PTA / PIA: FDA - Intella Connect - QTR2 - 2025 - FDA4929942

Created Date: 5/23/2025 4:37 PM Last Updated: 6/24/2025 4:45 PM

General Information

PTA / PIA Name:	FDA - Intella Connect - QTR2 - 2025 - FDA4929942	**PTA / PIA ID:**	3213929
Component Name:	FDA - OII Intella Connect	**ATO Boundary Name:**	CBER Office of Regulatory Operations
Overall Status:	Complete	**# of Days - Open:**	32
Submitter:		**Submit Date:**	5/23/2025
Next Assessment Date:	06/23/2028	**Expiration Date:**	6/23/2028
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?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
General 04:	ATO Date or Planned ATO Date.	5/18/2023
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	Stephan Reimers
PTA 01A:	POC Title and Organization	POC Title: Criminal Investigator/Senior Operations Manager POC Organization: Office of Regulatory Affairs (OII)
PTA 01B:	POC Email Address	Stephan.Reimers@fda.hhs.gov
PTA 01C:	POC Phone Number	240-642-8091
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)

PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The Food and Drug Administration (FDA) has made no changes to this system 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.	The FDA's Office of Criminal Investigations (OCI) utilizes the Digital Acquisition Reporting System (DARS) for law enforcement purposes. DARS is comprised of two components: Atlas and Intella Connect Plus. Intella Connect Plus is an eDiscovery platform that provides large amounts of data in a single solution used by FDA's Office of Criminal Investigations (OCI) within the Office of Inspections and Investigations (OII). As used by OCI, Intella Connect Plus provides a document repository for digital evidence, scanned versions of documents, and other evidence relevant to specific criminal investigations. It may contain digitalized evidence that has been recovered in accordance with court issued search warrants, subpoenas issued by the prosecution team, witness interviews with FDA Criminal Investigators, private sector sources, anonymous sources, social media sources, and pertinent information recovered from other sources during a criminal investigation. Sources of collected information include physical copies and electronic copies of documents recovered from regulated entities. Regulated entities can consist of individuals, groups, businesses, and other organizations as well as any other place or source specified in a court order or other legal authority. Evidence may also be collected directly from prospective witnesses and/or people under investigation.

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.	The documents and materials recovered and maintained via OCI's use of Intella Connect Plus include information required by law enforcement for law enforcement activities. The documents and materials may contain a variety of personally identifiable information (PII) including: (a) first and last name; (b) office and or personal email address; (c) office or personal phone number ; (d) personal mailing address; (e) financial account information; (f) receipts; (g) laboratory reports; (h) medical record information; (i) medical notes; (j) Social Security number; (k) driver's license number; (l) mother's maiden name; (m) certificates; (n) date of birth; (o) other photographic identifiers; (p) vehicle identifiers; (q) legal documents; (r) device identifiers and; (s) passwords. The documents recovered may also include office location, business telephone numbers, business email addresses and other administrative or work contact information. OCI may obtain PII from various sources including from FDA offices, other Department of Health and Human Services (HHS) Operating Divisions, Federal agencies outside HHS, State/Local/Tribal authorities, and foreign entities. The information in Intella Connect Plus also includes non-PII such as information about FDA-regulated products related to an agency investigation of misbranding, tampering, counterfeiting, buying, and/or selling such products illegally.
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card

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.	OCI uses Intella Connect Plus to store digital data on secure physical and virtual servers located within OCI Headquarters. To control system access, OCI's use of Intella Connect Plus employs multi-factor authentication requiring a Personal Identity Verification (PIV) card. Intella Connect Plus is only accessible by approved OCI IT staff (FDA employees and some Direct Contractors) with elevated privileges and\or access that is granted to users by an Intella Connect Plus administrator. Users are provided access via account creation by the Intella Connect Plus Administrator. Permissions are granted where least privileges are enforced, and user access is granted on a case-by-case basis. Evidence collected from the various sources includes information about individuals such as the subjects of investigations. Subjects of an investigation are typically members of the public, and in some instances may be FDA employees and/or Direct Contractors. OCI may investigate any person or person(s) where there is indication or signs of improper activity as it relates to misbranding, counterfeiting, tampering, buying or selling products illegally. Documents maintained in Intella Connect Plus may include information required by law enforcement in support of law enforcement activities and may contain a variety of PII about witnesses, investigators, the individual subjects of an investigation, and any other individuals with knowledge or information relevant to an investigation. Documents recovered may contain transactional contact information about individuals such as office location, business telephone numbers, business email addresses and other administrative or work contact information. Investigators (FDA employees and Direct Contractors) using Intella Connect Plus retrieve system records in different ways including utilizing several PII data types to retrieve information about and/or gathered from subjects, witnesses and others relevant to an investigation.
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://cishqs56.fda.gov:9999/
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	No
PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The purpose of the website is to access the system and only designated OCI users can access the web application. Users access the internal website via FDA issued computers and single sign on (SSO) credentials.
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?	No
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 Social Security Number Taxpayer ID Number (TIN) Passport Number Financial Account Information (e.g., account numbers, credit card numbers) Vehicle Identifiers (e.g., VIN, license plate number) Biographical Information Name Date of Birth Certificates (e.g., training certificates) Education Records Employment Status/History Legal Documents Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Email Address (Business) Mailing Address (Business) Phone Numbers (Business) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Photographic Identifiers Medical Information Medical Records Medical Records Number
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Patients Members of the public Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)

PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	100,000 – 999,999
PIA 25:	For what primary purpose is the PII used?	PII used in Intella Connect Plus may be an incidental capture of PII or may be a directed collection mandated by a court-order. Either way, the PII may be used to identify and associate individuals with actions and evidence in support of investigations of criminal activity related to suspected violations of the U.S. Federal Food, Drug, and Cosmetic Act (21 U.S.C. 372) and other crimes.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	OCI makes no secondary use of the PII.
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	SSNs maintained in Intella Connect Plus are not solicited or collected directly from individuals. SSNs may be maintained in the system incidentally when contained in documents collected during a criminal investigation.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	While an individual's SSN is not solicited or collected directly from the individual, SSNs may be incidentally collected in this system in the course of OCI investigative actions as authorized by warrant, court order or other federal legal process and authority. Authority is also provided in the Federal Food, Drug, and Cosmetic Act (e.g., 21 U.S.C. 372, establishing authority to conduct examinations and investigations; 21 U.S.C. 331 listing prohibited acts) and the crimes and criminal procedure provisions of Title 18 of the U.S. Code (U.S.C.). The use of the SSN as an identifier for federal employees is permissible per Executive Order 9397, as amended by Executive Order 13478 issued November 18, 2008. The collection of information in this Privacy Act system is covered by FDA System of Records Notices (SORNs) 09-10-002 and 09-10-0013 and the collection of information and evidence is provided for by the legal authorities specified in the SORNs including: 5 U.S.C. 301; Title 18 of the U.S. Code (U.S.C.); 21 U.S.C. 301, 331 (Federal Food, Drug, and Cosmetic Act); 28 U.S.C. 535(b); 44 U.S.C. 3101; 42 U.S.C. 201 (Federal Public Health Service Act); 45 CFR part 73; and, Executive Order 10450.

PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Section 702 of the U.S. Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301, 372) authorizes OCI to conduct investigations. Secrecy and confidentiality of information is further governed by the Federal Rules of Criminal Procedure (FRCP) Title III, Rule 6(e). 5 U.S.C. 301 authorizes the necessary establishment of systems and processes to maintain records and conduct agency activities.
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.	Investigators (FDA employees and Direct Contractors) using Intella Connect Plus retrieve system records in different ways. Generally, free text keywords are used that may include several PII data types to retrieve information about and/or gathered from subjects, witnesses and others relevant to an investigation.
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 1: 09-10-0002, Regulated Industry Employee Enforcement Records, HHS/FDA. SORN 2: 09-10-0013, Employee Conduct Investigative Records, HHS/FDA.
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 Phone Email Online Government Sources Within the OPDIV Other HHS OPDIV State/Local/Tribal Foreign Other Federal Entities Non-Government Sources Members of the Public Commercial Data Broker Public Media/Internet 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.	Intella Connect Plus does not collect data from the public using and information collection request as defined by the Paperwork Reduction Act (PRA). It is an analysis platform where the data is obtained via court-orders. An OMB collection number is not required.
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	State or Local Agency/Agencies Within HHS
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	The disclosures are discretionary and made to the extent that providing such data may enhance the underlying criminal investigation managed by the investigative team and prosecutors.
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)).	OCI may share criminal investigative information with other federal agencies as part of joint criminal investigations and pursuant to agreements under disclosure-controlling regulation, e.g., 21 CFR 20.85 (Disclosure to other Federal government departments and agencies). Information may also be shared with state or local authorities pursuant to agreements established under 21 CFR 20.88 (Communications with State and local officials). These regulations require the parties to execute specific agreements concerning the permissible uses of the shared information and to implement specific privacy and security controls. There are no Computer Matching Agreements (CMA), Memoranda of Understanding (MOU), or Information Sharing Agreements (ISA).
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.	Disclosures to other federal, state or local agencies are documented through written requests under 20 CFR 20.85 and 21 CFR 20.88 and through written responses to those requests. This practice also satisfies the accounting of disclosure requirements under the Privacy Act, 5 U.S.C. § 552a(c).
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Mandatory
PIA 33A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	Authority is provided in the Federal Food, Drug, and Cosmetic Act (e.g., 21 U.S.C. 372), establishing authority to conduct examinations and investigations; 21 U.S.C. 331 listing prohibited acts and the crimes and criminal procedure provisions of Title 18 of the U.S. Code.

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.	Subjects under criminal investigation are not able to opt out of the collection of their PII. An opt-out capability would jeopardize a criminal investigation. PII is obtained through legal law enforcement authority via warrants and subpoenas. As is the nature of investigations, in many instances PII is collected from sources other than the subject individual. The subject of the investigation or the entity being investigated who refuse to provide their PII in response to a subpoena may be subject to civil or criminal penalties.
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.	No such changes are anticipated. Note that there is no notification and consent process regarding major changes affecting the investigative aspects of the system because information is obtained and used for federal criminal investigative purposes and notification could compromise ongoing investigations. Relevant SORNs and HHS and FDA regulations specify that the investigative records in this system are exempt from the individual notice and other requirements of the Privacy Act (See 5 U.S.C. 552a(e)(3)).
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.	For subjects of investigative records, individuals may resolve these concerns as part of the legal proceedings related to the relevant criminal investigation. FDA regulations provide a process by which these individuals may seek access to a record about themselves in certain circumstances (see 21 CFR 21.65). Individuals who are the subject of records under the Privacy Act may exercise the rights provided by law to resolve any concerns they may have. Individuals may also contact OCI, seek assistance through FDA's employee help center, or report the matter to FDA's information security or privacy offices. Contact information for all of these offices is available on the FDA's internet and/or intranet pages.
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 DARS Administrator controls access to the data. Users are provided access by account creation by the DARS Administrator. The DARS Administrator assigns permissions that are restricted based on the individual user's role. OCI agents are provided access only to the cases to which they are assigned and working. Permissions are granted where least privileges are enforced, and user access is granted on a case by case basis.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators 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: Investigating Agents and OCI support staff (users) require access to the data, which may contain PII, to review the various evidence collected concerning subjects who are suspected of being involved in criminal activity. Administrators: Administrators will have access to PII data in Intella Connect Plus: Administrators may be exposed to PII information during the process of providing restrictive access to data to the Investigating Agents. Contractors: Direct Contractors require access to the data, which may contain PII, to review the various evidence collected concerning subjects who are suspected of being involved in criminal activity. These contractors help to identify financial records and underlying assets used in the commission of criminal activity and assets that may be subject to criminal and civil forfeiture.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The DARS Administrator controls access to the data. Users are provided access by account creation by the DARS Administrator. The DARS Administrator assigns permissions that are restricted based on the individual user's role. OCI agents are provided access only to the cases to which they are assigned and working. Permissions are granted where least privileges are enforced, and user access is granted on a case-by-case basis.
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.	OCI uses both technical and administrative methods to control access to PII in the system. The DARS Administrator assigns permissions (administrative control). OCI Case Agents are provided access to documents for cases they are working on only (technical controls). Permissions are assigned to OCI Case Agents (Prosecuting Attorneys, other Law Enforcement Officials (LEO's)) based on their responsibility and need to know. OCI Case Agents only have access to such information as needed to perform their duties that are related to their specific cases. Permissions are granted where least privilege principles are enforced, and user access is granted on a case-by-case basis.
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/OCI personnel including Direct Contractors are required to complete FDA's annual IT Security and Privacy Awareness training.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	Intensive system-specific user training is provided for all new employees during a Special Agent Training Program that covers Privacy Act concerns and Computer Security Awareness training. The Privacy Office is available to provide additional training.

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).	Retention time of the PII is dependent on the length of time the criminal case remains open. This practice is consistent with FDA Records Schedule 8900, Reference Materials, National Archives and Records Administration (NARA) Citation N1-088-05-1, which indicates that materials are destroyed or deleted when no longer needed for reference purposes. The storage of this information is temporary, not to exceed 90 days from the end of the investigation and when all judicial actions have been completed.
PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative controls include that the DARS System Administrator controls logical access to the data such that users are provided access only to the cases to which they are assigned. Permissions are granted and enforced under a “least privilege” principle at the individual level. The technical controls protecting PII include firewall use, current server Operating System, virtual private networks, and multi-factor authentication for network and system access. Physical controls applied include a keypad activated alarm system, layers of physical cage enclosures with key locks, motion detectors and video surveillance with barriers requiring PIV card authentication to gain physical access.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	5/23/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	0

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	5/23/2025
SOP Review Comments:	The FDA's Senior Official for Privacy (SOP) has: (a) approved the Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) conducted for the subject system/component; (b) reviewed and approved the associated security categorization; and (c) reviewed and confirmed acceptable implementation status of the assigned privacy controls.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	6/5/2025
Agency Privacy Analyst Review Comments:	Reviewer: Crystal Bland 6/5/2025 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	13

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	6/24/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	19

SAOP Signature

Date	User	Type	Name	Original Value	New Value
6/24/2025 2:58 PM	GUENTHER, BRIDGET	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
PIA 22	BLAND, CRYSTAL	5/28/2025	5/28/2025 On the next iteration of the PTA make sure that the PII elements listed in PIA-22 are also listed in PTA-5.	
PTA 01	BLAND, CRYSTAL	6/5/2025	6/5/2025 Per FDA's email, this system has an ATO. Yes, the system has an ATO. The ATO Date is 5/18/2023.	6-5-2025 EMAIL_RE_ FDA - Intella Connect - QTR2 - 2025 - FDA4929942.pdf