Drug Enforcement Administration

Privacy Impact Assessment
for the
DEA Data Lake 2.0

Issued by:
Robert McGovern
Senior Component Official for Privacy (Acting)
Drug Enforcement Administration

Approved by: Kameron Cox
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: November 10, 2026

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The DEA Data Lake 2.0 (DL 2.0) is a cloud-based infrastructure that serves as a centralized platform to produce analysis and insight into DEA datasets. DL 2.0 conducts overarching data analysis and can automate manual tasks utilizing data from existing DEA information systems. The architecture is configured into multiple data storage and processing components designed to support analytics-focused workloads and requires internal pipelines to move data between the lake and application data stores.

DL 2.0 provides an environment that both technical and non-technical users can employ to gain insight into DEA data, develop machine learning (ML) models, and generate business intelligence (BI) reports. DL environment updates, including the addition or removal of services utilized within the DL, will be approved via the formal System Change Request (SCR) process.

The primary data store application software supports a majority of the application and analytics workloads using cloud-based storage technologies, while Structured Query Language (SQL) and semi-structured JavaScript Object Notation (JSON) data will also exist within the platform.

The AWS Government Cloud (GovCloud) platform enables DEA agents, analysts, and data scientists to import, collect, and analyze real-time data from multiple internal DEA data sources. The DL 2.0 platform functions as a centralized repository for storing structured and unstructured data at scale, enabling storage, transformation, and analysis without requiring rigid data structures.

DL 2.0 consolidates data from DEA investigative systems and internal datasets, including case file data from the Investigative Management Program and Case Tracking (IMPACT) system and datasets from the Narcotics and Dangerous Drugs Information System (NADDIS).[1] The platform supports law enforcement operations by improving access to investigative data and enabling automated analytical processes.

DL 2.0 utilizes non-generative machine learning models to assist analysts in identifying patterns, correlations, and relationships within existing investigative datasets. These models are limited to analytical functions, do not generate new content or data, and do not operate autonomously. They are not used to make investigative or enforcement decisions. Outputs generated by these models are treated as analytical leads and are subject to review and validation by trained DEA personnel before any operational use.

During the initial privacy assessment, DEA determined that personally identifiable information (PII) will be processed and stored when DL 2.0 is operational and accredited. This Privacy Impact

[1] The DEA IMPACT PIA being updated and will cover NADDIS as a subsystem. It will be found at https://www.dea.gov/foia/privacy-impact-assessment

Assessment evaluates the privacy risks associated with the system and documents the safeguards implemented to mitigate those risks.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, the type of technology used (e.g., databases, video conferencing, Super Intelligence (SI), machine learning, privacy enhancing technologies),why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

DL 2.0 is used by DEA personnel to conduct investigative data analysis across multiple existing DEA systems. The platform provides centralized analytical capabilities that allow authorized users to identify patterns, correlations, and relationships within investigative information that may not be readily observable through manual analysis alone.

DL 2.0 supports several analytical capabilities, including data ingestion and storage, investigative data analysis, non-generative machine learning model development, business intelligence reporting, and data visualization and pattern detection. The platform operates as a near real-time data environment that enables agents, analysts, and data scientists to access and analyze information in support of ongoing investigations and research activities. DL 2.0 integrates data from existing DEA information systems and applies analytical techniques to enhance visibility into investigative data. The platform may generate link analysis, trend analysis, and data correlation reports to assist analysts in identifying relationships, patterns, and connections across investigative datasets. These outputs provide a consolidated view of relevant information from multiple DEA systems to support analytical review and investigative activities.

DL 2.0 employs a type of artificial intelligence, hereafter referred to as Super Intelligence (SI), through non-generative machine learning models that analyze existing data to identify statistical patterns, relationships, and anomalies. These models do not create new content, do not operate autonomously, and do not make investigative or enforcement decisions. The use of non-generative machine learning enhances analytical capabilities by improving the ability to detect trends, link related entities, and prioritize investigative leads across large datasets.

The outputs generated through these analytical processes provide users with improved situational awareness, more efficient identification of relevant information, and enhanced ability to support investigative decision-making. All results produced by machine learning models are treated as analytical leads and are reviewed and validated by trained DEA personnel prior to any operational use.

DL 2.0 may process investigative records derived from court-authorized electronic surveillance. Such information is not collected directly by DL 2.0 and does not include live interception or raw wiretap feeds. Instead, Title III-derived information exists in DL 2.0 only to the extent that it has already been documented within authorized DEA investigative records. In practice, this typically includes summarized communications, pertinent excerpts, or limited direct quotations contained in DEA-6 reports or similar investigative documentation, along with associated metadata such as dates, times, or

identifiers. Full verbatim transcripts or complete collections of intercepted communications are not ingested into DL 2.0 as a standalone dataset. DL 2.0 supports analytical processing of this previously collected information to identify patterns, relationships, and investigative leads, but does not expand the scope of surveillance or determine legal relevance. All Title III-derived information remains subject to applicable legal requirements, including minimization procedures, access restrictions, and handling controls, and is accessible only to authorized personnel with a validated need to know. Current DL 2.0 datasets include:

- **DEA-6s** (Reports of Investigation documenting DEA investigative efforts and results)
- **DEA-7s** (Reports of Drug Property Collected, Purchased, or Seized)
- **DEA-7As** (Acquisition of Non-Drug Property Seizure reports)
- **DEA-202** (Personal History Report arrest submissions filled out DEA Special Agents about arrestees).
- **Narcotics and Dangerous Drugs Information System** (NADDIS) (an automated indexing system that contains investigative case file information from DEA's case management system, IMPACT, and arrest data from DEA's Defendant Statistical System (DSS)[2]
- **National Seizure System (NSS)** (a repository of information on the interdiction, investigation, and/or seizures of clandestine laboratories, contraband (chemicals/precursors, currency, drugs, equipment, and weapons), locations of seizures, persons linked to seizures, and transportation used (aircraft, vehicles, and vessels).[3]
- **National Forensic Laboratory Information System (NFLIS) data** (a collection of results from drug chemistry analyses conducted by federal, state, and local forensic laboratories across the country).[4]

Data ingestion into DL 2.0 is governed by a formal review and approval process to ensure that only data relevant to DEA's authorized law enforcement mission is incorporated into the platform. Candidate datasets are identified by DEA program offices and subject matter experts based on operational need and are evaluated through a structured governance process that includes technical, legal, privacy, and security review. This evaluation considers the purpose of the data, applicable legal authorities, data minimization requirements, and any restrictions associated with the originating system. Oversight is provided by program management, information system security personnel, and privacy officials, who review and approve dataset onboarding to ensure compliance with Department of Justice and DEA policies.

---

[2] The privacy documentation discussing DEA-6s, DEA-7s, DEA-7As, DEA-202s and NADDIS can be found in the IMPACT PIA currently being updated. It will be found at https://www.dea.gov/foia/privacy-impact-assessment.

[3] The NSS is part of the El Paso Intelligence Center (EPIC) Inquiry System and information specific to that subsystem can be found in the EPIC Inquiry System PIA. https://www.dea.gov/sites/default/files/2025-07/DEA%20PIA%20for%20EPIC%20Inquiry%20System.pdf.

[4] NFLIS is part of the Registrant Support Network (RSN) and information specific to that subsystem can be found in the RSN PIA. https://www.dea.gov/sites/default/files/2025-02/508_DEA_PIA_23-1814_RSN%20-%20FINAL.pdf.

Prior to ingestion, access controls are defined and implemented using role-based and attribute-based mechanisms, including metadata tagging to align user permissions with the originating system and sensitivity of the data. Any changes to existing datasets, including modifications to data elements, structure, or access permissions, are subject to formal change management processes in accordance with established DEA policy. These processes ensure that updates are reviewed, approved, and documented before implementation. Additionally, all ingested data remains subject to audit logging, periodic access reviews, and continuous monitoring to ensure that access and use remain appropriate and consistent with authorized purposes.

PII categories will include the pertinent facts from investigative cases and will include names, phone numbers, social security numbers, among other items. The platform offers data exploration, reporting, analytics, machine learning, and data visualization, enabling users to gain an accurate understanding of relevant details related to any case, investigation, or operation. The interacting services of DL 2.0 are:

- **Cloud Object Storage Services.** Object storage services provide scalability, data availability, and security. Furthermore, data management features are tailored to optimize costs, manage data lifecycle, and meet regulatory requirements.

- **Cluster Management Services.** Customizable cluster management services with full control over instance configurations will be utilized. Data scientists and engineers will have the ability to utilize cluster management services to merge data from multiple sources into a data warehouse for large datasets.

- **Data Integration Services.** Data Integration Services will be utilized to assist analytics users in the discovery, preparation and integration of data from multiple sources. It supports all workloads and scales on demand.

- **Data Query Services.** A federated query solution, will allow all of the above technologies to query unstructured, semi-structured, and structured stores in the lake using the a database query interface.

DL 2.0 is the data storage component that allows DEA special agents, analysts, and data scientists to import any amount of data in real-time. The DL 2.0 primary data store now uses relational database services for a majority of the application and analytics workloads, but SQL and semi-structured JSON data will exist.

- **Lake Formation.** Lake Formation is a service that simplifies and automates the process of creating data lakes. It provides its own permissions model that augments the Identity and Access Management (IAM) permissions model, enabling fine-grained access to data stored in data lakes through a grant or revoke mechanism. These permissions are enforced using granular controls at the column, row, and cell levels across analytics and machine learning services.

- **Data Lake Storage** is repository for storing, processing, and maintaining diverse data sources.

- **Data Factory Services** manage, integrate and transform large data sets on demand.

Further, DL 2.0 will build a universal platform for data analytics incorporating additional tools:

- **Relational Database Services.** Relational Database Services provides the ability to create a new database in minutes and offers database customization flexibility. Relational Database Services facilitates the deployment and maintenance of relational databases in the cloud. It can be used to set up, operate, manage and scale a relational instance of a cloud database.

- **Data Streams.** Database as a service and data processing applications will be utilized to read data records and sends processed records to dashboards, which are approved services within the AWS GovCloud infrastructure and be used to send processed records to dashboards, generate alerts, dynamically, or send data to other services.

- **PowerBI.** Business Analytic Services in the cloud provides the level of analytical capabilities needed to provide a 'dig deeper' into the data.

- **Machine Learning (ML).** ML services connect the data lake to the external data stores. It supports data exploration, experimentation, "Extract, Transform, and Load" (ETL), ML development, and model deployment. ML services are essential for data lake ingest, data-driven applications and Business Intelligence. Machine learning models within DL 2.0 assist analysts in identifying correlations and patterns across investigative datasets. These models support analytical review and do not independently determine investigative outcomes. DL 2.0 does not use machine learning models to make automated investigative or enforcement decisions. Analytical outputs generated by machine learning models are reviewed by trained DEA personnel before being used in operational or investigative activities.

The DL 2.0 platform maintains approximately five years of investigative data originating from DEA source systems. Data within the platform is refreshed daily, and automated processes remove records exceeding the five-year retention window to ensure that the platform maintains only the most recent five years of data.

During the initial privacy assessment, DEA determined that Personally Identifiable Information will be processed and stored when DL 2.0 is operational and accredited.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	28 United States Code (U.S.C.) § 534 (Acquisition, preservation, and exchange of identification records and information.) 21 U.S.C. § 801 *et seq*, (Controlled Substance Act)

	44 U.S.C. § 3101 (Records management by agency heads, general duties)
Executive Order	
Federal regulation	28 C.F.R. §§ 0.100 and 0.101.
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

DL 2.0 does not conduct interception of communications. Instead, the system may store investigative records derived from court-authorized electronic surveillance conducted pursuant to Title III after those records have been entered into authorized DEA investigative systems.

DL 2.0 does not modify or overwrite investigative records maintained in the originating DEA systems and is used solely to support analytical processing of data derived from those systems.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, *and* D	Names of members of the public (US or non-USPER) involved in investigations and of DEA or other Federal Government personnel associated with investigation may be present.
Date of birth or age	X	C *and* D	Date of birth or age of members of the public (US or non-USPER) involved in investigations may be present.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Place of birth	X	C *and* D	Place of birth, of members of the public (US or non-USPER) involved in investigations may be present.
Gender	X	C *and* D	Gender of members of the public (US or non-USPER) involved in investigations may be present.
Race, ethnicity, or citizenship	X	C *and* D	Race, ethnicity, or citizenship information of members of the public (US or non-USPER) involved in investigations may be present.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C *and* D	Social Security number of members of the public (US or non-USPER) involved in investigations may be present.
Tax Identification Number (TIN)	X	C *and* D	Tax ID numbers of members of the public (US or non-USPER) involved in investigations may be present.
Driver's license	X	C *and* D	Government assigned Identifiers (driver's licenses), of members of the public (US or non-USPER) involved in investigations may be present.
Alien registration number	X	C *and* D	Alien registration numbers of members of the public (US or non-USPER) involved in investigations may be present.
Passport number	X	C *and* D	Passport numbers of members of the public (US or non-USPER) involved in investigations may be present.
Mother's maiden name	X	C *and* D	Mother's maiden name of members of the public (US or non-USPER) involved in investigations may be present.
Vehicle identifiers	X	C *and* D	Vehicle identifiers of members of the public (US or non-USPER) involved in investigations may be present.
Personal mailing address	X	C *and* D	Personal addresses of members of the public (US or non-USPER) involved in investigations may be present.
Personal e-mail address	X	C *and* D	Personal email addresses of members of the public (US or USPER) involved in investigations may be present.
Personal phone number	X	C *and* D	Personal phone numbers of members of the public (US or non-USPER) involved in investigations may be present.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Medical records number	X	C *and* D	Information including medical record numbers of members of the public (US or non-USPER) involved in investigations may be present.
Medical notes or other medical or health information	X	C *and* D	Information including health information of members of the public (US or non-USPER) involved in investigations may be present.
Financial account information	X	C *and* D	Financial account information of members of the public (US or non-USPER) involved in investigations may be present.
Applicant information			
Education records			
Military status or other information	X	C *and* D	Military status or other military information of members of the public (US or non-USPER) involved in investigations may be present.
Employment status, history, or similar information	X	C *and* D	Employment-related information of members of the public (US or non-USPER) involved in investigations may be present.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C *and* D	Employment performance information of members of the public (US or non-USPER) involved in investigations may be present incidentally.
Certificates			
Legal documents	X	C *and* D	Legal document information of members of the public (US or non-USPER) involved in investigations may be present.
Device identifiers, e.g., mobile devices	X	C *and* D	Electronic device identifiers (IP address IMEI and MAC Address), information of members of the public (US or non-USPER) involved in investigations may be present.
Web uniform resource locator(s)	X	C *and* D	Web Uniform resource locator information of members of the public (US or non-USPER) involved in investigations may be present.
Foreign activities	X	A, B, C *and* D	Some Hosted Systems contain information of foreign activities of DEA and other federal GOV personnel and/or of members of the public (USPER & non-USPER). (See relevant PIAs where applicable)

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C *and* D	Criminal records information of members of the public (US or non-USPER) involved in investigations may be present.
Juvenile criminal records information	X	C *and* D	
Civil law enforcement information, e.g., allegations of civil law violations	X	C *and* D	Civil law enforcement information of members of the public (US or non-USPER) involved in investigations may be present.
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information	X	C *and* D	Information related to or compiled for Grand Juries related to members of the public (US or non-USPER) involved in investigations may be present.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C *and* D	Criminal witness-related information of members of the public (US or non-USPER) involved in investigations may be present.
Procurement/contracting records			
Proprietary or business information	X	A, B, C, and D	Business-related addresses, emails, and phone numbers related to members of the public (US or non-USPER) involved in investigations as well as of associated DEA and/or other Federal personnel may be present.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	Location information of members of the public (US or non-USPER) involved in investigations as well as of associated DEA and other Federal personnel may be present.
Biometric data:			
- **Photographs or photographic identifiers**	X	C *and* D	Photos, or photographic identifiers of members of the public (US or non-USPER) involved in investigations may be present.
- **Video containing biometric data**	X	C *and* D	Videos and/or biometrics of members of the public (US or non-USPER) involved in investigations may be present.
- **Fingerprints**	X	C *and* D	Fingerprints of members of the public (US or non-USPER) involved in investigations may be present.
- **Palm prints**	X	C *and* D	Palm prints of members of the public (US or non-USPER) involved in investigations may be present.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Iris image**	X	C *and* D	Iris images of members of the public (US or non-USPER) involved in investigation may be present.
- **Dental profile**	X	C *and* D	Dental records/profiles of members of the public (US or non-USPER) involved in investigations may be present.
- **Voice recording/signatures**	X	C *and* D	Voice recordings of members of the public (US or non-USPER) involved in investigations may be present.
- **Scars, marks, tattoos**	X	C *and* D	Images or records describing identifiable scars, marks and tattoos of members of the public (US or non-USPER) involved in investigations may be present.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	C *and* D	Palm or finger vein biometrics of members of the public (US or non-USPER) involved in investigations may be present.
- **DNA profiles**	X	C *and* D	DNA profiles and other DNA information of members of the public (US or non-USPER) involved in investigations may be present.
- **Other (specify)**	X	C *and* D	Any identifying particulars of members of the public (US or non-USPER) involved in investigations may be present.
System admin/audit data:			
- **User ID**	X	A *and* B	User ID of DEA employees, contractors, detailees and other Federal personnel users of the system. are maintained.
- **User passwords/codes**	X	A *and* B	Passwords of DEA employees, contractors, detailees and other Federal personnel users of the system are maintained.
- **IP address**	X	A *and* B	IP Address of DEA employees, contractors, detailees and other Federal personnel users of the system are maintained.
- **Date/time of access**	X	A *and* B	Time of system access of DEA employees, contractors, detailees and other Federal personnel users of the system are maintained.
- **Queries run**	X	A *and* B	Query information of DEA employees, contractors, detailees and other Federal personnel users of the system are maintained.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Contents of files**	X	A *and* B	Content information of the files accessed/searches run by DEA employees, contractors, detailees and other Federal personnel users of the system are maintained.
Other (please list the type of info and describe as completely as possible):	X	C *and* D	Potential for the following information of members of the public (US and non-USPERs) to be present: Usernames/ID, passwords, IP addresses, date/time of access and queries run; data on obtained from commercial data brokers; communications metadata that may be present in IMPACT; other personally identifying information not listed here; and acquisition of commercially acquired data.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X				
Other (specify): includes DHS, Treasury (FINCEN), and DOD					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	
Commercial data brokers	X				
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Information maintained within DL 2.0 may be shared with authorized DEA personnel and, when appropriate, with federal, state, local, tribal, and international law enforcement agencies in support of legitimate law enforcement purposes.

Information sharing occurs in accordance with established agreements, policies, and legal authorities governing the sharing of law enforcement information. Data shared through DL 2.0 is limited to information necessary to support authorized investigative activities and is consistent with the purposes for which the information was originally collected.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	X	X	Data from DL 2.0 should be available to authorized Special Agents, Intelligence Analysts, and Task Force Officers with a need to know in the course of job duties
DOJ Components	X			Other DOJ components do not have direct access to DL 2.0. However, if evidence obtained in a case is relevant to a different investigation or prosecutions by DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the disclosure provision of Title III, if applicable, 28 C.F.R. § 0.103, and SORN Justice/DEA-008, routine use "a" or with prosecutors in US Attorney offices.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal Entities		X		These entities do not have direct access to DL 2.0. However, if evidence obtained in a case is relevant to a different investigation by non-DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the disclosure provision of Title III, if applicable, 28 C.F.R. § 0.103, and SORN Justice/DEA-008, routine use "a". Generally, data is shared with other Federal entities through bulk transfers in accordance with established Memoranda of Understanding (MOUs).
State, local, tribal gov't entities	X			These entities do not have direct access to DL 2.0. However, if evidence obtained in a case is relevant to a different investigation by non-DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the disclosure provision of Title III, if applicable, 28 C.F.R. § 0.103, and SORN Justice/DEA-008, routine use "a" or as allowed in the disclosure provision in the Court Order, the agreement or MOU with the party that granted access or provided the information.
Public				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			These entities do not have direct access to DL 2.0. However, if evidence obtained in a case is relevant to a different investigation by non-DOJ entities, that evidence may be shared with investigators working on the second investigation, consistent with the disclosure provision of Title III, if applicable, 28 C.F.R. § 0.103, and SORN Justice/DEA-008, routine use "a" or as allowed in the disclosure provision in the Court Order, the agreement or MOU with the party that granted access or provided the information.
Private sector				
Foreign governments	X			Certain data in or accessed through DL 2.0 may be shared with foreign law enforcement partners with agreements but they do not have direct access to the system.
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

DL 2.0 does not release application information to the public for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act §

552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

DL 2.0 processes information originating from DEA investigative systems that collect and maintain information pursuant to applicable statutory authorities. Notice regarding the collection and use of information is provided through the applicable System of Records Notices associated with the source systems.

Generally, no specific notice is provided as the information gathered is used to properly identify suspects. Additional general notice of the existence, contents, and uses the information in the constituent databases of DL 2.0 and any sub systems will be provided by the publication of this PIA and the SORN for the underlying data delivered by the DL 2.0 system as published in the Federal Register. The applicable SORN is JUSTICE/DEA-008, "Investigative Reporting and Filing System" 77 Fed. Reg. 21808 (April 11, 2012).

Any notice of collection, if not otherwise exempted, is covered by the privacy documentation for those source systems. When law enforcement agents and officers interact with individuals in connection with an investigation, the individuals are generally aware that their information will be recorded and stored. However, because this system is used for a law enforcement purpose and contains sensitive information related to criminal and civil investigations, it is not feasible or advisable to provide notice to individuals at the time their information is accessed by the system.

To the extent applicable to some information in DL 2.0, 18 U.S.C. § 2518 requires after-the-fact notification of interception to parties that law enforcement can identify and notify. DEA keeps track of the details of any parties whose communications are intercepted for subsequent notification and housed in the relevant investigatory files from which data in DL 2.0 was uploaded. Any after-the-fact notification will be provided through process defined by the applicable source dataset owner. Also, no notice is required to be provided by the government to a subscriber when a search warrant is issued upon a service provider to obtain the contents of the subscriber's stored communications, in accordance with 18 U.S.C. § 2703.

Similarly, in the conduct of executing a Federal Rule of Criminal Procedure, Rule 41 search warrant, although notice usually is required to be provided to the owner of the property being searched, delay of notice may be sought where there is reason to believe notification will result in adverse results. See 18 U.S.C. § 3103a. No notification beforehand can be accommodated due to the risk of compromising ongoing investigations. However, if formally charged, the parties whose data was collected as evidence have the right to challenge the accuracy of the collected information in their defense, as well as the manner and means by which the information was collected.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

DL 2.0 collects no information from individuals directly and its component databases and sub-systems also generally do not collect information directly from individuals without their consent, with some exceptions. Some information is collected from private sector service providers through legal processes such as warrants or administrative subpoenas, communications with sources and cooperating witnesses or from direct surveillance in public locations. The systems with information in DL 2.0 that

receive or otherwise collect much of that information, except for the cases of cooperating witnesses and confidential sources, generally provide no notice. Because of the DEA law enforcement or intelligence purposes for which the information is collected, opportunities to refuse consent are limited or nonexistent. For example, parties whose communications are intercepted pursuant to a court order and do not have an opportunity to voluntarily participate in or choose to decline the collection, use, or dissemination of information. No notification beforehand can be accommodated due to the risk of compromising ongoing investigations.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals seeking access to records maintained by DEA may submit requests through the procedures established under the Privacy Act and the Freedom of Information Act. Requests for access, amendment, or correction of records are handled in accordance with DOJ and DEA policies governing Privacy Act requests.

DL 2.0 itself is only available to authorized users. A Freedom of Information Act (FOIA) or Privacy Act access request can be made through the DEA FOIA office for data contained therein; however, most information in DL 2.0 is not available. This is because DL 2.0 data is related to official case files and pursuant to 28 C.F.R. §16.92, the Attorney General has made information within the DEA's Investigative Reporting and Filing System (and other listed systems) exempt from the access/disclosure and amendment elements of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). In addition, DL 2.0 information are also records complied for law enforcement purposes and thus also generally excluded from production under the Freedom of Information Act (FOIA) 5 U.S.C. §552(b)(7).

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** This system was authorized to be piloted ATP on 10/27/2023 and expires 9/30/2024. An ATP extension will be requested prior to expiration. **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATO signed 11/25/2024

	Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: DL 2.0 Privacy POA&M is pending based on OPCL signature and approval of the IPA and this PIA. Once this is received the POA&M will be closed.
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** DL 2.0 is assigned the security category of Moderate as defined in FIPS 199 based on the information types: Personal Identity and Authentication, Crime Prevention, Criminal Apprehension, Criminal Investigation and Surveillance, Substance Control, Legal Investigation, and Legal Prosecution and Litigation. DL 2.0 uses a Cloud console, Firebird Active Federated Services (ADFS), DOJ Public Key Infrastructure (PKI) for PIV Card, and Multi-Factor Authentication (MFA) to implement authentication mechanisms that meet FIPS 140-2 compliance requirements. These components implement cryptographic modules that comply with FIPS 140-2 approved encryption algorithms, including AES128 and higher, RSA2048 and higher, SHA256 and higher, and SHA2. DLZ Information Systems' cryptographic modules include On-Prem User Firebird Authentication (ADFS/PKI), Okta MFA Authentication (HTTPS/TLS), PIV Card Authentication, Privileged user Secure Shell Authentication, Privileged user Remote Desktop Protocols (RDP/FB AD), Cloud console Web-based Authentication, AWS Account Authentication, data storage protections, and VPN IPEC Encryption.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. CISO/CIO updates are a continuous monitoring objective following the full implementation and authorization of DL 2.0. Any changes to system risk that may impact DEA data via the operational environment is communicated to the CISO/CIO and Privacy.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with DEA Incident

	Response Plan. DEA TCVV monitors on-prem assets using the Splunk event correlation tool to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Remedy ticketing system.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. As a standard operating procedure, all contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually**. **Indicate whether there is additional training specific to this system, and if so, please describe:** Required training is distributed and tracked via the DOJ Learning Management System DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and Cyber Security awareness training that are applicable to all DEA component personnel. However, the Office of Chief Counsel (OCC) is working on a role-based annual privacy training which will be published soon.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Physical Safeguards:

The DL 2.0 servers reside in a private Government Cloud virtual server system ecosystem under a Federal Risk and Authorization Management Program (FedRAMP) Moderate authorization. However, hybrid server or fully on-premises environment(s), may exist and be used for data feeds in which interconnection MOUs are in place. Any physical server for databases providing data to DL 2.0 are stored within Federal/DEA buildings in a secure room with controlled access or using appropriate GSA-approved security systems. Any physical records, as well as access points located in federal buildings with restricted access and physical security systems. DEA uses Security in Depth relying on multiple layers of physical and electronic protection of the system and the data contained within the system. Physical intrusions by unauthorized individuals into DEA facilities are prevented by perimeter security protections such as armed guards and video surveillance (where applicable), and physical access is only possible through controlled entry to all DEA occupied buildings and facilities with Personal Identification Validation (PIV) card readers for all entries.

Technical Protections

DL 2.0 operates within the Amazon Web Services (AWS) GovCloud environment, which maintains a FedRAMP authorization and complies with Department of Justice cloud security policies and Federal Information Security Modernization Act (FISMA) requirements.

Information stored within DL 2.0 is protected through multiple layers of security controls including:

- Encryption of data at rest and in transit using FIPS-140-2 compliant encryption
- Role-based access control mechanisms
- Multi-factor authentication using Personal Identity Verification (PIV) credentials
- Continuous monitoring and logging of system activity
- Physical and logical access controls

Protection of information system resources is provided by management, operational, and technical security and privacy controls. Access to all records is controlled and limited to approved personnel with an official need for access to perform their duties. Access to datasets is granted and approved by the data owner and tracked through the ServiceNow ticketing system. The use of individual passwords or user identification codes is required to access information system resources. The system is housed within an alarmed controlled access room within another outer perimeter area that is also alarmed and controlled access providing multiple layers of physical protection.

Security measures are in place to safeguard information including IT monitoring tools; firewalls at the system boundaries; intrusion detection at the systems edge, data loss prevention mechanisms; and audit logs to provide system security. Access to DL 2.0 is granted only after authorized personnel have signed required memo stating the proper permissions to users.

All data stored in or made accessible to DL 2.0 is encrypted per the recommendation from National Institute of Standards and Technology under Special Publication 800-111. The system meets the Federal Information Processing Standard (FIPS) Publication 140-2 requirements to safeguard all the information the system collects, including encryption of data in transit, encryption at rest, and password protection of IT systems compliant to DOJ guidelines.

Administrative Security and Privacy Controls:

Access to Data Lake 2.0 is limited to authorized users who are DEA Special Agents, Task Force Officers, Analysts, and Data Scientists. A user's access will be limited and approved based on their role and the specific datasets for which they were granted. Access to the Data Lake environment is via multi-factor authentication. Role based access controls, security groups and detailed logging are implemented within Data Lakes to further restrict access to datasets where an individual has a verified need to know, and to track user/system interactions.

Only authorized individuals are given access to DEA's information, and each user is required to review and acknowledge the DEA IT Rules of Behavior as part of the online IT Security Training. This reduces the risk of unauthorized use or disclosure of DEA's pertinent information. The limited distribution of the information from the applications, continuous monitoring of access to the applications, and the observance of the IT Rules of Behavior limit privacy risks.

DEA also has implemented an audit regimen for DL 2.0, conducting multiple scans and enforcing access control limitations. Users are informed of proper system usage, and DEA personnel and contractors are cleared to work on the system. Users must read and agree to the annual review of the Rules of Behavior. The system collects audit log files, which are reviewed daily by a security analyst and sent to an automated system for continuous review. DL 2.0 uses automated security threat detection services to monitor user behavior and report unauthorized activity. With Identity and Access Management integration, administrators can restrict or disable user accounts posing security or privacy risks upon receiving alerts.

User access to DL 2.0 is reviewed periodically in accordance with Department of Justice and DEA access control policies to ensure that permissions remain appropriate for each user's assigned role and responsibilities. These reviews verify that access is limited to individuals with a valid need to know and that user privileges align with current job functions. Accounts for users who no longer require access, including those who have changed roles or separated from the agency, are promptly modified or removed. Periodic audits and supervisory reviews support compliance with access control requirements, reinforce the principle of least privilege, and help ensure the continued protection of sensitive investigative information.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.) If the project involves Super Intelligence (SI) and/or machine learning, indicate if the information is used for training SI models, and if so, how this will impact data retention and disposition.

The disposition standards for the federal records in DL 2.0 application are implemented in accordance with the National Archives and Records Administration (NARA) approved retention schedule, 1303 Agency Records Center Case Files, Temporary, N01-0064-1987-0001 Item 1303, "Cut off when records center is no longer in operation. Place case file in inactive file. Destroy when 3 years old." (N1-64-87-1). When information from DL 2.0 is placed in a case file, the retention period of the data is governed by the applicable DEA approved retention policy. When documents are placed in and inactive file, they will share the same retention period as initial source records. DL 2.0 data is refreshed at daily intervals and will synchronize from the source.

DL 2.0 maintains approximately five years of investigative data. Automated lifecycle management processes refresh the dataset daily and remove records exceeding the five-year retention window to ensure that the system retains only relevant investigative information.

The five-year retention window supports DEA analytical and investigative activities by enabling analysts to identify patterns and relationships across recent investigative activity while limiting long-term retention of sensitive information.

DL 2.0 supports ad-hock record expunged and is designed to expunge applicable records within 24 hours.

A different schedule applies to the records regarding the management of the DL 2.0 IT system development project through its various stages: concept development, requirements gathering, procurement, implementation, system testing, "go-live," and hand-off to production. These case files, maintained by system, may include copies of approved product plan and approvals authorizing the project; project plans and other planning documents; copies of procurement documents kept for reference during the project and contract management records (official copies are maintained by the Contracting Officer in Acquisitions); communications with contractors; deliverables as specified by project; change control records; and closeout records. Temporary N01-0064-2008-0012 Item 5 "Destroy/delete 5 years after system is retired." (N1-64-08-12, item 5).

DL 2.0 utilizes non-generative machine learning models that are trained using data derived from existing DEA investigative systems that have been lawfully collected and are already authorized for analytical use. DL 2.0 does not ingest, maintain, or rely on separate, standalone training datasets distinct from the operational data environment. Instead, model development and training activities are conducted within controlled analytical environments using subsets of existing data that are subject to the same access controls, governance processes, and legal restrictions as the originating systems.

No external, publicly available, or commercially sourced datasets are used for training purposes, and no generative or Super Intelligence models are employed. Training data is not persistently retained as a separate dataset; rather, it remains part of the governed data environment and is subject to the same lifecycle management controls as operational data. This includes the application of the DL 2.0 five-year retention window, daily data refresh processes, and automated purge mechanisms that remove records exceeding the retention threshold.

All training activities are limited to authorized personnel and are conducted for analytical support purposes only. The use of data for training does not alter the classification, ownership, or retention requirements of the underlying records, and all data remains subject to applicable approved retention schedules and DEA policies governing investigative information.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ___X__ Yes.

DL 2.0 functions solely as an analytical environment that processes information derived from existing DEA systems of record and does not independently collect information directly from individuals.

Authorized contractors supporting DEA information technology operations may be granted access to DL 2.0 when necessary to perform official duties. Contractor personnel are subject to the same access control, training, and confidentiality requirements as DEA personnel.

Users of DL 2.0 must complete Department of Justice privacy and information security training prior to receiving system access. Access is granted only after approval through DEA access control procedures and is limited to personnel with authorized investigative, analytical, or administrative roles.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

JUSTICE/DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May, 25, 2017) (amendment), https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf

JUSTICE/DEA-003, *Automated Records and Consolidated Orders System-Diversion Analysis and Detection System (ARCOS-DADS)*, 69 Fed. Reg. 51104 (Aug, 17, 2004)(full text); 82 Fed. Reg. 24147 (May, 25, 2017) (amendment) https://www.govinfo.gov/content/pkg/FR-2004-08-17/pdf/04-18827.pdf

and to the extent applicable:

JUSTICE/DEA-005, *Controlled Substances Act Registration Records (CSA)*, 52 Fed. Reg. 47182, 208 (Dec. 11, 1987) (full text); 66 Fed. Reg. 8425 (Jan. 31 2001), 82 Fed. Reg. 24147 (May, 25, 2017) (amendments), https://www.justice.gov/opcl/docs/52fr47182.pdf

JUSTICE/DEA-011, Operations Files, 52 Fed. Reg. 47182, 214 (Dec. 11, 1987)(full text), 66 Fed. Reg. 8425 (Jan. 31 2001), 82 Fed. Reg. 24147 (May, 25, 2017) (amendments), https://www.justice.gov/opcl/docs/52fr47182.pdf.

JUSTICE/DEA-017, *Grants of Confidentiality Files (GCF)*, 52 Fed. Reg. 47182, 218 (Dec. 11, 1987) (full text); 66 Fed. Reg. 8425 (Jan. 31 2001), 82 Fed. Reg. 24147 (May, 25, 2017)(amendments), https://www.justice.gov/opcl/docs/52fr47182.pdf.

JUSTICE/DEA-020, *Essential Chemical Reporting System*, 52 Fed. Reg. 47182, 219 (Dec. 11, 1987) (full text); 66 Fed. Reg. 8425 (Jan. 31 2001), 82 Fed. Reg. 24147 (May, 25, 2017) (amendments), https://www.justice.gov/opcl/docs/52fr47182.pdf.

JUSTICE/DEA-022, *El Paso Intelligence Center (EPIC) Seizure System (ESS)*, 71 Fed. Reg. 36362 (Jun. 26, 2006)(full text); 82 Fed. Reg. 24147 (May, 25, 2017)(amendment), https://www.govinfo.gov/content/pkg/FR-2006-06-26/pdf/E6-9977.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated? For projects involving the use of Super Intelligence and/or Machine Learning, identify the privacy risks uniquely associated with the use of SI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

a. Potential Threats Related to the Collection of the Information

Privacy Risk: Over-collecting and maintaining more personal information than necessary to accomplish DEA's official duties and its mission.

Mitigation: This risk is mitigated. The original rationale to collect the amount of information present in the other datasets accessible to DL 2.0 is not part of the purview of DL 2.0 process. The scope of the information DL 2.0 gathers is determined by users' requests and this information is secure, maintained and collected by DEA authorized employees using the information necessary to conduct their investigations and effectuate DEA's mission. However, the determination to enter the information into the systems accessible by DL 2.0 are largely made by trained law enforcement personnel who collect and document only that information about an individual that is relevant and necessary to accomplish DEA's mission of enforcing the national controlled substances laws.

Additionally, DL 2.0 is meticulously designed to manage, protect, and ensure the proper handling of sensitive information. In the context of preliminary investigation files that do not progress to full criminal or civil investigations, as well as segregated or non-relevant information, DL 2.0 handles preliminary investigation file in the following ways.

- Retention and Disposal: For files that do not evolve into full investigations, DL 2.0 ensures that information is retained according to legal and organizational policies. This is done by setting up automated retention schedules, which are based on the type and sensitivity of the information, and secure deletion protocols, which ensure that data is permanently erased when no longer needed.

- Access Control: DL 2.0 provides a high level of control over access to preliminary investigation files, limiting it to authorized personnel only. The system uses robust role-based access controls to prevent unauthorized access, ensuring the security of sensitive information.

- Segregation or Non-relevant Information: DL 2.0 would handle information that needs to be segregated (such as non-pertinent portions of recordings under Title III) by implementing data tagging or metadata classification. DL 2.0 uses metadata tagging to identify the source, sensitivity, and investigative context of data within the platform. These tags are used to enforce role-based access controls, ensuring that users can only access information relevant to their authorized duties and need to know. Tagging also supports the segregation of sensitive information and enables filtering of query results based on user permissions. In addition, metadata tagging supports data governance by identifying applicable restrictions and facilitating auditing and oversight of data access and use. This helps in clearly distinguishing between relevant and non-relevant information.

- Data Masking and Redaction: For segregated information, DL 2.0 might apply data masking or redaction techniques, if determined necessary to ensure that non-relevant parts are not exposed to unauthorized users. This is particularly important for sensitive information that must be protected even when not directly pertinent to the investigation.

- Data Handling Policies: DL 2.0 plays a crucial role in enforcing data handling policies. It ensures that all data, including segregated or non-relevant information is managed according to its sensitivity level. This includes ensuring that such information is stored securely and accessed only by those with appropriate authorization. In essence, DL 2.0 systems are designed to ensure that all types of information, whether part of preliminary investigations or segregated from relevant content, are managed, protected, and disposed of in accordance with legal requirements and organizational policies.
- Audit Trails: DL 2.0 maintains comprehensive audit trails to track all access and modifications to preliminary investigation files. This transparency ensures that all interactions with these files are logged for security and compliance purposes, instilling confidence in the system's integrity.

Privacy Risk: DEA may collect PII for investigations or activities beyond the scope of its Title 21 authority

Mitigation: This risk is mitigated. The determination and rationale to collect information in the information systems feeding data into the Data Lake is not part of the DL 2.0 process, since those determinations were made by DEA's investigators. However, information from those systems accessible by DL 2.0 is within DEA's authority. In general, DEA policy requires supervisory approval before beginning an investigation wherein any issues regarding Title 21 authority would be surfaced and addressed. If the material in question was obtained by legal process, warrant applications would demonstrate DEA's authority and justification for the collection in the process to obtain court authorizations for Title III wiretaps and when collecting pen register activity, trap and trace information, and electronic data content (such as voicemail, text messaging, push-to-talk communications, short messaging service (SMS) and e-mail messages). Additionally, it is a statutorily mandated requirement for all domestic wiretap requests to be authorized by a high-level official at the Department of Justice prior to court approval. Investigators and monitors are required to read the Title III application, affidavit, and court order which collectively identify, and the scope of the interception authorized and the applicable minimization procedures in each case. Likewise, administrative subpoenas will contain a listing of legal authority and would receive approval by supervisors. Lastly, in the course of DEA investigations, Special Agents may acquire information or evidence of non-controlled substance related crimes. In such instances, DEA is authorized to take steps to preserve the information or evidence and then coordinate with a law enforcement agency that has the requisite jurisdiction to investigate those crimes.

Privacy Risk: By aggregating data from many systems, potentially including information originally collected by federal, state, local, tribal, and foreign law enforcement agencies, DEA may exceed the minimal amount of data necessary to satisfy DEA's law enforcement mission.

Mitigation: This risk is mitigated. All data accessed by DL 2.0 at this stage of implementation is information collected within DEA criminal investigation and regulatory authority and the collection of which was authorized by the Controlled Substances Act. DL 2.0 is intended to collect and consolidate all investigative details from existing DEA information systems and conduct overarching data analysis. These systems include DEA's case management system, an indexing system of case management data fields coupled with case disposition information, a system for deconfliction of certain types of tracked information from DEA cases, and controlled

substance transaction data by DEA registrants. DL 2.0 is simply a central platform to produce analysis and insight into DEA data. Additionally, DL 2.0 is designed to manage, protect, and ensure the proper handling of sensitive information and protect segregated or non-relevant information as noted above.

Future expansions of the databases feeding into DL 2.0 will include additional information DEA databases, and potentially at some point include datasets of information originally collected by federal, state, local, tribal, and foreign law enforcement agencies. DEA will assess the privacy implications and needs analysis on an ongoing basis and supplement this PIA as necessary.

DEA will carefully evaluate each data set proposed to be added to DL 2.0 to determine whether its use is directly relevant and necessary to accomplish the investigative purposes DEA is authorized to pursue. DEA estimates DL 2.0 will ingest no more than three to five data sets per year with a total of 15 data sets added over the next several years. This PIA will be updated continually to document information about current and pending data sets to be added to DL 2.0. For each new data set added DEA will employ an onboarding process for engaging, prioritizing, documenting, vetting, and then loading new data sets. This onboarding process will be comprehensive, to include an assessment of data minimization to protect privacy and the development of or modification to applicable Initial Privacy Assessments to ensure formal consideration of PIA and SORN update requirements of the source systems, as well as whether access control rules or user types that need to be reviewed, modified, or created.

Privacy Risk: Possibility that the PII of an unrelated individual (who is not under suspicion or the subject of investigation) is collected as part of an incident or investigation about someone else.

Mitigation: This risk is mitigated the determination to collect information is not part of the DL 2.0 processes those determinations were made by investigators using the component systems feeding data into DL 2.0. In general, however, DEA will only retain third party information that is associated with those who may be linked or connected to a person of law enforcement interest, connected to potentially criminal or other illicit activity, or for identifying individuals or entities of concern. Monitoring of domestic conversations will terminate immediately when it is determined that the conversation is unrelated to communications subject to interception under Title III. Interception will be suspended immediately when it is determined through voice identification, physical surveillance, or otherwise, that none of the Targets, or any of their confederates, when identified, are participants in the conversation, unless it is determined during the portion of the conversation already overheard that the conversation is criminal in nature. Raw Wiretap transcriptions will not be directly ingested into the Data Lake. However, any transcriptions of wiretap information deemed relevant by the DEA-6 form originator may be included in the DEA-6 report, which will be ingested into the DL 2.0 environment at regularly scheduled intervals.

DL 2.0 uses metadata tagging to identify the source, sensitivity, and investigative context of data within the platform. These tags are used to enforce role-based access controls, ensuring that users can only access information relevant to their authorized duties and need to know. Tagging also supports the segregation of sensitive information and enables filtering of query results based on user permissions. In addition, metadata tagging supports data governance by identifying applicable restrictions and facilitating auditing and oversight of data access and use.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Potential for use of PII in a manner incompatible/inconsistent with the intended uses of or specified purposes for collection of the information

Mitigation: This risk is mitigated. The data collected and shared through DL 2.0 and its database subsystems are intended to support law enforcement information sharing among DEA and other federal, state, local, tribal, and international law enforcement partners. The information in the DL 2.0 was collected for purposes of criminal investigations, and access to DL 2.0 is restricted to authorized personnel with a validated need-to-know, so any use of information from criminal files that is compatible with law enforcement purposes is a legitimate use. Risk of illegitimate use is minimized through access controls, required training, and audit logging that monitors and reviews all user activity. Role-based access controls limit visibility of sensitive investigative data. All data collected with within the DEA's authority and is authorized for law enforcement use. The platform can be used for data exploration, reporting, analytics, machine learning, and data visualization, enabling users to gain a more accurate understanding of relevant details related to any case, investigation, or operation—all of which are legitimate law enforcement purposes.

Further, the data shared is appropriately limited to law enforcement data only and originates from DEA law enforcement collections activities in the areas of drug enforcement, criminal law enforcement and criminal investigations. Additionally, system users must complete the DEA IT Rules of Behavior prior to being granted access to the system information. Furthermore, all users with access to PII data have been trained on the proper use of PII information and have signed applicable acknowledgement documentation. Lastly, DL 2.0 can only be accessed by approved users with a need to know and is configured for multi-factor authentication.

Privacy Risk: Potential for a system breach by physical intrusion or technical exploitation of the data at rest or in transit.

Mitigation: This risk is partially mitigated. The DL 2.0 servers are a hybrid cloud virtual server system. Any actual servers for DL 2.0 or the physical servers for databases providing data to DL 2.0 are stored within Federal/DEA buildings in a secure room with controlled access or using appropriate GSA-approved security systems. Further, DL 2.0 access points are also located in federal buildings with restricted access and physical security systems. DEA uses Security in Depth relying on multiple layers of physical and electronic protection of the system and the data contained within the system. Physical intrusions by unauthorized individuals into DEA facilities are prevented by perimeter security protections such as armed guards and video surveillance (where applicable), and physical access is only possible through controlled entry to all DEA occupied buildings and facilities with PIV card readers for all entries.

Protection of information system resources is provided by management, operational, and technical security controls. Access to all records is controlled and limited to approved personnel with an official need for access to perform their duties. The use of individual passwords or user identification codes is required to access information system resources. DL 2.0 data protected with encryption meeting the Federal Information Processing Standard (FIPS) Publication 140-2 standard for data at rest and in transit. The system is housed within an alarmed controlled access room within another outer perimeter area that is also alarmed and controlled access providing multiple layers of physical protection. See Section 6.2 for additional technical controls.

In addition, the need to know is established through the Access control list signed by the appropriate official, physically located at the entrance to the server room where data is stored.

Privacy Risk: Changes may be made in the underlying source system that are not reflected in DL 2.0 data used for analysis until the refresh cycle, potentially causing the inaccuracies and data retention in the DL 2.0 needs to align with that of the original DEA system from which the data was taken.

Mitigation: This risk is mitigated. DL 2.0 supports analytical activities and does not replace the originating systems of record that are used to maintain authoritative investigative information. With respect to DEA 6 information, only final DEA 6 forms approved by supervisors are downloaded and therefore no changes would be made to those documents. Additionally, DL 2.0 data synchronization processes refresh source system information regularly. For any other data obtained from DL 2.0, where some data relied upon was downloaded after the last refresh synchronization, the DEA users collecting that information are aware they will need to confirm that data from the underlying source system.

Further, the authoritative, official record of the PII Information, data or relevant evidence downloaded to DL 2.0. Therefore, with respect to investigative files, information will be retained in the underlying source systems under the relevant NARA or NARA-approved DEA retention schedules (usually 25 years after close of the case), but any products of Title III authorizations are kept generally for 10 years or whenever the judge authorizes destruction of such evidence.[5] Currently, DL 2.0 maintains approximately five years of data, and automated processes update DL2.0 to purge records daily to maintain the five-year retention window. Therefore, retention in DL2.0 will not be longer than the underlying source schedules for the most critical investigative information.

c. Potential Threats Related to the Dissemination of the Information

Privacy Risk: Potential for DEA personnel to share or disclose PII Information to an inappropriate party or for an improper use.

Mitigation: This risk is mitigated. The data collected and shared through DL 2.0 and its database subsystems are intended to support law enforcement information sharing among DEA and other federal, state, local, tribal, and international law enforcement partners. The data shared in accordance with established, signed Memorandums of Understanding (MOU) and is appropriately limited to law enforcement data only and originates from DEA law enforcement collections activities. This information is collected during law enforcement missions in the areas of drug enforcement, criminal law enforcement and criminal investigations. The data use restrictions imposed on all the included law enforcement member agencies, ensure that the use of this

[5] Within the underlying source system, collected Title III evidence is destroyed when there is no longer an agency, court or media interest in the material, and only after securing any necessary authorization for destruction from a court of competent jurisdiction. Currently there is no schedule for non-Title III products. While there is no schedule, DEA data retention policy controls the length of retention for up to 20 years. See, https://www.justice.gov/archives/usam/archives/usam-1-6000-doj-personnel-witnesses.

information is consistent with the original law enforcement purposes for which DEA originally collected data. Internal DOJ and DEA users that have a validated need-to-know and have been granted official access to DEA information must sign a non-disclosure agreement.

Privacy Risk: Potential for access by DEA personnel with no authorization or no need to know the information.

Mitigation: This risk is mitigated. DL 2.0 implements multi-factor authentication using PIV credentials, role-based access controls, encryption of data at rest and in transit, and continuous monitoring. System activity is logged and subject to auditing. An authorized user's access is limited, controlled and tracked by the system. A user is granted access to DL 2.0 by completing applicable IT user training, completing applicable PII Awareness training and signed applicable non-disclosure documentation. A DL 2.0 user login and password must meet the Department of Justice's complex password policy requirements, and both the DEA issued Personal Identity Verification card and user logins are required when accessing the system. All user activities are monitored by security analysts and an automated system looking at events logged by the system. User access privileges are different that administrator access privileges. No user will be given enough privileges to misuse on their own. Separation of duties between user and administrator are statically defined and users cannot be administrators and vice versa.

Further, collected information is only used by authorized users specific to the types of investigations, criminal organizations or Divisional areas for each user and further sharing and use of the data is appropriately limited to law enforcement data only. Access to data within DL 2.0 is restricted not only by user role within the platform, but also by the user's authorization to access the originating DEA systems from which the data is derived. Access control mechanisms ensure that users may only query or view data associated with source systems for which they have been granted appropriate access through established DEA authorization processes. These controls are enforced through role-based access controls and metadata tagging that align user permissions with the source system of record, ensuring that users cannot access data from systems for which they are not authorized. All personnel involved with the DL 2.0 program have been cleared and have signed a non-disclosure agreement (NDA). This data collected is kept online (soft copy), offline (soft copy) and may be printed in some individual cases.

In addition, each user annually is required to review and acknowledge the DEA IT Rules of Behavior as part of the mandated online IT Security Training. These individuals confirm that they have read and accepted the IT Rules of Behavior regarding the proper handling of all DEA documents and data. This mitigates the risk of unauthorized use or disclosure of DEA's pertinent information. The limited distribution of the information from the applications, continual monitoring of access to the applications, and the observance of the IT Rules of Behavior, limit privacy risks. Outside of DEA, Federal Government users must also comply with computer security requirements, participate in annual security training, and acknowledge updated rules of behavior.

d. Potential Threats Related to the system's Use of Super Intelligence

Privacy Risk: The use of Super Intelligence (SI) algorithms/Machine Learning (ML) in the operations of DL2.0 theoretically could contribute to output inaccuracies and affect determinations drawn from the data results that the SI algorithm selects.

Mitigation: This risk is mitigated. Machine learning models within DL 2.0 are used solely to support analytical review and do not make or determine investigative outcomes. Outputs are treated as preliminary analytical indicators and are validated by trained DEA personnel using underlying source data and investigative context. The system emphasizes human review, cross-referencing with authoritative records, and reliance on multiple data points rather than single-model outputs. Additionally, model development and use are controlled and limited to authorized users, and the models are not relied upon as the sole source of information for any determination. These controls ensure that any potential inaccuracies do not directly impact investigative or enforcement decisions.

Privacy Risk: SI models/Machine Learning tools could be trained on inadvertently faulty historical datasets resulting in an algorithmic demographic subjectivity and potentially inaccurate outcomes.

Mitigation: This risk is mitigated. DL 2.0 utilizes non-generative machine learning models that operate on existing investigative datasets for analytical support purposes only. These models are not used to make or inform investigative or enforcement decisions and are not used to independently identify or target individuals. Outputs generated by these models are treated as analytical leads and are subject to review and validation by trained DEA personnel prior to any operational use. In addition, model development and use are limited to authorized personnel, and results are interpreted within the broader investigative context. Because the system relies on human review and does not automate decision-making, the risk of bias directly affecting outcomes is mitigated.

Privacy Risk: SI/ML algorithms in this system could be considered opaque (i.e., a "Black Box") meaning officers and auditors cannot completely understand how the system reached a specific conclusion and making it challenging for DEA personnel to understand and testify to how a tool reached a specific conclusion.

Mitigation: This risk is mitigated. DL 2.0 employs non-generative machine learning models that support analytical activities and do not independently produce conclusions or decisions. Outputs from these models are used only to highlight patterns, correlations, or relationships within existing data and are always reviewed by trained DEA personnel. Analysts rely on the underlying source data, not the model itself, to interpret results and support investigative findings. Because the models are not used as the basis for determinations and do not replace analyst judgment, the need for full algorithmic explainability is reduced, and transparency is maintained through human review and reliance on original investigative records.

Privacy Risk: Super intelligence/Machine Learning tools could be subject to SI "hallucinations"—where SI invents transcriptions/images/events that never happened.

Mitigation: This risk is mitigated. DL 2.0 does not utilize generative SI, and does not generate new content, narratives, or data. The platform employs non-generative machine learning models that analyze existing data to identify statistical patterns and relationships. These models do not create or infer new facts, and all outputs are derived directly from underlying datasets. Because the system does not generate content and all analytical outputs are reviewed by DEA personnel against source data, the risk of fabricated or “hallucinated” information is not present.