterly basis to adjust users' access roles and permissions and delete unneeded accounts from the system, a function that requires access to the PII associated with user accounts maintained in the system. Developers: System developers require access to PII in the ER system in order to troubleshoot issues with the system, its performance, and access. This includes access to user and personnel information necessary to identify and resolve technical issues that may affect the availability, integrity, or security of PII maintained in the system. Developer access to PII is governed by role-based access controls and the principle of minimum necessary access, ensuring that developers have access only to the PII necessary to perform their official duties

		related to the development and maintenance of the system. Contractors: HHS and OpDiv Direct Contractors require access to PII in the ER system in order to support the IT team for administration, troubleshooting, and development of the system. This includes both Direct Contractors as well as FDA employees who may serve in the capacity of users, administrators, and developers regarding the Imports system. Contractor access to PII is governed by role-based access controls and the principle of minimum necessary access, and all contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. All contractors who have access to PII in the system complete mandatory security and privacy awareness training at a minimum of once a year, and users receive system-specific training and review and adhere to the Rules of Behavior to ensure the proper handling and protection of PII.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA users (employees and Direct Contractors) with valid network accounts who require access to ER must obtain formal supervisor approval and signature before access is granted. This ensures that access to PII within the system is granted only to individuals who have a demonstrated and legitimate need for access in order to perform their official duties related to import review and regulatory decision-making. The requirement for formal supervisor approval and signature provides a documented record of the authorization for each individual's access to PII within the system, supporting accountability and traceability in the access control process. The scope of access granted to each user is restricted based on role-based criteria, with supervisors indicating on user account creation forms the minimum access required for users to complete their jobs. This ensures that the principle of minimum necessary access is applied consistently across all categories of system users, including administrators, developers, and contractors, limiting each user's access to PII to only that which is necessary to perform their official duties. The system's role-based access controls are consistent with the Need to Know and Minimum Necessary principles established by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, and implemented as part of the system's Authorization to Operate (ATO) process. 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, ensuring that access to PII remains current and appropriate to each user's official duties. In addition to these quarterly reviews, OII

performs separate annual reviews to evaluate user access at a program level. These two review processes are complementary and distinct: the quarterly reviews focus on account maintenance and access role adjustments, while the annual OII reviews provide broader program-level oversight to ensure that access to PII maintained in the system remains relevant and appropriate to the agency's mission and operational needs.

All contracts include FAR and other appropriate clauses ensuring adherence to privacy provisions and practices, providing an additional layer of oversight and accountability for contractors who have access to PII in the system. All FDA personnel, including contractors, who have access to PII in the system complete mandatory security and privacy awareness training at a minimum of once a year, and users receive system-specific training and review and adhere to the Rules of Behavior to ensure the proper handling and protection of PII. These administrative procedures collectively ensure that access to PII within the ER system is granted, maintained, and revoked in a controlled and accountable manner, consistent with applicable federal laws, regulations, and guidance governing the protection of PII in federal information systems.

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.	FDA users' supervisor will indicate on user account creation forms the minimum access that is required in order for users to complete their jobs. The scope of access is restricted based on role-based criteria. 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 ER. 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. 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 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 ER, 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, including system owners, managers, operators, contractors, and program managers who use the ER system, are required to complete mandatory security and privacy awareness training at a minimum of once a year. This annual training requirement applies to all categories of system users regardless of their role or affiliation, ensuring that all individuals with access to the sensitive entry, product, firm, and compliance information, including PII, maintained in the system are aware of their responsibilities for protecting that information. The Office of Digital Transformation (ODT) is responsible for tracking completion of the annual security and privacy awareness training course, providing a centralized mechanism for ensuring and documenting compliance with this mandatory training requirement across all categories of system users.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	In addition to the mandatory annual security and privacy awareness training tracked by ODT, users of the ER system receive system-specific training designed to provide them with a more detailed understanding of their responsibilities for protecting the specific types of information collected and maintained by the ER system. This system-specific training supplements the general security and privacy awareness training with practical guidance tailored to the unique characteristics and requirements of the system, ensuring that users are equipped with the knowledge and skills necessary to fulfill their responsibilities for protecting the sensitive entry, product, firm, and compliance information, including PII, maintained in the system. All ER system users are also required to review and adhere to the Rules of Behavior, which establish the specific expectations and responsibilities for the appropriate use and handling of information within the system. The Rules of Behavior provide users with clear and actionable guidance on their obligations for protecting the information maintained in the system, supplementing the general security and privacy awareness training with system-specific behavioral standards and expectations. Users may also obtain additional privacy guidance from the agency's privacy officials as needed, providing an additional resource for addressing specific privacy-related questions or concerns that may arise in the course of their official duties related to import review and regulatory decision-making.

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 ER are governed by a variety of records schedules specific to the nature of the records. The retention and destruction periods generally range from 10 to 30 years after an action closes or when a record is no longer needed. ER database records are maintained in accordance with National Archives and Records Administration (NARA) approved citation N1-088-09-3 which states that records disposition is temporary, with records 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.
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.	Several administrative safeguards are in place to protect PII maintained in the ER system. All FDA personnel, including system owners, managers, operators, contractors, and program managers who use the ER system, are required to complete mandatory security and privacy awareness training at a minimum of once a year, with completion tracked by the Office of Digital Transformation (ODT). In addition to this general training, users receive system-specific training, review and adhere to the Rules of Behavior, and may obtain additional privacy guidance from the agency's privacy officials. System documentation advises users on the proper use of the system and the appropriate handling of PII. The Need to Know and Minimum Necessary principles are applied consistently when awarding access to the system, with supervisors indicating on user account creation forms the minimum access required for users to complete their jobs. FDA users with valid network accounts who require access to ER must obtain formal supervisor approval and signature before access is granted, and 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. In addition to these quarterly reviews, OII performs separate annual reviews to evaluate user access at a program level, providing broader program-level oversight to ensure that access to PII maintained in the system remains relevant and appropriate to the agency's mission and operational needs. These two review processes are complementary and distinct: the quarterly reviews focus on account maintenance and access role adjustments, while the annual OII reviews provide broader program-level oversight to ensure that access to PII maintained in the system remains relevant and appropriate to the agency's mission and operational needs. All contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices, providing an additional layer of oversight and accountability for contractors who have access to PII in the system. Several technical safeguards are in place to protect PII maintained in the ER system. The system utilizes the FDA's Single Sign-On (SSO)

infrastructure for authentication, with users authenticating via their Personal Identity Verification (PIV) card credentials managed through Active Directory, ensuring that only authorized FDA personnel can access the sensitive information contained within the system. Multi-factor authentication is implemented to provide an additional layer of security for user access to the system. Firewalls and network monitoring and intrusion detection tools are in place to control and monitor network traffic and detect and respond to potential security incidents involving PII. The system's role-based access controls ensure that each user's access to PII is limited to only that which is necessary to perform their official duties, consistent with the principle of minimum necessary access. The ER system maintains audit logs that provide traceability and transparency throughout the import review process, containing detailed information about user activity and access information that can be used to detect and investigate potential unauthorized access to or disclosure of PII. Additional technical controls have been selected and implemented from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, as determined using Federal Information Processing Standards (FIPS) 199, appropriate to the system's categorization as a high impact information system. The system's login audit trail records the Local Area Network (LAN) ID, workstation ID, login date, login time, user ID, logout date, and logout time of all logons to the system, and automatic disconnect occurs after three failed attempts to log into the system. Application timeout controls are also in place, automatically logging out users after a predefined period of inactivity to prevent unauthorized access to PII through unattended workstations.

All system servers supporting the ER system are located at facilities protected by a comprehensive set of physical security controls designed to prevent unauthorized physical access to the hardware and infrastructure supporting the system. These physical controls include security guards, locked facility doors, and climate controls to protect the physical infrastructure of the system from unauthorized access, theft, and environmental hazards. The majority of the system's production and pre-production server infrastructure is located at the Ashburn Data Center (ADC), with some components hosted in Amazon Web Services (AWS) GovCloud, both of which maintain robust physical security controls appropriate to the sensitivity of the information processed and maintained by the system. Together, these physical controls ensure that the hardware and infrastructure supporting the ER system, and the PII maintained therein, are protected from unauthorized physical access, theft, and environmental damage, consistent with applicable federal laws, regulations, and guidance governing the physical protection of federal information systems and the PII they maintain.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/15/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/15/2026
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: Shanai Shobowale 5/21/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	6

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 3:01 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	5/18/2026	5/18/2026 Per FDA Email, Attached a copy of the PIA.	OII Entry Review SOP approved.pdf