PTA / PIA: FDA - eNSpect - QTR2 - 2026 - FDA5270356

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

General Information

PTA / PIA Name:	FDA - eNSpect - QTR2 - 2026 - FDA5270356	**PTA / PIA ID:**	4500099
Component Name:	FDA - OII Electronic Inspection	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	16
Submitter:		**Submit Date:**	5/19/2026
Next Assessment Date:	05/28/2029	**Expiration Date:**	5/28/2029
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.	3/4/2025
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 eNSpect 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.	In support of FDA Office of Inspections and Investigations (OII) inspection activities, the Electronic Inspection system (eNSpect) allows FDA Consumer Safety Officers (CSOs) and FDA Consumer Safety Investigators (CSIs) to work completely offline — without a connection to the FDA network — on FDA-issued Windows laptops and tablets while performing inspections at establishments regulated by the FDA. eNSpect is a locally installed application deployed on FDA-issued Windows laptops and tablets. While it is not a traditional mobile application available for public download, it incorporates mobile device management and data synchronization infrastructure — including Systems, Applications, and Products in Data Processing (SAP) Afaria 7.0 for mobile device management, SAP Mobilink for data synchronization, SAP Relay Server for secure communication, and SAP Structured Query Language (SQL) Anywhere as a local database — to support its offline capabilities in the field. eNSpect is one component of the overall OII Case and Workload Management (OCWM) system, formerly known as the Systems for Inspections, Recall, Compliance and Enforcement (SIRCE). FDA has assessed the other OCWM components in separate Privacy Impact Assessments (PIAs). The purpose of eNSpect is to support FDA investigators in performing inspections onsite at the physical locations of FDA-regulated establishments, commonly referred to as firms, and to provide records used by FDA employees in investigations of possible violations of laws enforced by the agency. The eNSpect system is comprised of both an online and an offline application for FDA investigators to use in documenting their inspections. The offline application allows investigators to record inspection observations and findings, generate legally required documentation, and utilize digital signatures via their FDA Personal Identity Verification (PIV) card, all without network access. This offline capability is essential because inspections are conducted at physical firm locations where network connectivity may not be available or appropriate. The system supports the full lifecycle of inspection documentation, including the generation of the FDA Establishment Inspection Report (EIR), documented in FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations). The FDA Form 483 is issued to firms at the conclusion of an inspection when an investigator has observed conditions that in their judgment may constitute violations of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and related Acts.

eNSpect also includes a team inspections feature that allows more than one investigator to share and contribute their work during an inspection, eliminating bottlenecks and the need to manually consolidate inputs from multiple team members. The types of inspections supported include domestic and foreign inspections in support of compliance, consumer complaints, recalls, and product safety surveillance, covering firms responsible for the manufacturing and processing of foods, feeds, drugs, medical devices, and in-vitro diagnostic devices.

After completing their inspection in the field, CSOs and CSIs connect to the eNSpect online application through the FDA network to manage, finalize, and submit their inspection reports and associated documentation. Upon returning from the field, investigators synchronize their offline inspection data with the eNSpect online application through FDA's Single Sign-On (SSO) authentication process using Multi-Factor Authentication (MFA). The production URL for the eNSpect portal is https://OII.fda.gov/enspect/portal, which is internal-facing and accessible only to FDA personnel. eNSpect does not require, use, collect, or maintain system-specific logon credentials such as a separate username and password, as authentication is handled entirely through the FDA enterprise SSO process.

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.	eNSpect collects, maintains, and shares several categories of information in support of FDA inspection activities. The system captures data about the FDA-regulated establishment being inspected, including the firm's name, address, and type, as well as the FDA Establishment Identifier (FEI) number and the date of the inspection. These latter two elements are considered potential Personally Identifiable Information (PII). Additionally, eNSpect collects PII about the firm's Point-of-Contact (POC), including the POC's name(s), job title within the firm, work phone number, work email address, and work fax number. This information is work-related in nature and is provided voluntarily either by the individual POC or by their employing firm, either in person at the time of inspection or during initial and/or follow-up contact with the firm. The system also maintains PII about the FDA investigators themselves as part of the official inspection records and legal documentation. This includes each investigator's first and last name, work phone number, work email address, and work fax number. This investigator information is not directly entered by the investigator but is instead obtained from other internal FDA systems, specifically FDA's Active Directory, the Enterprise Administrative Support Environment (EASE), and the OII Operations Database. The subject of separate Privacy Impact Assessments (PIAs). Beyond structured data fields, eNSpect captures investigator observations and findings through free text fields. This narrative information supports and describes the investigator's inspection activities and may include any type of information the investigator deems necessary to document their findings, and therefore may contain PII beyond what is otherwise specifically collected by the system. Specifically, this includes FDA Form 483 citation observations, a summary of inspection findings, inspection endorsement, and the Establishment Inspection Report (EIR) narrative report. All data maintained in eNSpect is shared internally within FDA for inspections, product recalls, compliance, and enforcement purposes. No PII contained in the system is shared outside of the Department of Health and Human Services (HHS) with any individuals or entities external to the agency. eNSpect records are maintained under the National Archives and Records Administration (NARA) Citation N1-088-09-1, FDA file code 7300 series, for Establishment Inspections and Compliance Action Files. Records are destroyed 10 years after an inspection is classified as "no action indicated" or "voluntary action indicated," and 30 years after the close of a case where official action was indicated.

PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	FDA's Active Directory FDA Enterprise Oracle Internet Directory (OID) SAP Afaria 7.0
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.	Establishment information is collected and maintained in eNSpect to accurately identify and document the FDA-regulated firm being inspected. The firm's name, address, type, FEI number, and inspection date are necessary to create an official and legally defensible inspection record that can be used for compliance, enforcement, and analysis activities. This information ensures that inspection records are properly attributed to the correct establishment and can be retrieved and referenced in future regulatory actions, product recalls, or enforcement proceedings. PII about the firm's POC — including the POC's name(s), job title within the firm, work phone number, work email address, and work fax number — is collected and maintained for business contact purposes and to facilitate efficient communication between FDA investigators and the regulated establishment. This information is necessary to allow FDA personnel to follow up with the appropriate individual at the firm regarding inspection findings, corrective actions, or other regulatory matters. The POC's PII is provided voluntarily either by the individual POC themselves or by their employing firm and consists exclusively of work-related details. It is important to note that all PII collected about firm POCs is used to retrieve records only on rare occasions and solely for the purpose of efficient communication, such as when a firm POC contacts an inspector for follow-up directly. PII about FDA investigators — including first name, last name, work phone number, work email address, and work fax number — is collected and maintained as part of the official inspection records and legal documentation generated during the inspection process. This information is required because eNSpect produces legally significant documents, including FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations), which must identify the FDA investigator(s) responsible for conducting the inspection. Investigator PII is obtained from internal FDA systems, specifically FDA's Active Directory, the Enterprise Administrative Support Environment (EASE), and the OII Operations Database, rather than being entered manually by the investigator. Narrative information entered by investigators into eNSpect's free text fields — including FDA Form

		483 citation observations, summary of inspection findings, inspection endorsement, and the Establishment Inspection Report (EIR) narrative — is collected and maintained to create a comprehensive and accurate record of the inspection. This documentation serves as the official account of the investigator's findings and observations at the firm and is used by FDA in support of inspections, product recalls, compliance determinations, and enforcement actions. The free text nature of these fields allows investigators the flexibility to fully describe any conditions or violations observed during the inspection, which may include any type of information necessary to support their findings. All of the information described above is shared internally within FDA across relevant offices and programs for the purposes of inspections, product recalls, compliance, and enforcement. The sharing of this information supports FDA's broader regulatory mission by ensuring that inspection data is accessible to the appropriate FDA personnel who need it to make informed regulatory decisions. No PII maintained in eNSpect is shared outside of HHS with any individuals or entities external to the agency, ensuring that the privacy of both firm POCs and FDA investigators is appropriately protected.
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/enspect/portal
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.	eNSpect does not include a website or online application that is accessible to the general public. However, eNSpect does have an internal online application component that FDA investigators access after returning from their field inspections. The purpose of this online application is to allow FDA Consumer Safety Officers (CSOs) and Consumer Safety Investigators (CSIs) to connect to the eNSpect system through the FDA network to manage, finalize, and submit their inspection reports and associated documentation after completing their work in the field. This online component complements the offline, locally installed application that investigators use during the inspection itself. Access to the eNSpect online application is strictly limited to internal FDA personnel, specifically investigators and their supervisors involved in the inspection process. The production URL for the eNSpect portal is https://OII.fda.gov/enspect/portal, and the pre-production URL is https://OII.preprod.fda.gov/enspect/portal. These URLs are internal-facing and are not accessible to the general public. Users access the system through FDA's SSO authentication process, which incorporates Multi-Factor Authentication (MFA) using the investigator's FDA Personal Identity Verification (PIV) card. Importantly, eNSpect does not require, use, collect, or maintain system-specific logon credentials such as a separate username and password, as authentication is handled entirely through the FDA enterprise/Active Directory SSO process.
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?	Yes
PTA 14A:	Is the mobile application HHS developed and managed or a third-party application?	HHS
PTA 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	The purpose of eNSpect's mobile/offline application component is to allow FDA Consumer Safety Officers (CSOs) and Consumer Safety Investigators (CSIs) to conduct and document inspections at FDA-regulated establishments completely offline, without requiring a connection to the FDA network. This capability is essential because inspections are conducted at physical firm locations where network connectivity may not be

available or appropriate. The offline application allows investigators to record inspection observations and findings, generate legally required documentation including FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations), and utilize digital signatures via their FDA Personal Identity Verification (PIV) card, all without network access. The offline application also supports a team inspections feature that allows more than one investigator to share and contribute their work during an inspection, eliminating bottlenecks and the need to manually consolidate inputs from multiple team members.

The types of inspections supported by the eNSpect mobile/offline application include domestic and foreign inspections in support of compliance, consumer complaints, recalls, and product safety surveillance, covering firms responsible for the manufacturing and processing of foods, feeds, drugs, medical devices, and in-vitro diagnostic devices. The mobile/offline application supports the full lifecycle of inspection documentation, from the initial recording of inspection observations and findings in the field to the synchronization of completed inspection records with the eNSpect online application upon the investigator's return to the FDA network.

The eNSpect mobile/offline application is not a traditional mobile application available for download from a public application store. Rather, it is a locally installed application deployed on FDA-issued Windows laptops and tablets. While eNSpect is an agency-developed and managed application developed and maintained by the Food and Drug Administration (FDA), an Operating Division (OpDiv) of the Department of Health and Human Services (HHS), it incorporates the following third-party technologies developed and maintained by Systems, Applications, and Products in Data Processing (SAP), a third-party vendor, to support its offline and mobile device management capabilities on FDA-issued Windows laptops and tablets:

SAP Afaria 7.0 — A third-party mobile device management platform used to manage and secure FDA-issued Windows laptops and tablets on which the eNSpect offline application is deployed.

SAP Mobilink — A third-party data synchronization technology used to synchronize offline inspection data collected during field inspections with the eNSpect online application upon the investigator's return to the FDA network.

SAP Relay Server — A third-party secure communication technology used to provide encrypted communication channels between the eNSpect offline application on FDA-issued mobile devices and the eNSpect backend database servers

located at the Ashburn Data Center (ADC).

SAP Structured Query Language (SQL) Anywhere — A third-party local database technology used to store inspection data, including Personally Identifiable Information (PII), collected during field inspections on FDA-issued Windows laptops and tablets while operating in offline mode.
While these third-party SAP technologies are integral to the eNSpect mobile/offline application's offline and mobile device management capabilities, the eNSpect application itself is developed, owned, and managed by FDA. All third-party technologies are deployed and managed within FDA's enterprise information technology infrastructure and are subject to FDA's information security and privacy policies and procedures, including the applicable security controls selected and implemented in the course of providing the system with an Authority to Operate (ATO).

Access to the eNSpect mobile/offline application is strictly limited to internal FDA personnel, specifically FDA Consumer Safety Officers (CSOs), Consumer Safety Investigators (CSIs), and their supervisors who are involved in the inspection process. The application is deployed exclusively on FDA-issued Windows laptops and tablets and is not accessible to the general public or to individuals outside of FDA. System access requests for eNSpect are reviewed and approved by the system and business owner along with the eNSpect management team, and access is granted and restricted at the individual level as appropriate to the individual's duties, using a role-based access control model that ensures each user is granted only the minimum level of access necessary to perform their specific job responsibilities. The access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted as appropriate, with unneeded accounts purged from the system to ensure that only authorized personnel retain access to the application and the PII it contains.

Users access the eNSpect mobile/offline application on FDA-issued Windows laptops and tablets through FDA's enterprise SSO authentication process, which incorporates Multi-Factor Authentication (MFA) using the investigator's FDA Personal Identity Verification (PIV) card. This ensures that only authenticated and authorized FDA personnel can access the application and the PII it contains. The eNSpect mobile/offline application does not require, use, collect, or maintain system-specific logon credentials such as a separate username and password, as authentication is handled entirely through the FDA Enterprise Active Directory and Oracle Internet Directory (OID) via the FDA enterprise SSO process, consistent with Federal Information Processing Standard (FIPS) Publication 201-2, Personal Identity Verification (PIV) of

		Federal Employees and Contractors. Upon completing their inspection in the field, investigators connect to the FDA network to synchronize their offline inspection data with the eNSpect online application, accessible at the internal production URL https://OII.fda.gov/enspect/portal, through the same FDA enterprise SSO authentication process. Data synchronization between the offline application and the online application is managed through SAP Mobilink and SAP Relay Server, which provide secure and encrypted communication channels to protect PII during transmission between the mobile device and the backend database servers located at the Ashburn Data Center (ADC).
PTA 16:	Does the mobile application have a privacy notice?	No
PTA 17:	Does the mobile application contain links to non-federal government websites external to HHS?	No
PTA 18:	Does the mobile application use measurement and customization technology?	No
PTA 19:	Does the mobile application have any information directed at children under the age of thirteen?	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.	Job title within the firm — While job title alone may not constitute PII in all contexts, when combined with other identifying information such as the POC's name and contact details, it may constitute PII. Mailing Address (Business) — The firm's mailing address is collected and maintained as part of the establishment record rather than as PII about a specific named individual. It is collected to accurately identify and document the physical location of the FDA-regulated establishment being inspected, and is necessary to create an official and legally defensible inspection record that can be used for compliance, enforcement, and analysis activities. While the firm's mailing address is listed as a PII type in PIA-22 for completeness, it is important to note that it is collected as establishment information rather than as personal contact information about a specific individual, and its inclusion in the inspection record does not constitute the collection of PII about a named individual in the traditional sense. Work fax number — Potential PII when associated with a specific named individual. FDA Establishment Identifier (FEI) number and inspection date — The FEI number and inspection date are collected and maintained as part of the inspection record-potential PII in combination with other information to identify a specific individual or establishment associated with an inspection. Free text narrative fields — eNSpect captures investigator observations and findings through free text fields, including FDA Form 483 citation observations, a summary of inspection findings, inspection endorsement, and the Establishment Inspection Report (EIR) narrative report. Because these are free text fields, they may contain any type of information the investigator deems necessary to document their findings and therefore may contain PII beyond what is otherwise specifically collected by the system. The nature and extent of any PII contained in these free text fields will vary depending on the specific inspection and the information recorded by the investigator.
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.	5,000 – 9,999

PIA 25:	For what primary purpose is the PII used?	The primary purpose for which PII is used in eNSpect is to support FDA's inspection, compliance, and enforcement mission. Specifically, FDA and OII use the PII collected and maintained in eNSpect to manage inspection actions, accurately document an inspection for compliance purposes, for business contact purposes, and in support of enforcement and analysis activities where inspection data is relevant. PII about firm POCs — including name(s), job title, work phone number, work email address, and work fax number — is used primarily to facilitate efficient communication between FDA investigators and the regulated establishment during and after the inspection process. This includes allowing FDA personnel to follow up with the appropriate individual at the firm regarding inspection findings, corrective actions, or other regulatory matters. Records are retrieved using firm POC PII elements only on rare occasions and solely for the purpose of efficient communication, such as when a firm POC contacts an inspector for direct follow-up. PII about FDA investigators — including first name, last name, work phone number, work email address, and work fax number — is used to accurately identify and attribute inspection records and legally significant documentation, including FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations), to the responsible investigator(s). This attribution is essential to the legal integrity of the inspection record and supports accountability in the inspection process.
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 following legal authorities govern the use and disclosure of information in eNSpect: Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. 374 — This provision of the FD&C Act specifically authorizes FDA investigators to conduct inspections of FDA-regulated establishments. It provides the legal basis for FDA's authority to enter and inspect facilities, review records, and collect information about regulated establishments and their operations. This is the primary legal authority under which eNSpect's inspection documentation and recordkeeping activities are conducted. Public Health Service Act (PHSA), 42 U.S.C. 262-264 — These provisions of the Public Health Service Act provide additional legal authority governing FDA's inspection and regulatory activities, particularly as they relate to biological products and public health matters. This authority supports FDA's broader mission to protect and promote public health through the inspection and regulation of establishments involved in the manufacture and distribution of biological products and other regulated commodities.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA 29A:	Please specify which PII data elements are used to retrieve records.	All of the PII elements in the system that are associated with firm POCs are used to retrieve records. These PII data elements include: Name(s) of the firm POC Job title within the firm Work phone number of the firm POC Work email address of the firm POC Work fax number of the firm POC It is important to note that these retrievals are rare and are conducted exclusively for the purpose of efficient communication, such as when a firm POC contacts an inspector for direct follow-up regarding an inspection. Record retrievals using firm POC PII elements are not a routine or frequent occurrence, but rather an exception conducted only when necessary to facilitate communication between FDA investigators and the regulated establishment.
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	SORN Number: 09-10-0002 SORN Title: Regulated Industry Employee Enforcement Records, HHS/FDA/OC URL: https://www.hhs.gov/privacy/sorns/09100002/index.html

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax 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 eNSpect because neither the system itself nor the standardized forms it generates are subject to the information collection approval requirements of the Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13). The basis for this determination is explained in detail below. eNSpect as an Internal System — eNSpect is an internal FDA inspection documentation and recordkeeping system used exclusively by FDA investigators and their supervisors to record, manage, and generate inspection documentation. Access to eNSpect is restricted exclusively to internal FDA personnel through FDA's enterprise Single Sign-On (SSO) authentication process and is not available to the general public. As such, eNSpect does not independently collect information from the public in a manner that triggers PRA requirements, which apply to standardized information collections directed at ten or more members of the public through forms, surveys, and questionnaires directed at the general public. FDA Form 482 (Notice of Inspection) — eNSpect is used to generate FDA Form 482, the Notice of Inspection, which is an administrative, legally mandated presentation of credentials issued by the federal government to a private facility under Section 704 of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. 374. Because FDA Form 482 represents a one-way statutory notification from the federal government to a regulated establishment, rather than an agency information collection request targeting the public, it does not fall under PRA reporting requirements and does not have an OMB control number. The form is exempt from PRA requirements. FDA Form 483 (Inspectional Observations) — eNSpect is also used to generate FDA Form 483, the Inspectional Observations form, which is an administrative law enforcement action issued during an active, targeted investigation of a specific FDA-regulated establishment. Under federal regulations, specifically 5 C.F.R. § 1320.3(h)(3), information collected in the field by agency investigators during an active audit or

		enforcement operation is completely exempt from PRA requirements and does not require an active OMB control number. Accordingly, FDA Form 483 does not have an OMB control number, and the physical form remains active and legally enforceable without one. It should be noted that a historical OMB tracking number, 0910-0563, did exist in the Reginfo.gov database, but was specifically assigned to the reporting burden associated with human drug manufacturers choosing to file formal appeal letters or scientific dispute resolutions regarding a Form 483's findings — not to the Form 483 itself. This tracking number is not an active OMB control number for the form and does not affect the form's exempt status under the PRA. Personally Identifiable Information (PII) Collected About Firm Points-of-Contact (POCs) — The PII collected about firm POCs — including name, job title, work phone number, work email address, and work fax number — is provided voluntarily by the individual POC or their employing firm in person at the time of inspection or during follow-up contact, and is collected in the context of FDA's statutory inspection authority under the FD&C Act, 21 U.S.C. 374 and the Public Health Service Act (PHSA), 42 U.S.C. 262-264. This type of information collection, conducted in the course of an agency's regulatory and law enforcement activities, is exempt from PRA requirements under 5 C.F.R. § 1320.4, which excludes from PRA coverage information collected during the conduct of an administrative action, investigation, or audit involving an agency against specific individuals or entities. PII Collected About FDA Investigators — The PII collected about FDA investigators is obtained from internal FDA systems — specifically FDA's Active Directory, the Enterprise Administrative Support Environment (EASE), and the OII Operations Database — rather than directly from the public and therefore does not constitute a public-facing information collection subject to PRA requirements. In summary, neither eNSpect as an internal system nor the standardized forms it generates — FDA Form 482 and FDA Form 483 — are subject to OMB information collection approval requirements under the PRA, and accordingly, no OMB information collection approval number is required for eNSpect.
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.	FDA employs different notification methods depending on the category of individual whose PII is collected and maintained in eNSpect. With respect to firm Points-of-Contact (POCs) at FDA-regulated establishments, notification is provided at the outset of the inspection through the issuance of FDA Form 482 (Notice of Inspection), which serves as formal notice that an FDA inspection is being conducted under the agency's statutory authority. Firm POC PII is provided voluntarily either by the individual POC themselves or by their employing firm in person at the time of inspection or during initial and/or follow-up contact with the firm. Individuals who do not wish to have their PII submitted may work with their employer to designate an alternative point-of-contact. Firm POCs may also object to or discuss inspection observations with the FDA representative during the inspection or by contacting FDA after the inspection. Public notice of FDA's collection, maintenance, use, and disclosure of firm POC PII is provided through Privacy Act SORN 09-10-0002. With respect to FDA investigators, PII is collected from internal FDA systems — specifically FDA's Active Directory, the Enterprise Administrative Support Environment (EASE), and the OII Operations Database — rather than directly from the investigators themselves. As federal employees, FDA investigators are subject to applicable federal laws, regulations, and agency policies governing the collection and use of employee information in the course of official duties. Prior individual consent for the inclusion of investigator work contact information in official inspection records and legal documentation is not required, as this information is necessary to fulfill FDA's statutory inspection and enforcement mission under the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. 374 and the Public Health Service Act (PHSA), 42 U.S.C. 262-264. FDA personnel are made aware of their privacy rights and responsibilities through mandatory annual security and privacy awareness training, system-specific training, and the Rules of Behavior.
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.	In the event of major changes to eNSpect that affect the collection, use, or disclosure of Personally Identifiable Information (PII) — such as changes to data uses or disclosure practices that differ from the notice provided at the time of original collection — FDA will employ different processes to notify affected individuals depending on their category. With respect to firm Points-of-Contact (POCs) at FDA-regulated establishments, FDA will provide notice of any material changes through updates to Privacy Act System of Records Notice (SORN) 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," published in

the Federal Register in accordance with the requirements of the Privacy Act of 1974, 5 U.S.C. 552a, and Office of Management and Budget (OMB) guidance. It should be noted that providing prior individual notice to all firm POCs whose PII is maintained in eNSpect may not always be practicable, given that the system maintains PII about an estimated 5,000 to 9,999 individuals associated with FDA-regulated establishments across a wide range of industry sectors. In such cases, FDA will rely on Federal Register notices and updates to the applicable SORN as the primary means of providing public notice of any material changes to the collection, use, or disclosure of firm POC PII in eNSpect, consistent with the requirements of the Privacy Act of 1974, 5 U.S.C. 552a. This Privacy Impact Assessment (PIA) will also be updated to reflect any such changes during the next scheduled assessment.

With respect to FDA investigators, notification of major changes to the system that affect the collection, use, or disclosure of investigator PII will be provided through internal FDA communication channels, including updates to system-specific training materials, the Rules of Behavior, and other agency privacy guidance. As federal employees, FDA investigators are already subject to applicable federal laws, regulations, and agency policies governing the collection and use of employee information in the course of official duties, and are made aware of any relevant changes through mandatory annual security and privacy awareness training, the completion of which is tracked by the Office of Digital Transformation (ODT).

In all cases, any material changes to the collection, use, or disclosure of PII in eNSpect that require updates to the applicable SORN will be processed in accordance with OMB guidance and the requirements of the Privacy Act of 1974, 5 U.S.C. 552a, including the publication of any required Federal Register notices prior to the implementation of such changes. Any individual with a concern about changes to the collection or use of their PII may contact the FDA Privacy program using information provided on FDA.gov, or may consult SORN 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html, for additional information about their Privacy Act rights.

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.	Personnel may raise concerns and/or submit data corrections through supervisory channels and FDA's Employee Resource and Information Center (ERIC). Individuals who are members of the inspected establishment (firm) may contact FDA through numerous paths such as email, phone, and standard mail avenues, all of which are listed on FDA.gov. Additionally, 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 feel is inaccurate. All FDA personnel are required to rapidly report the potential or suspected unauthorized access or use of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Individuals seeking to understand their Privacy Act rights regarding the PII maintained in eNSpect, including their right to access and amend their records, should consult SORN 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html. Any individual with a concern about their PII may also contact the FDA Privacy program using information provided on FDA.gov.

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.	All PII maintained in eNSpect is relevant to FDA's inspection, compliance, and enforcement mission. Forms and processes are designed to collect only PII that is necessary for the relevant agency activity. PII about a firm point-of-contact is necessary to communicate with regulated establishments, and PII about FDA investigators is necessary to accurately attribute inspection records and legally significant documentation to the responsible investigator(s). Accuracy is ensured by individual review of inspection reports and correcting data in the course of OII's use of the system and information, such as updating the name and phone number for an establishment point-of-contact. Firms and individuals may amend their submitted contact information by contacting FDA. FDA personnel may correct and update their own information through the internal FDA systems from which investigator PII is sourced, specifically FDA's Active Directory, the Enterprise Administrative Support Environment (EASE), and the OII Operations Database. Integrity and availability are protected by security controls selected and implemented in the course of providing the system with an Authority to Operate (ATO). Controls are selected based on National Institute of Standards and Technology (NIST) guidance concerning the ATO process, appropriate to the system's level of risk as determined using NIST's Federal Information Processing Standards (FIPS) 199. The access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted, with unneeded accounts purged from the system, to ensure that only authorized personnel retain access to PII maintained in eNSpect. The periodic review process for PII maintained in eNSpect is conducted in a manner consistent with the retention and access requirements outlined in SORN 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html. Records are maintained and destroyed in accordance with the National Archives and Records Administration (NARA) Citation N1-088-09-1, FDA file code 7300 series, for Establishment Inspections and Compliance Action Files, with records destroyed 10 years after classification of an inspection as "no action indicated" or "voluntary action indicated," and 30 years after the close of a case where official action was indicated.
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 need access to PII to perform and document FDA inspections at regulated establishments. This includes recording firm POC information, generating legally required inspection documentation such as FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations), and managing inspection records in support of FDA's compliance and enforcement mission. Administrators need access to PII in the course of performing analysis of historical inspection activities and to review work in process. Administrator access to PII is necessary to ensure the integrity, availability, and accuracy of inspection records maintained in eNSpect, and to support the overall management and operation of the system. Developers need access to PII to perform level 3 helpdesk support activities. This level of support involves resolving complex technical issues that require direct access to system data, including PII, that cannot be addressed at lower helpdesk support levels without such access. Contractors need access to PII to perform level 1 and level 2 helpdesk support activities. This includes resolving user-reported technical issues and support requests that may require access to PII maintained in eNSpect in order to identify and resolve the reported issue. Contractor access to PII is governed by FAR and other appropriate privacy clauses included in their contracts with FDA, ensuring that PII is handled in a manner consistent with applicable federal privacy laws, regulations, and agency policies.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	FDA has established a comprehensive set of administrative procedures to determine which system users may access PII maintained in eNSpect. These procedures apply to all categories of individuals with access to the system, including users, administrators, developers, and contractors, and are designed to ensure that access to PII is granted only to those individuals who have a demonstrated need to know in the performance of their official duties. System access requests for eNSpect are reviewed and approved by the system and business owner along with the eNSpect management team. Access is granted and restricted at the individual level as appropriate to the individual's duties, using a role-based access control model that ensures each user is granted only the minimum level of access necessary to perform their job responsibilities. This Need to Know and Minimum Necessary approach

		to access management ensures that PII maintained in eNSpect is accessible only to those individuals who require it to fulfill their specific role in the inspection, compliance, and enforcement process. System accounts are reviewed on a regular basis to determine if access is still required for each user. Specifically, the access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted as appropriate, with unneeded accounts purged from the system to ensure that only authorized personnel retain access to PII maintained in eNSpect. This quarterly review process applies to all categories of system users, including users, administrators, developers, and contractors, and is designed to ensure that access privileges remain current and appropriate to each individual's duties and responsibilities. With respect to contractors, all HHS/OpDiv Direct Contractors with access to PII maintained in eNSpect are subject to contracts that include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. These contractual provisions ensure that contractors who have access to PII are legally obligated to handle that information in a manner consistent with applicable federal privacy laws, regulations, and agency policies, including the Privacy Act of 1974, 5 U.S.C. 552a, and HHS and FDA privacy policies and guidance. All FDA personnel and contractors with access to eNSpect are required to complete mandatory annual security and privacy awareness training at a minimum of once a year, the completion of which is tracked by the Office of Digital Transformation (ODT). Additionally, all system 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. These training and awareness requirements ensure that all individuals with access to PII maintained in eNSpect are aware of their responsibilities for protecting that information and are equipped to handle it in a manner consistent with applicable federal privacy laws, regulations, and agency policies.
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.	eNSpect employs several technical methods to ensure that individuals with access to PII maintained in the system can access only the minimum amount of information necessary to perform their job responsibilities. These technical methods complement the administrative procedures and together form a comprehensive access control framework designed to protect the privacy and security of PII maintained in eNSpect. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) — Access to the eNSpect online application is controlled through FDA's

enterprise SSO authentication process, which incorporates MFA using the investigator's FDA PIV card. This ensures that only authenticated and authorized FDA personnel can access the system and the PII it contains. eNSpect does not require, use, collect, or maintain system-specific logon credentials such as a separate username and password, as authentication is handled entirely through the FDA enterprise/Active Directory SSO process.

Role-Based Access Control — When system accounts are created for personnel, supervisors determine the scope of required access and apply the minimum information system access that is required for the user to complete his or her job. Access is granted and restricted at the individual level as appropriate to the individual's duties, using a role-based access control model that ensures each user is granted only the minimum level of access necessary to perform their specific job responsibilities. This technical implementation of the Need to Know and Minimum Necessary principles ensures that PII maintained in eNSpect is accessible only to those individuals who require it to fulfill their specific role in the inspection, compliance, and enforcement process.

Quarterly Access Reviews — The access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted as appropriate, with unneeded accounts purged from the system. This technical control ensures that access privileges remain current and appropriate to each individual's duties and responsibilities, and that individuals who no longer require access to PII maintained in eNSpect are promptly removed from the system.

Offline Application Controls — The eNSpect offline application, which is locally installed on FDA-issued Windows laptops and tablets, incorporates technical controls to ensure that access to PII collected during field inspections is restricted to authorized FDA investigators and their supervisors. The offline application utilizes mobile device management infrastructure, including SAP Afaria 7.0, to manage and secure FDA-issued devices and the PII stored on them during field inspections. Data synchronization between the offline application and the eNSpect online application is managed through SAP Mobilink and SAP Relay Server, which provide secure communication channels to protect PII during transmission between the mobile device and the backend database.

Physical and Infrastructure Security — All eNSpect system servers are located at FDA facilities, specifically the Ashburn Data Center (ADC), protected by guards, locked facility doors, and climate controls. The production and pre-production environments are hosted on Oracle WebLogic 19c application servers running Oracle

		Enterprise Linux 8.x, with additional SAP Mobilink, SAP Relay Server, and SAP SQL Anywhere components supporting the offline inspection capabilities of the system. Access to the underlying database and server infrastructure is restricted to authorized system administrators and is controlled through a combination of network security controls, including firewalls and intrusion detection systems, and database-level access controls that enforce the minimum necessary access principles described above. Security Controls — Additional technical safeguards have been selected and implemented from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as determined using Federal Information Processing Standard (FIPS) 199, appropriate to the system's level of risk. These controls include the use of firewalls, access controls, and regular testing of information technology systems to ensure the ongoing protection of PII maintained in eNSpect.
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 and contractors with access to eNSpect, including system owners, managers, operators, contractors, and program managers, are required to complete mandatory security and privacy awareness training at a minimum of once a year. Completion of mandatory annual security and privacy awareness training is tracked by the Office of Digital Transformation (ODT) to ensure that all system users remain current in their training requirements. This training is designed to ensure that all individuals with access to information maintained in eNSpect, including Personally Identifiable Information (PII), are aware of their responsibilities for protecting that information in accordance with applicable federal privacy laws, regulations, and agency policies, including the following: Privacy Act of 1974, 5 U.S.C. 552a — Training covers the requirements of the Privacy Act of 1974, including the rights of individuals whose PII is collected and maintained in federal information systems, and the responsibilities of federal employees and contractors for protecting that information in accordance with applicable Privacy Act provisions and agency privacy policies, including Privacy Act System of Records Notice (SORN) 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html. Federal Information Security Modernization Act (FISMA) — Training covers the requirements of the Federal Information Security Modernization Act (FISMA) and applicable National Institute of Standards and Technology (NIST) guidance, including the security controls selected and implemented to protect federal information systems and the information they contain,

		consistent with NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, and Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. PII Handling and Protection — Training covers the proper handling, use, and protection of PII collected and maintained in federal information systems, including the Need to Know and Minimum Necessary principles that govern access to PII, the prohibition on unauthorized access to or disclosure of PII, and the procedures for reporting suspected or confirmed unauthorized access to or disclosure of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). Incident Reporting — Training covers the procedures for rapidly reporting the potential or suspected unauthorized access or use of PII to the CIOCC, consistent with FDA's incident response policies and procedures and applicable federal incident response requirements, including NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide. Roles and Responsibilities — Training covers the specific roles and responsibilities of system owners, managers, operators, contractors, and program managers with respect to the protection of information collected and maintained in federal information systems, including eNSpect, and the consequences of failing to fulfill those responsibilities in accordance with applicable federal laws, regulations, and agency policies. HHS and FDA Privacy and Security Policies — Training covers applicable HHS and FDA privacy and security policies and guidance, including the FDA Information Security and Privacy Protection Guide (IS2P), and ensures that all system users are aware of and comply with agency-specific privacy and security requirements applicable to eNSpect and the PII it contains.
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 described in PIA-42, all eNSpect system users receive system-specific training and are subject to additional requirements designed to ensure that they are equipped to use the system in a manner consistent with applicable federal privacy laws, regulations, and agency policies, and that they are aware of their specific responsibilities for protecting the PII collected and maintained in eNSpect in the course of their official duties. The following system-specific training and additional requirements apply to all categories of eNSpect system users, including users, administrators, developers, and contractors: System-Specific Training — All eNSpect system users receive system-specific training that covers

the purpose, functionality, and proper use of the eNSpect system, including both the offline application used during field inspections and the online application used to manage, finalize, and submit inspection reports and associated documentation after returning from the field. This training ensures that system users are familiar with the technical capabilities and limitations of the system, including the mobile device management and data synchronization infrastructure — specifically Systems, Applications, and Products in Data Processing (SAP) Afaria 7.0, SAP Mobilink, SAP Relay Server, and SAP Structured Query Language (SQL) Anywhere — that supports eNSpect's offline inspection capabilities, and that they are equipped to use the system in a manner that protects the privacy and security of PII collected and maintained in eNSpect. System-specific training also covers the proper handling and protection of PII collected during field inspections, including the PII of firm Points-of-Contact (POCs) and FDA investigators maintained in eNSpect as part of the official inspection records and legal documentation generated during the inspection process.

Rules of Behavior — All eNSpect system users are required to review and adhere to the Rules of Behavior for the system, which set forth the specific responsibilities and expected behaviors of system users with respect to the protection of information collected and maintained in eNSpect, including PII. The Rules of Behavior cover topics such as the proper handling and use of PII, the prohibition on unauthorized access to or disclosure of PII, the requirement to use eNSpect only on FDA-issued Windows laptops and tablets managed through SAP Afaria 7.0, and the procedures for reporting suspected or confirmed unauthorized access to or disclosure of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC). System users are required to acknowledge their understanding of and agreement to comply with the Rules of Behavior as a condition of being granted access to eNSpect, and this acknowledgment is documented and maintained by the eNSpect management team as part of the system's access control records.

Role-Specific Privacy Guidance — In addition to system-specific training and the Rules of Behavior, eNSpect system users may obtain additional privacy guidance from the agency's privacy officials as needed to address specific privacy questions or concerns that arise in the course of their use of the system. This role-specific privacy guidance is designed to supplement the general security and privacy awareness training and system-specific training described above, and to ensure that system users have access to the privacy expertise and guidance they need to fulfill their responsibilities for protecting PII collected and maintained in eNSpect in accordance with applicable federal privacy laws, regulations, and agency policies, including Privacy Act System of Records Notice (SORN) 09-10-0002, "Regulated

		Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html. Helpdesk Support Training — Contractors performing level 1 and level 2 helpdesk support activities, as well as developers performing level 3 helpdesk support activities, receive additional training specific to their roles in supporting eNSpect users. This training covers the proper handling and protection of PII that may be accessed in the course of performing helpdesk support activities, including the procedures for escalating privacy-related issues to the appropriate FDA privacy officials and for reporting suspected or confirmed unauthorized access to or disclosure of PII to the CIOCC. Helpdesk support training also ensures that contractors and developers are aware of their obligations under the Federal Acquisition Regulation (FAR) and other appropriate privacy clauses included in their contracts with FDA, and that they handle PII maintained in eNSpect in a manner consistent with applicable federal privacy laws, regulations, and agency policies. Digital Signature and Personal Identity Verification (PIV) Card Training — FDA investigators and their supervisors who use eNSpect to generate and sign legally required inspection documentation, including FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations), receive additional training on the proper use of digital signatures via the FDA Personal Identity Verification (PIV) card as required on these forms. This training ensures that investigators are familiar with the digital signature process and are equipped to use their FDA PIV card in a manner consistent with applicable federal identity, credential, and access management requirements, including Federal Information Processing Standard (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors.
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	FDA has established processes and guidelines for the retention and destruction of PII maintained in eNSpect that are consistent with applicable federal records management requirements, including the Federal Records Act, 44 U.S.C. 31, the Privacy Act of 1974, 5 U.S.C. 552a, and the regulations and guidance issued by the National Archives and Records Administration (NARA). These processes and guidelines apply to all categories of PII maintained in eNSpect, including PII about firm Points-of-Contact (POCs) at FDA-regulated establishments and PII about FDA investigators, and are designed to ensure that PII is retained only for as long as necessary to fulfill the purposes for which it was collected and to meet applicable legal and regulatory requirements. NARA Records Retention Schedule — eNSpect records, including all PII maintained in the system, are retained and destroyed in accordance with the

following NARA records retention schedule:

NARA Citation: N1-088-09-1
FDA File Code: 7300 series
Record Series Title: Establishment Inspections and Compliance Action Files
Retention Periods — The retention periods applicable to eNSpect records under NARA Citation N1-088-09-1 are as follows:

10 years after classification of an inspection as "no action indicated" or "voluntary action indicated" — Records associated with inspections that result in no regulatory action or voluntary corrective action by the inspected establishment are retained for a period of 10 years following the classification of the inspection, after which they are destroyed in accordance with applicable NARA records destruction requirements. This retention period applies to all PII maintained in eNSpect as part of those inspection records, including PII about firm POCs and FDA investigators associated with the inspection.

30 years after the close of a case where official action was indicated — Records associated with inspections that result in official regulatory action by FDA, such as a Warning Letter, injunction, seizure, or other enforcement action, are retained for a period of 30 years following the close of the case, after which they are destroyed in accordance with applicable NARA records destruction requirements. This retention period applies to all PII maintained in eNSpect as part of those inspection records, including PII about firm POCs and FDA investigators associated with the inspection and any resulting enforcement action.

Destruction Process — Upon reaching the applicable retention period, eNSpect records, including all PII maintained in the system, are destroyed in accordance with applicable NARA records destruction requirements and FDA records management policies and procedures. The destruction of records is carried out in a manner that ensures the complete and irreversible destruction of all PII contained in the records, consistent with the requirements of the Privacy Act of 1974, 5 U.S.C. 552a, and applicable NIST guidance on the secure disposal of information system media, including NIST Special Publication (SP) 800-88, Guidelines for Media Sanitization. This includes the secure destruction of PII stored on FDA-issued Windows laptops and tablets used by investigators in the field, which is managed through the mobile device management infrastructure, specifically SAP Afaria 7.0, in accordance with FDA's mobile device management policies and procedures.

All PII maintained in eNSpect is relevant to FDA's inspection, compliance, and enforcement mission, and forms and processes are designed to collect only PII that is necessary for the relevant agency

		activity. PII about firm POCs is necessary to communicate with regulated establishments and to accurately document inspection records and legal documentation, while PII about FDA investigators is necessary to accurately attribute inspection records and legally significant documentation to the responsible investigator(s). PII is retained only for as long as necessary to fulfill these purposes and to meet the applicable retention periods specified in NARA Citation N1-088-09-1 and is destroyed promptly upon reaching the applicable retention period in accordance with the destruction process described above. The retention and destruction of eNSpect records, including all PII maintained in the system, is overseen by the eNSpect system owner and business owner in coordination with FDA's records management officials and privacy officials. The system owner and business owner are responsible for ensuring that eNSpect records are retained and destroyed in accordance with the applicable NARA records retention schedule and FDA records management policies and procedures, and that any changes to the retention and destruction requirements applicable to eNSpect records are reflected in updates to this Privacy Impact Assessment (PIA) and the applicable Privacy Act System of Records Notice (SORN) 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html.
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.	FDA has implemented a comprehensive set of administrative, technical, and physical controls to secure PII maintained in eNSpect in accordance with applicable federal information security and privacy requirements, including the Federal Information Security Modernization Act (FISMA), the Privacy Act of 1974, 5 U.S.C. 552a, and applicable National Institute of Standards and Technology (NIST) guidance. Security controls have been selected and implemented based on NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, as determined using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, appropriate to the system's level of risk. Each of the three categories of security controls is described in detail below. Administrative controls are policies, procedures, and practices designed to ensure that PII maintained in eNSpect is handled in a manner consistent with applicable federal privacy laws, regulations, and agency policies. The following administrative controls are in place to secure PII maintained in eNSpect: Mandatory Annual Security and Privacy Awareness Training — All FDA personnel and contractors with

access to eNSpect, including system owners, managers, operators, contractors, and program managers, are required to complete mandatory annual security and privacy awareness training at a minimum of once a year. Completion of this training is tracked by the Office of Digital Transformation (ODT) to ensure that all system users remain current in their training requirements. This training covers the requirements of the Privacy Act of 1974, 5 U.S.C. 552a, the Federal Information Security Modernization Act (FISMA), applicable NIST guidance, and HHS and FDA privacy and security policies and guidance, including the FDA Information Security and Privacy Protection Guide (IS2P), and ensures that all system users are aware of their responsibilities for protecting PII collected and maintained in eNSpect.

System-Specific Training and Rules of Behavior — In addition to mandatory annual security and privacy awareness training, all eNSpect system users receive system-specific training and are required to review and adhere to the Rules of Behavior for the system, which set forth the specific responsibilities and expected behaviors of system users with respect to the protection of PII collected and maintained in eNSpect. System users are required to acknowledge their understanding of and agreement to comply with the Rules of Behavior as a condition of being granted access to eNSpect, and this acknowledgment is documented and maintained by the eNSpect management team as part of the system's access control records.

Need to Know and Minimum Necessary Access — System access requests for eNSpect are reviewed and approved by the system and business owner along with the eNSpect management team. Access is granted and restricted at the individual level as appropriate to the individual's duties, using a role-based access control model that ensures each user is granted only the minimum level of access necessary to perform their specific job responsibilities. This Need to Know and Minimum Necessary approach to access management ensures that PII maintained in eNSpect is accessible only to those individuals who require it to fulfill their specific role in the inspection, compliance, and enforcement process.

Quarterly Access Reviews — The access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted as appropriate, with unneeded accounts purged from the system. This administrative control ensures that access privileges remain current and appropriate to each individual's duties and responsibilities, and that individuals who no longer require access to PII maintained in eNSpect are promptly removed from the system.

Contractor Privacy Obligations — All HHS/OpDiv

Direct Contractors with access to PII maintained in eNSpect are subject to contracts that include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices. These contractual provisions ensure that contractors who have access to PII are legally obligated to handle that information in a manner consistent with applicable federal privacy laws, regulations, and agency policies, including the Privacy Act of 1974, 5 U.S.C. 552a, and HHS and FDA privacy policies and guidance.

Incident Reporting — All FDA personnel are required to rapidly report the potential or suspected unauthorized access or use of PII to the Cybersecurity and Infrastructure Operations Coordination Center (CIOCC), consistent with FDA's incident response policies and procedures and applicable federal incident response requirements, including NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide. This administrative control ensures that any potential or confirmed privacy incidents involving PII maintained in eNSpect are promptly identified, reported, and addressed in accordance with applicable federal incident response requirements.

Records Retention and Destruction — eNSpect records, including all PII maintained in the system, are retained and destroyed in accordance with National Archives and Records Administration (NARA) Citation N1-088-09-1, FDA file code 7300 series, for Establishment Inspections and Compliance Action Files. Records are destroyed 10 years after classification of an inspection as "no action indicated" or "voluntary action indicated," and 30 years after the close of a case where official action was indicated, consistent with applicable NARA records retention and destruction requirements and NIST Special Publication (SP) 800-88, Guidelines for Media Sanitization.

Privacy Act System of Records Notice (SORN) — PII maintained in eNSpect is covered by Privacy Act System of Records Notice (SORN) 09-10-0002, "Regulated Industry Employee Enforcement Records, HHS/FDA/OC," available at https://www.hhs.gov/privacy/sorns/09100002/index.html, which provides public notice of FDA's collection, maintenance, use, and disclosure of PII maintained in eNSpect and ensures that the system's privacy practices are consistent with the requirements of the Privacy Act of 1974, 5 U.S.C. 552a.

Technical controls are hardware and software mechanisms designed to protect PII maintained in eNSpect from unauthorized access, use, disclosure, modification, or destruction. The following technical controls are in place to secure PII maintained in eNSpect:

Single Sign-On (SSO) and Multi-Factor Authentication (MFA) — Access to the eNSpect online application is controlled through FDA's enterprise Single Sign-On (SSO) authentication process, which incorporates Multi-Factor Authentication (MFA) using the investigator's FDA Personal Identity Verification (PIV) card. This ensures that only authenticated and authorized FDA personnel can access the system and the PII it contains. eNSpect does not require, use, collect, or maintain system-specific logon credentials such as a separate username and password, as authentication is handled entirely through the FDA Enterprise Active Directory and Oracle Internet Directory (OID) via the FDA enterprise SSO process, consistent with Federal Information Processing Standard (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors.

Role-Based Access Control — eNSpect implements a role-based access control model that restricts access to PII based on each user's specific job responsibilities and duties. When system accounts are created for personnel, supervisors determine the scope of required access and apply the minimum information system access that is required for the user to complete his or her job, ensuring that PII maintained in eNSpect is accessible only to those individuals who require it to fulfill their specific role in the inspection, compliance, and enforcement process. The access list for the information system is reviewed on a quarterly basis, and users' access permissions are reviewed and adjusted as appropriate, with unneeded accounts purged from the system.

Mobile Device Management and Offline Security — The eNSpect offline application, which is locally installed on FDA-issued Windows laptops and tablets, incorporates mobile device management infrastructure, including SAP Afaria 7.0, to manage and secure FDA-issued devices and the PII stored on them during field inspections. Data synchronization between the offline application and the eNSpect online application is managed through SAP Mobilink and SAP Relay Server, which provide secure and encrypted communication channels to protect PII during transmission between the mobile device and the backend database servers located at the Ashburn Data Center (ADC). SAP SQL Anywhere serves as the local database on FDA-issued mobile devices to store PII collected during field inspections and is secured through the mobile device management controls described above.

Firewalls and Intrusion Detection Systems — Network traffic to and from eNSpect is controlled and monitored by firewalls and intrusion detection systems (IDSs) to protect PII maintained in the system from unauthorized access, use, or disclosure. These technical controls are supplemented by the Security Management Center

(SMC), which monitors the FDA enterprise network for unusual behavior that may indicate a potential security incident involving PII maintained in eNSpect, consistent with NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations.

Encryption and Secure Communications — PII transmitted between the eNSpect offline application, and the online application is protected through secure and encrypted communication channels, including SAP Relay Server, which provides encrypted data transmission to protect PII during synchronization between the mobile device and the backend database. Additional encryption controls have been implemented in accordance with applicable NIST guidance and Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, to ensure the confidentiality and integrity of PII transmitted to and from eNSpect.

Database Security — Access to the eNSpect backend databases, which are hosted on Oracle 19c database servers running Oracle Enterprise Linux 8.x at the Ashburn Data Center (ADC), is restricted to authorized system administrators and is controlled through a combination of database-level access controls, including user accounts, passwords, and database roles, that enforce the minimum necessary access principles described above. Access to the database server requires both a server account identification and password combination and an Oracle account identification and password to run specific Oracle applications, ensuring that unauthorized individuals cannot gain access to PII maintained in the eNSpect backend databases.

Continuous Monitoring — eNSpect is subject to continuous monitoring in accordance with applicable NIST guidance, including NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, to ensure the ongoing protection of PII maintained in the system. This includes regular vulnerability scanning, security assessments, and other monitoring activities designed to identify and address potential security risks to PII maintained in eNSpect in a timely manner, consistent with FDA's information security continuous monitoring program and the FDA Information Security and Privacy Protection Guide (IS2P).

Digital Signatures — eNSpect utilizes digital signatures via the investigator's FDA Personal Identity Verification (PIV) card as required on FDA Form 482 (Notice of Inspection) and FDA Form 483 (Inspectional Observations) and Establishment Inspection Report (EIR) documentation. This technical control ensures the integrity and authenticity of legally significant inspection

documentation generated by eNSpect, and provides a tamper-evident record of the investigator's findings and observations at the inspected establishment, consistent with applicable federal digital signature requirements.

Physical controls are measures designed to protect the physical infrastructure supporting eNSpect and the PII maintained in the system from unauthorized physical access, damage, or destruction. The following physical controls are in place to secure PII maintained in eNSpect:

Secured Data Center Facilities — All eNSpect system servers are located at the Ashburn Data Center (ADC), an FDA facility protected by a comprehensive set of physical security controls, including security guards, locked facility doors, access control systems, and climate controls. These physical controls ensure that unauthorized individuals cannot gain physical access to the servers and infrastructure supporting eNSpect and the PII maintained in the system, consistent with applicable NIST guidance on physical and environmental protection, including NIST Special Publication (SP) 800-53 controls PE-1 through PE-20.

FDA-Issued Mobile Devices — The eNSpect offline application is deployed exclusively on FDA-issued Windows laptops and tablets, which are subject to FDA's mobile device management policies and procedures, including SAP Afaria 7.0 for mobile device management. These physical controls ensure that the PII collected during field inspections is stored only on FDA-issued and managed devices, and that unauthorized individuals cannot gain physical access to the PII stored on those devices. In the event that an FDA-issued device is lost or stolen, SAP Afaria 7.0 provides the capability to remotely wipe the device to prevent unauthorized access to PII stored on the device.

Access Controls for Physical Infrastructure — Access to the physical infrastructure supporting eNSpect, including the servers and networking equipment located at the Ashburn Data Center (ADC), is restricted to authorized system administrators and other personnel with a demonstrated need for physical access to that infrastructure. Physical access controls include security guards, locked facility doors, and access control systems that require authorized personnel to authenticate their identity before gaining physical access to the data center facilities, consistent with applicable NIST guidance on physical and environmental protection.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/19/2026
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/19/2026
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: Crystal bland 5/21/2026 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	2

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 3:08 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	5/21/2026	5/21/2026 Per FDA's email attached a copy of the PIA.	OII Electronic Inspection System (eNSPECT)_SOP approved.pdf