Drug Enforcement Administration

Privacy Impact Assessment
for the
Registrant Support Network (RSN)

Registrant Support Network
Issued by:
James Robert Bryden

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: May 5, 2023

(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 Privacy Impact Assessment (PIA) for the Registrant Support Network (RSN), of the Drug Enforcement Administration (DEA) covers a dedicated network of IT infrastructure hosting a group of applications that collect and maintain information – pursuant to the Controlled Substances Act of 1970, as amended, and other authorities – about persons that handle or seek to handle controlled substances and listed chemicals.[1]

As background, the Controlled Substances Act of 1970 and its implementing regulations make it unlawful to manufacture, distribute, dispense, or possess controlled substances or List I chemicals except in an authorized manner. Those that seek to handle controlled substances or List I chemicals must obtain a registration from the Attorney General. The Controlled Substances Act of 1970 and regulations also impose reporting and record-keeping requirements.[2]

Section 2: Purpose and Use of the Information Technology

Explain in more detail than above the purpose of the information technology, 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.

2.1 Purpose of Registrant Support Network

The Drug Enforcement Administration (DEA) Diversion Control Division (DC) mission is to prevent, detect, and investigate any diversions of controlled pharmaceuticals and listed chemicals from legitimate sources while ensuring an adequate and uninterrupted supply for legitimate medical, commercial, and scientific needs. RSN applications automate application, registration, compliance, and reporting, and it supports investigation and enforcement efforts.

[1] "Persons" include any individual, corporation, government or governmental subdivision or agency, business trust, partnership, association, or other legal entity. 21 CFR Part 1300.01(b).

[2] This legal framework (contained in Title 21 of the U.S. Code and Title 21 of the Code of Federal Regulations) is available at http://www.deadiversion.usdoj.gov/21cfr/index.html. See 21 U.S.C. § 802(6) and (34) for the definitions of "controlled substance" and "List I chemical."

Applicants and registrants can access RSN internet applications via the DC website: https://www.deadiversion.usdoj.gov.

DEA personnel with authorization to access an RSN application can query those applications. Authorized users receive a role, user ID, and password to allow user to add, modify, delete, or edit information within RSN databases. The user's role and need-to-know determines their access and capabilities. A DEA user only receives access to an RSN application once a supervisor approves access and requests logon credentials.

Examples of DC activities that RSN helps facilitate are the following:

- Investigate the identity and qualifications of applicants and registrants to ensure that only qualified and approved individuals, businesses, and organizations are authorized to handle controlled substances and List I chemicals;
- Collect information about controlled substances that are subject to national drug production quotas and international treaty obligations;
- Collect information about regulated sellers' compliance with the Combat Methamphetamine Epidemic Act (CMEA) of 2005 in order to assist prevention, detection, and investigation of the diversion of scheduled listed chemical products from legitimate channels;
- Receive notifications and/or reports of the theft or significant loss of controlled substances and any unusual or excessive loss or disappearance of a listed chemical;
- Produce special reports required for statistical and analytical purposes to facilitate computerized monitoring and tracking of the distribution of controlled substances and listed chemicals;
- Verify payment of registration fees;
- Support investigative actions on applicants, registrants, and other individuals, businesses, and organizations associated with applicants and registrants by providing a suite of software to track and collate name, address, authorized drug schedules, transaction information, and regulatory compliance;

Applicants and registrants[3] enter information into RSN databases through DC web forms, including information about their business/organization and processes. This information[4] includes:

- Applicant/registrant identification information (name of individual, business or organization, place of business address, name, phone number, and point-of-contact email address);
- Debt collection information (individual applicant's/registrant's social security number for debt collection);

[3] Applicants are persons that have applied for a registration but have not yet obtained it. Registrants are persons that have obtained a registration, including registrants that are applying for a renewal of their registration.

[4] Note that while many of the items of information pertain to the applicant or registrant, some of them pertain to others (e.g., a point of contact who is entering the information on behalf of the applicant or registrant).

- Taxpayer identification number (of business or organization applicants/registrants);
- DEA registration number/identifier (of registrants only);
- Information about practitioner and mid-level practitioner applicants/registrants (professional degree, professional school, year of graduation, national provider identification, date of birth);
- State license information (state license number; state-controlled substance license number);
- Liability information (e.g., whether the applicant/registrant has ever been convicted of a crime in connection with a controlled substance; whether the applicant/registrant has ever surrendered or had a controlled substance registration revoked, suspended, denied, restricted, or placed on probation);
- Application fee information for validation purposes (credit card number and expiration date, name of credit card holder). Only payment type, amount, and payment status are retained;
- Drug theft or loss information (e.g., incident details, product information, police report details, new security measures taken);
- Transaction information (e.g., name of parties, DEA registration number of parties, address and contact information of parties, order form number); and
- User information (e.g., name, email address, user ID, password).

RSN provides the backbone for several different registrant support applications. There are two main divisions of applications: RSN Internal and DEA DMZ (for DC Website applications). Within the RSN Internal division, the Registrant Information Consolidated System (RICS) is the umbrella name for most registrant support applications. RICS is composed of independent browser-based database applications designed to automate user registration, compliance, reporting, and to support investigation and enforcement efforts. Once an application is approved, the applicant/registrant receives a DEA registration number. This number becomes a key identifier to accessing the applicant/registrant's information throughout RICS. Four other applications, though housed and operated on RSN within the RSN Internal side, are not part considered part of the RICS.

An explanation of each application, the information it collects, and how information is used by the application follows:

I. RSN INTERNAL

A. Registrant Information Consolidated System (RICS)

Automated Reports and Consolidated Orders System (ARCOS)
The CSA requires manufacturers and distributors of certain controlled substances to report certain transactions of such substances to the Attorney General. The Automated Reports and Consolidated Orders System monitors the flow of drugs from their point of manufacture through commercial distribution channels to point of sale or distribution at the dispensing/retail level (e.g., hospitals, retail pharmacies, practitioners, Mid-Level Practitioners (MLP), teaching institutions). ARCOS collects information about these transactions, which are then summarized into reports that give investigators in federal and state agencies information that can be used to identify persons who may be diverting controlled substances into illicit channels of distribution. Investigators and prosecutors also use the

information to strengthen criminal, administrative, and civil cases. See also, DEA System of Records Notice (SORN) Justice/DEA-003, Automated Records and Consolidated Orders System - Diversion Analysis and Detection System, 69 Fed. Reg. 51104 (Aug. 17, 2004), and ARCOS II PIA, https://www.dea.gov/foia/privacy-impact-assessment.

Bulk Chemical Manufacturers Reporting (BCMR)
As provided for in 21 C.F.R. § 1310.05(d), each regulated bulk manufacturer of a listed chemical shall submit manufacturing, inventory, and use data on an annual basis as set forth in Section 1310.06(h). For this assessment, the term "regulated bulk manufacturer of a listed chemical" means a person who manufactures a listed chemical by means of chemical synthesis or by extraction from other substances, not including persons whose sole activity consists of the repackaging or relabeling of listed chemical products or the manufacture of drug dosage form products which contain a listed chemical. The Bulk Chemical Manufacturers Reporting application allows these persons to complete these reports online. Information about registrants is downloaded from the CSA application using the DEA registration number. BCMR also collects login information and information about the use of the chemical(s) (e.g., chemical name, manufactured aggregate quantity, year-end inventory). DEA uses this information to investigate the bulk manufacture of listed chemicals and to ensure that the manufacturer does not produce excessive product (which may indicate diversion). BCMR is routinely queried by reference to name and DEA registration number (where applicable). These queries retrieve much of the information in the system associated with those identifiers. See, DEA SORN JUSTICE/DEA-020, Essential Chemical Reporting System, 52 Fed. Reg. 4219 (Dec. 11, 1987).

Combat Methamphetamine Epidemic Act (CMEA) Application
The Combat Methamphetamine Epidemic Act of 2005, an amendment of the CSA, requires regulated sellers of scheduled listed chemical products to submit a self-certification to the Attorney General that the seller understands the substantive requirements of the Act (e.g., placement of such substances "behind the counter") and that those who are responsible for delivering such substances to purchasers, or who deal directly with purchasers by obtaining payment for the substances (e.g., employees of the seller), have undergone training regarding the Act's substantive requirements. The CMEA application allows sellers to self-certify online; the application ensures compliance with the self-certification requirement. While this self-certification is separate from registration to handle controlled substances or List I chemicals under the Controlled Substances Act (via the CSA application), CMEA downloads information about regulated sellers that are also controlled substance registrants from CSA by querying the CSA database with the seller's DEA registration number. CMEA collects additional information from the seller, such as the number of employees who work for the seller, and assigns the seller a certificate ID number.

Controlled Substances Act (CSA) Application
The CSA application automates registration and renewal of DEA accounts. Information collected by CSA is used to assist DEA in verifying and approving applicants and renewing registrants. In addition, DEA administrative and investigative actions (e.g., orders to show cause, civil fines, letters of admonition) on registrants are reported and tracked through CSA. Information collected by CSA is queried by various data elements, including DEA registration number, and may be used to produce reports sorting registrants and applicants by geographic area, drug schedule authorization, DEA registration number expiration date, business activity, and other fields. See also, SORN DEA-005 (Controlled Substances Act Registration Records), 52 Fed. Reg. 47208 (Dec. 11, 1987). The CSA

database is a High Valued Asset (HVA), monitored by DOJ using IBM Guardium (continuous data monitoring (CDM) tool).

Chemical Transaction Analysis System (CTRANS)
The Chemical Transaction Analysis System is the name given to the following group of subsystems. The information contained in these CTRANS modules is used to monitor and track the distribution of listed chemicals and controlled substances and to identify suspicious transactions and relationships between distributors from the wholesale level to the retail level. See, DEA SORN JUSTICE/DEA-020, Essential Chemical Reporting System, 52 Fed. Reg. 4219 (Dec. 11, 1987).

- **Chemical Import/Export (CH IMEX)**
  The Chemical Import/Export system collects and maintains information about imports and exports of listed chemicals that are imported into, exported from, or transshipped through the United States, for the purposes of tracking such transactions and ensuring compliance with 21 U.S.C. § 971, and with 21 C.F.R. Part 1313. When an importer or exporter who is also a DEA registrant undertakes the transaction, the DEA registration information is retrieved from the CSA application using DEA registration number. Additional information is collected directly from importers and exporters, such as information about the other party (e.g., name, contact information, DEA registration number if applicable); transaction information (e.g., whether it is an import or export, location information); information about the substance; and transportation information (e.g., name of vessel).

- **Controlled Substance Import/Export (CS IMEX)**
  The Controlled Substance Import/Export system collects and maintains information about imports and exports of listed controlled substances that are imported into, exported from, or transshipped through the United States, for the purposes of tracking such transactions and ensuring compliance with 21 U.S.C. §§ 952-953 and 21 C.F.R. Part 1312. When an importer or exporter who is also a DEA registrant undertakes the transaction, the DEA registration information is retrieved from the CSA application using DEA registration number. The same types of additional information collected directly from importers and exporters by CH IMEX is also collected by CS IMEX.

- **Regulated Machines Import Export (RM-IMEX)**
  The Regulated Machines Import Export application will permit regulated persons (as defined in the CFR§1310.05) to report the domestic sale, import, and/or export of tableting and encapsulating machines via an interactive application on the Diversion Control website. When the transaction is entered into RM-IMEX by an importer or exporter with a DEA registration, the registration information is retrieved from CSA using the DEA registration number. Additional information is collected directly from importers and exporters, such as information about the other party (e.g., name, contact information, DEA registration number if applicable); transaction information (e.g., whether it is an import or export, location information); information about the substance; and transportation information (e.g., name of vessel). Applications are routinely queried by reference to DEA registration number or name, retrieving much of the information associated with those identifiers.

- **Chemical Handlers Enforcement Management System (CHEMS)**
  The Chemical Handlers Enforcement Management System consolidates information about handlers of and transactions involving listed chemicals from a variety of sources for reporting and analytical purposes in order to support investigations. Sources of information include CSA; invoices; import/export declarations; and investigator notes and reports. Information maintained by CHEMS includes registration information retrieved from CSA; CHEMS ID (a unique ID number that serves as the key element by which all other information in the system is tracked and collated); information about past investigations of individuals, businesses, and organizations; information contained in investigator notes and reports; invoice information; and import/export information. By allowing DEA users to sort, assemble, and organize this information in a variety of ways, CHEMS enables DEA to track the flow of listed chemicals in support of diversion control efforts and investigations.

- **Leads Application**
  The Leads application allows the CBP to report the seizure of illegal tableting and encapsulating machines to the Diversion Control Division, Regulatory Section (DRG). It will allow DRG personnel to modify, comment upon, and assign reports to DEA field operatives.

- **Mail Order System (MOS)**
  MOS permits required persons to submit reports to DEA regarding the shipment/receipt of certain chemicals through the mail.

- **Port Import/Export Reporting System (PIERS)**
  This application receives data from the Journal of Commerce regarding water-borne imports/exports of listed chemicals (Note: this application will sunset in 2023)

Harmonized Tariff Schedule (HTS)
The Harmonized Tariff Schedule maps HTS codes to drug codes for use with import and exports of chemicals and controlled substances.

Guidance Document Portal (GDP)
The Guidance Document Portal allows for the upload and indexing of DC guidance documents for the public.

Image Scanning Application
Physical materials received through the mail (lets, new and renewal applications, etc.) must be scanned into the database and then linked to the appropriate CSA record. The Image Scanning application allows users to accomplish this task.

Industry Tip Reporting (ITR)
The Industry Tip Reporting application allows pharmacists to report suspicious pharmacological orders. This application is for the use by pharmacists in their practice.

Manufacturer and Distributors Briefing Report (MDBR)

The Manufacturer and Distributors Briefing Report collects data from the field about which manufacturers and distributors have received briefings from their local field office. It tracks the date, assigned personnel, and the subjects covered.

National Drug Death Reporting System (NDDRS)

The National Drug Death Reporting System) collects scientifically verified drug-related death information from the offices of coroners and medical examiners. This is used to detect new and changing trends in drug abuse, monitor the diversion of legitimately marketed drugs, and provide information in support of drug scheduling actions.

Year-End Reporting and Quota Management System (QMS)

Each year DEA establishes quotas for the total annual needs for controlled substances in Schedules I and II, and the List I chemicals ephedrine, pseudoephedrine, and phenylpropanolamine. Certain CSA registrants are required to submit applications for quotas to DEA. The Quotas application downloads CSA registration information from the CSA database using the registrant's DEA registration number. The Year-End Reporting and Quota Management System (QMS) also collects information about registrants (e.g., estimated inventory, estimated dispositions, estimated manufacture), about substances (e.g., dosages, requested quantities, packaging/labeling information), and about buyers (e.g., name, contact information, point of contact, transaction information). E1 manufacturers who have registered for one or more of the following drug codes: 9670, 9600, and 9040 are required to file a Narcotic Raw Material (NRM) report. Collection of this information helps DEA evaluate registrants' past supply and use of substances, and analyze registrants' estimated future use of substances.

Reporting (Cognos Analytics)

Reporting/Cognos Analytics is RSN's data warehouse reporting solution, permitting authorized internal DEA users to correlate, analyze, extract, and report on data gathered from many of the RSN applications.

R Abuse

The prescription abuse application (Rx Abuse) collects data on the abuse of pharmaceutical drugs, such as oxycodone and hydrocodone, and the doctors and pharmacies involved in their distribution.

Synthetic Drug Reporting System (SDRS)

The Synthetic Drug Reporting System collects information concerning the suspicious distribution and misuse of synthetic drugs.

Suspicious Order Reporting System (SORS II)

The Suspicious Order Reporting System II receives reports from all registrants who have received a suspicious order. SORS II replaced two previously available DC systems:

- **Suspicious Orders and Non ARCOS Reporting System (SONARS)**
  The Suspicious Orders and Non ARCOS Reporting System (SONARS) is the legacy application to the Suspicious Order Reporting System (SORS), DEA personnel to analyze suspicious order reports made by registrants. The application reports only reported sales and purchases.

- **Suspicious Order Reporting System (SORS)**
  This application no longer accepts data. It was the predecessor to the SORS II system and received reports from registrants who received a suspicious order.

Theft/Loss Reporting (TLR) Application
Registrants are required to notify DEA of the theft or significant loss of a controlled substance and/or listed chemical. The TLR application enables the reporting of such incidents to DEA over the internet. Registrants access TLR by entering their name and DEA registration number; entry of this information enables TLR to download information about the registrant from CSA. TLR collects additional information about the theft or loss (e.g., incident details, police report details, quantity lost or stolen, new security measures taken). DEA personnel use TLR not only to ensure compliance with reporting requirements but also to investigate specific registrants (e.g., to determine whether the registrant is taking appropriate security measures) or recurring instances of theft or loss (e.g., to determine if theft or loss is more prevalent with regard to certain substances or in certain geographic areas).

Toxicology (TOX) Application
This application tracks toxicology reports at the request of an individual at the occasion of an overdose or death as a result from a controlled substance. The application collects the requested data, the requesting facility, incident date, and any drugs identified.

B. Non-RICS Applications

Diversion Resource Management System (DRMS)
The DRMS application tracks DC employee and position data. New employee and position data are referenced from the Table of Organization Management System (TOMS). An account has been established with the Office of Finance, Financial Systems Section, Technical Support Unit (FNS) to allow a view into two (2) data tables. This occurs through an Open Database Connectivity (ODBC) connection directed through Firebird, and through a File Transfer Protocol (FTP) connection through Firebird and the FNS system.

Geospatial Information System (GIS)
GIS allows global mapping and positioning of registrant address data. Its applications extend query and reporting capabilities for multiple RSN applications. GIS maps primarily to CSA address tables.

Integrated Voice Response (IVR) Network
The IVR network allows registrants limited access to their account through the telephone lines. Bi-directional communication exists between IVR and CSA, with both parties in the transaction able to send and receive information. Because IVR is open to the public phone lines, communications between IVR and the rest of RSN is secured by a firewall.

National Forensic Laboratory Information System (NFLIS)
The National Forensic Laboratory Information System collects results from drug chemistry analyses conducted by federal, state, and local forensic laboratories across the country. NFLIS resides on the RSN DMZ environment; unlike other RSN applications, it has no counterpart in the internal environment. A third-party vendor is contracted to review and report on the data that forensic laboratories submit to NFLIS. The vendor’s connection to the NFLIS environment on RSN is secured by DEA’s network.

Print on Demand (POD) Network

The Print on Demand (POD) network processes printing requests from RSN applications. POD is segregated from the rest of the network because of the difference in hardware required for its operation.

II. RSN DEMILITARIZED ZONE (DMZ)

The RSN DMZ hosts the online DC Website applications. They are independent browser-based registration, compliance, and reporting applications used primarily by the registrant population.

ARCOS Online

Automated Reports and Consolidated Orders System Online (ARCOS Online) collects information about the flow of controlled substances from their point of manufacture through commercial distribution channels to point of sale or distribution at the dispensing/retail level (e.g., hospitals, retail pharmacies, practitioners, MLPs, teaching institutions). The information is summarized in RSN Internal ARCOS into reports that give investigators in federal and state agencies information that can be used to identify persons who may be diverting controlled substances into illicit channels of distribution. Investigators and prosecutors also use the information to strengthen criminal, administrative, and civil cases.

BCMR Online

The Bulk Chemical Manufacturers Reporting Online (BCMR Online) application allows regulated bulk manufacturers to submit manufacturing, inventory, and use data on an annual basis. The web form collects the chemical name, manufactured aggregate quantity, and year-end inventory.

Bulk Data Interchange (BDI)

The BDI allows authorized registrants to upload certain data and reports to DEA.

CSA Online

Controlled Substances Act Online (CSA Online) comprises a collection of separate web forms that, taken together, collect and manage applicant and registrant accounts. Any information collected by the CSA Online web forms is used to assist DEA in verifying and approving applicants and renewing registrants, and is therefore subject to review by DC users in the internal version of CSA. The following table lists the CSA web forms:

Web Form	Purpose
New Applications	Allows individuals to register with DEA using electronic versions of DEA Forms 224, 225, 363, and 510
Renewal Applications	Allows individuals to renew their registration with DEA using electronic versions of DEA Forms 224a, 225a, 363a, and 510a
Registration Changes	This web form allows registrants to make the following changes to their registration: • Name • Address • Schedule • Drug Code

Web Form	Purpose
Duplicate Certificate	Allows registrants to request a duplicate certificate using an electronic version of DEA Form 223
Order Forms	Registrants may request that DEA Form 222 be mailed to them through the USPS.
Duplicate Receipt of Registration	Allows those registrants who have applied or renewed online to query for and reprint their receipt.
Online Pharmacy Modification	Allows users who are registered as Retail Pharmacies or Online Pharmacies to change the following registration information: • Modify Business Activity from Retail Pharmacy to Retail Online Pharmacy and vice versa • Modify existing Retail Online Pharmacy information
Registrant Validation	Allows registrants to confirm the registration information of other registrants
Controlled Substances Disposal Registration	Allows registrants to perform the following actions: • Modify eligible DEA registration to collect pharmaceutical controlled substances from ultimate users (e.g., patients) • Modify DEA registration to stop being a collector • Modify existing collector registration information
Authorized Collector Location Search	Allows users to search for an authorized controlled substance collection site. Users do not have to be DEA registrants.
Registrant Datasets Access (RDA) Download	Provides CSA registrant records to authorized individuals
Chemical Exemption	The Chemical Exemption application allows external population to complete a Chemical Exempt request.

CMEA Online

The Combat Methamphetamine Epidemic Act Online (CMEA Online) application allows sellers to self-certify online for the ability to sell ephedrine, pseudoephedrine, and phenylpropanolamine products. Anyone, including CSA registrants, must self-certify. However, the $21 fee is waived for the registrant population because they have already paid for a registration; non-registrants must pay the fee.

While this self-certification is separate from registration to handle controlled substances or List I chemicals under the Controlled Substances Act (via the CSA application), CMEA downloads information about regulated sellers that are also controlled substance registrants from CSA by querying the CSA database with the seller's DEA registration number. CMEA collects additional information from the seller, such as the number of employees who work for the seller, and assigns the seller a certificate ID number.

Diversion Investigator Worksheet (DI Worksheet)
The DI Worksheet provides computational worksheets for the Diversion Investigator Cyclic Investigations.

Theft and Loss Reporting (TLR) Online
Registrants are required to notify DEA of the theft or significant loss of a controlled substance or listed chemicals. Registrants access the Theft and Loss Online application by entering their name and DEA registration number, which is then checked against the CSA database, to log in to the application. Regulated persons who manage chemicals but who are not required to register with DEA must request an identifier upon their first report. The application will collect their business name, business type, address, phone number, email address, and point of contact information. Once registered with TLR Online and logged in, the registrant/regulated person may then provide detailed information about a theft or loss.

Guidance Document Portal (GDP) Online
GDP Online allows users to view uploaded DC guidance documents.

IMEX Online
The Import-Export Online (IMEX Online) application collects and maintains information about imports and exports of listed chemicals and controlled substances that are imported into, exported from, transshipped through the United States, or brokered by an entity within the US that involves parties otherwise outside US jurisdiction. When the transaction is undertaken by an importer or exporter that is also a DEA registrant, the DEA registration information is retrieved from the CSA application using a DEA registration number. Additional information is collected directly from importers and exporters, such as information about the other party (e.g., name, contact information, DEA registration number if applicable); transaction information (e.g., whether it is an import or export, location information); information about the substance; and transportation information (e.g., name of vessel). This application fulfills the requirements for the following DEA forms: 486 and 386 (List Chemicals); 161, 236, 357 (Controlled Substances).

ITR Online
The Industry Tip Reporting Online (ITR Online) application allows pharmacists to report suspicious pharmacological orders. This application is for the use by pharmacists in their practice.

Leads Online
The Leads Online application allows the CBP to report the seizure of illegal tableting and encapsulating machines to the DRG. It allows DRG personnel to modify, comment upon, and assign reports to DEA field operatives.

National Takeback Initiative (NTBI)
The National Takeback Initiative encourages the public to return their unused, unwanted, and unneeded prescription medication to designated NTBI sites. The NTBI web form allows federal, state, and local governments or federal, state, and local law enforcement officials to register as an NTBI

collection site. NTBI events are performed in conjunction with state, local and tribal law enforcement partners.

Pharmacy Diversion Awareness Conference (PDAC)
The Pharmacy Diversion Awareness Conference (PDAC) is designed to assist pharmacy personnel in identifying and preventing diversion activity. They consist of two, one-day conferences open to pharmacists, pharmacy technicians, or loss prevention personnel employed by pharmacies or hospitals/clinics. Attendees are provided instruction on drug trends, corresponding responsibility, State Pharmacy Board updates, CMEA, Medicare/Medicaid fraud, and theft. The PDAC application allows individuals to register online for conferences sponsored by DC.

Quotas/Year-End Reporting System (YERS)/ Narcotic Raw Material (NRM)

The Quotas/YERS/NRM application is divided into two online web forms: one for data collection/reporting, and one for quota requests.

Web Form	Purpose
YERS/NRM	Allows registered manufacturers to submit data on their year-end inventory of Schedules I and II, Schedules III-V Psychotropic substances, NRM substances, and List I chemicals. The data entered here is used to establish subsequent quotas.
Quotas	Allows registered manufacturers of schedules I and II controlled substances, and importers of List I chemicals, to submit applications for manufacturing/procurement quotas. DEA Forms: 189, 250, 488

RM IMEX Online
The Regulated Machines Import Export (RM-IMEX) application will permit regulated persons (as defined in the CFR§1310.05) to report the domestic sale, import, and/or export of tableting and encapsulating machines via an interactive application on the Diversion Control website.

℞ Abuse Online
The prescription abuse online application (℞ Abuse Online) is an on-line reporting mechanism allowing the public to report illegal activity concerning controlled pharmaceuticals, such as oxycodone and hydrocodone, by the doctors and pharmacies involved in their distribution.

SDRS
The Synthetic Drug Reporting System (SDRS) collects info concerning the suspicious distribution and misuse of synthetic drugs.

SORS Online
The Suspicious Order Reporting System (SORS) Online allows registrant to file reports about potentially suspicious or unusual controlled substance orders.

Suspicious Online Pharmacies
This web form users to enter information about online pharmacies that appear to be suspicious or fraudulent.

TLR Online
Registrants are required to notify DEA of the theft or significant loss of a controlled substance. Registrants access TLR by entering their name and DEA registration number, which is then checked against the CSA database, to log in to the application. Once logged in, the registrant may then provide detailed information about a theft or loss.

TOX Online
This application tracks toxicology reports at the request of an individual at the occasion of an overdose or death as a result from a controlled substance. The application collects the requested data, the requesting facility, incident date, and any drugs identified.

Unlawful Medical Products Internet Reporting Effort (Umpire)
Unlawful Medical Products Internet Reporting Effort (UMPIRE) is a web-based system that allows the public to report suspicious internet pharmacies.

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	Controlled Substances Act (CSA), Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970
Executive Order	
Federal Regulation	Title 21, Code of Federal Regulations, Part 1300 to the end.[5]
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.

[5] For more information, see http://www.deadiversion.usdoj.gov/21cfr/cfr/index.html.

(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

Name	X	B C D	CSA and TOX CSIMEX, CHIMEX, and RMIMEX, name of organization DRMS; IMEX applications may also contain the name, phone number, and address of non-US entities.
Date of birth or age	X	C B	CSA and TOX DRMS
Place of birth			
Gender	X	C B	TOX DRMS
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C B	CSA, full SSN DRMS, full SSN
Tax Identification Number (TIN)	X	C	CSA and CMEA
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers	X	C	CSA collects the license plate and expiration date of mobile narcotic treatment program registrants.
Personal mailing address	X	C D	CSIMEX, CHIMEX, and RMIMEX, organization mailing address, including city, state, country, and zip
Personal e-mail address			
Personal phone number	X	C D	CSIMEX, CHIMEX, and RMIMEX, organization phone, fax, telex numbers
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	C	CSA
Education records	X	C B	CSA, medical school and year graduated only DRMS, indicates honors during BDIT
Military status or other information			
Employment status, history, or similar information	X	B	DRMS

(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

Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents	X	C	POAs are collected from the relevant applicants
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C	UMPIRE
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C	CSA collects responses for four liability questions related to the registrants' handling of controlled substances; it also records civil actions and fines taken against registrants.
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	C	ARCOS, BCMR, CTRANS, CHEMS, CHIMEX, CSIMEX, MOS, SORS, and PIERS
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			

(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

- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	C	CSA
- **User passwords/codes**			
- **IP address**	X	C	All RSN Applications
- **Date/time of access**	X		All RSN Applications
- **Queries run**	X		
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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

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

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

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

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	Access to the data is provided to authorized users within DEA. CSA data is shared with the DEA Information Systems Data group, which maintains a data warehouse and data search functionality
DOJ Components	X			See explanation below this table.
Federal entities		X		Reports regarding registrant information are provided to authorized and validated federal government entities.
State, local, tribal gov't entities		X		See the State **Regulatory Agencies** section below this table.
Public		X	X	See the section, “Registrants”, below. Aggregated statistics of registrant data (for example, the number of providers in a given state) is provided in Registrant Population reports on the DEA Diversion Control Division Website (https://apps.deadiversion.usdoj.gov/RAPR/raprRegistrantPopulationSummary.xhtml). See section 4.2 of this document.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X	X	Registrant data may be provided to authorized DEA personnel for the purpose of civil action against a registration.

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.**
Private sector	X	X		CSA registration information is shared with registrants for the purpose of allowing them to validate other registrants' status. Registration information is also shared with vetted 3rd party vendors to allow them to provide validation, accreditation, and verification services for registrants. In both cases, registrants or vetted 3rd parties must provide authorized credentials to view or download CSA information.
Foreign governments				
Foreign entities		X		Exports. Through the UN Pre-Export Notification Online system[6]
Other (specify):				

In the event that a DOJ law enforcement component such as the FBI or a U.S. Attorney's Office requests information from an RSN database, there are procedures in place to ensure that DEA has approved the request, and there is an official need-to-know information (i.e., to further investigate a particular registrant). DEA approval happens at the component's level of access to the information:

- Upon receipt of such a request, a DEA employee must document the purpose of the disclosure and the information to be shared with the component.

- If direct access to an RSN database is needed, the requesting component must:

  - Obtain a user account for DEA's internal network, which requires agreement with the DEA IT Rules of Behavior for General Users as well as DEA approval of the desktop computer that will be used to access the network.

  - Obtain an RSN administrator account. DEA strictly controls a component's level of access to information in RSN. In addition, users from other components will have read-only access to RSN. Information is transmitted through a secure connection to the user's workstation.

Information stored in RSN is shared with or received by the following entities external to the DOJ:

Third Party Accreditation/Validation Services

DEA provides registration information from CSA to third party accreditation and validation services that assist registrants in validating registrants' status with DEA. For example, a hospital considering

[6] See http://www.unodc.org/unodc/en/global-it-products/pen.html for more information.

hiring an anesthesiologist will contact an accrediting company to assure that their applicant has a valid DEA registration to handle controlled substances.

All third-party applicants for access to registration information are vetted by DEA prior to being granted a username and password. Data is stored in text files that authorized users may download on a daily basis. Users requesting access must agree to abide by DEA's data usage policy which prohibits unauthorized distribution of the dataset.

The following information is shared with third party accreditation/validation services: Business Activity Code, Drug Schedules, Name, Additional Company Info, Address, City, State, Zip Code, Business Activity Sub-Code, Activity (Active, Inactive).

State Regulatory Agencies
Information in CSA and SORS is routinely shared with state regulatory agencies. The disclosed data include the name of registrant, the registrant's address, business activity, authorized drug schedule, the DEA registration number, the issuance date, registration expiration date, and the fee status. The information is shared to better enable state agencies to identify discrepancies between CSA records and their own records and thus enforce laws, regulations, and policies regarding controlled substances and List I chemicals. State agencies requesting access to this data must agree to abide by DEA's data usage policy which prohibits unauthorized distribution of the dataset.

Customs and Border Protection
Information in CTRANS is routinely shared with Customs and Border Protection. The disclosed data include the details of import and export orders, permits, and declarations. Information is shared with CBP in the course of easing and validating the import, export, and transshipment of controlled substances, listed chemicals, and regulated machines. Data exchanged with CBP is under protection of an Interconnection Security Agreement (ISA) which details the methodology for the exchange of data, and a Memorandum of Understanding which restricts the usage of the data to the enforcement of applicable laws.

Department of Health and Human Services
Information in CSA is routinely shared with the Department of Health and Human Services. The disclosed data include the name of registrant, the registrant's address, business activity, authorized drug schedule, the DEA registration number, the issuance date, registration expiration date, the fee status, registrant date of birth (if applicable), and the professional school and year of graduation (if applicable). Information is shared with the Department of Health and Human Services in the course of investigations of medical fraud and for verification of registrant data. Prior to accessing this data, and every time they access the data, HHS agrees to abide by DEA's data usage policy which prohibits unauthorized distribution of the dataset.

International Narcotics Control Board
Information in CHIMEX is routinely shared with the International Narcotics Control Board. All data elements gathered regarding a specific chemical export transaction are shared via the Pre-Export Notification Database. This information is shared to verify transaction information and is mandated by International Treaty to facilitate enforcement.

Registrants
Information in CSA is routinely shared with registrants. The shared information includes the DEA registration number, name, business address, approved drug schedules, registration expiration date, issuance date, and fee status. This information is provided to allow registrants to verify the status of registrants with whom they may conduct business. For example, prior to ordering a controlled substance or List I chemical, a registrant may verify that the individual, organization, or business from which they are ordering is registered with DEA, and therefore legally permitted to handle the product.

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.

Aggregate data on registrant population is shared with the public through the Registrant Population link on the Diversion Control Division public website. The public can access summaries of the number registrants by fiscal quarter, by state, or by business activity.

The data provided to the public is simple sums of the number of registrants within a given geographical region, or according to their business activity. No PII is divulged.
URLs for the data access are below:

Summary: https://apps.deadiversion.usdoj.gov/RAPR/raprRegistrantPopulationSummary.xhtml
Active Registrants by State:
https://apps.deadiversion.usdoj.gov/RAPR/raprRegistrantPopulationSummary.xhtml
Active Registrants by Business Activity:
https://apps.deadiversion.usdoj.gov/RAPR/raprRegistrantPopulationByBusinessActivity.xhtml
Active Chemical Handler Registrants:
https://apps.deadiversion.usdoj.gov/RAPR/raprActiveChemicalHandlers.xhtml
Qualifying Practitioners by State[7]:
https://apps.deadiversion.usdoj.gov/RAPR/raprQualifyingPractitionersByState.xhtml

<u>Section 5:</u> 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.

Notices that address the authority for the collection of information, the purposes for which information is intended to be used, its dissemination, and the effects of not providing all or any part of the

[7] This report contains information on DATA waived registrants. The DATA Waive series was discontinued during Q2 of fiscal year 2023, but historical records continue to exist.

requested information, are displayed on the applications on the DC website.[8] Such notices are also available in hard copy paper form. The notice on the website explains how DEA will use and share information individuals voluntarily provide to DEA to obtain a benefit from DEA – a license to handle controlled substances and List I chemicals. As such, there is minimal risk that an individual will be unaware that their information is being collected or of how it will be used.

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.

Individuals have the opportunity to decline to provide information. No individual is required to provide information. However, registration is a requirement for individuals, organizations, and businesses wishing to handle controlled substances and list I chemicals. Failing to provide the requested information precludes registration. There are also Privacy Act notices stating the same thing provided with online DEA registration forms (Forms 224, 225, 363 and 510). See also the Diversion website privacy notice: https://www.deadiversion.usdoj.gov/security.htm

Individuals have an opportunity to consent to particular uses of the information. The uses of information gathered by RSN applications are stipulated on the application's login page. Providing the information requested indicates consent to those uses.

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 information pertaining to them in RSN may submit a Freedom of Information Act request under Subpart A, Part 16, Title 28, Code of Federal Regulations and/or Privacy Act request under Subpart D, Part 16, Title 28, Code of Federal Regulations.

Individuals may also request information pertaining to them from the following SORNs, however, exemptions may apply: DEA-005 (Controlled Substances Act Registration Records), 52 Fed. Reg. 47208 (Dec. 11, 1987), DEA-003 (ARCOS Diversion Analysis and Detection System), 69 Fed. Reg. 51104 (Aug. 17, 2004), DEA-008 (Investigative Reporting and Filing System), 77 Fed. Reg. 21808 (April 11, 2012), DEA-020, Essential Chemical Reporting System, 52 Fed. Reg. 471219 (Dec. 11, 1987).

<u>Section 6</u>: Maintenance of Privacy and Security Controls

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

[8] For example, see http://www.deadiversion.usdoj.gov/security.htm

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):** 11/8/22 **If an ATO has not been completed, but is underway, provide status or expected completion date:** 5/8/2023 **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:** POAMs are deemed sensitive information and are not released publicly. POAMs are tracked within DOJ CSAM database.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
	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: RSN is a Moderate system based on FIPS 199 Security Categorization.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** A vulnerability management policy is in place to protect the system from malicious code and from other system weaknesses. Vulnerability scans are run and analyzed regularly. Regular reviews are conducted to provision and/or cancel user accounts as appropriate.
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:** Role-based access (as determined by DEA management based on users' duties); monitoring, auditing, and logging all user activity; Internal log review performed daily and SIEM tool forwards collected logs for further evaluation and review by separate DEA security group.
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**.
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:

No additional training is required for this system outside of that available on DEALS.

6.2 Explain Key Privacy and security administrative, technical, or physical controls that are designed to minimize privacy risk. 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

RSN is categorized as a Moderate control baseline per the NIST Special Publication 800-53 methodology.. Accordingly, security controls for both internal and DMZ applications are inherited from RSN. NIST privacy controls have been assessed for RSN. Rev 5 Baseline has been reviewed and control assessment and validation has occurred; indicated within Security and Privacy Plan The following controls were selected and applied to bolster RSN's privacy protections and risk strategies to reduce the possibility of unauthorized access and/or disclosure:

NIST 800-53 Control Number	Requirement	Implementation
AC-8: System Use Notification	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems:	In order to access RSN applications on the private, DEA network, authorized users are required to acknowledge that their use may be monitored, recorded and subject to audit. They are notified that they are accessing a U.S. Government information system, and that unauthorized use of the system is subject to civil and criminal penalties. Access to the internal system is not available until the user acknowledges and accepts these stipulations. Users interacting with RSN applications online receive notices regarding authorized information use, privacy accommodations, and references to applicable laws regarding the collection of data. The privacy statement for RSN online applications can be viewed here: https://www.deadiversion.usdoj.g

	(i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of authorized uses of the system.	ov/security.htm Additional, application-centric information is provided to users prior to logging in.
AC-22: Publicly Accessible Content	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	The Information Systems Division, Diversion Technology Section (TGD) designates a Content Manager who is responsible for reviewing and posting updates to the publicly accessible portions of RSN applications. The Content Manager performs periodic reviews of content posted to the publicly accessible portions of RSN applications in order to ensure that public access to such information is consistent with applicable laws and policies (such as the Privacy Act). If it is determined that public access to the information does not comport with such authorities, the information is restricted from public access or removed.
AR-2: Privacy Impact and Risk Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The RSN PIA complies with guidance in OMB Memorandum M-03-22.
IA-8: Identification and Authentication (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Section 4.1 of this PIA establishes the non-organizational users with access to information on the system, and delineates the parameters for that access.
RA-3: Risk Assessment	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the	Risk Assessments are conducted annually at minimum on Diversion Control systems, including the systems which

	unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results; c. Reviews risk assessment results; and d. Updates the risk assessment at an organizationally defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	house RSN applications. These assessments are documented, reviewed and approved by organizational management. Deviations from security controls are documented and reviewed quarterly at minimum, until resolved.

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.)

The retention period of the information is temporary and ranges from 5 years to 55 years, or when no longer needed for reference purposes.[9]

CSA information is scheduled under NC1-170-77-1 and N1-170-89-1. CTRANS information is scheduled under N1-170-06-1. The retention period for the information in these systems is 55 years for current business purposes. These schedules will be updated to reflect changes as needed. CMEA information is new and presently unscheduled. Disposition is not authorized. CMEA information is under review, and the proposed schedule will mirror that of CSA data. DC continues to work with the DEA Records Management Unit on appropriate retention policies.

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

[9] The retention schedule for registration application files varies depending on the action taken by DEA. For example, the schedule calls for an approved application to be destroyed after eight (8) years from the date of the approval. Conversely, the schedule calls for an application that has been administratively coded (i.e., denied, revoked, or suspended) to be transferred to a federal records center after ten (10) years, then destroyed after 55 years from the date of the coded action.

in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

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:***

This system is covered by an existing system of records notice. Privacy Act-protected information in RSN is covered by the system of records notices DEA-005 (Controlled Substances Act Registration Records), 52 Fed. Reg. 47208 (Dec. 11, 1987), DEA-003 (ARCOS Diversion Analysis and Detection System), 69 Fed. Reg. 51104 (Aug. 17, 2004), DEA-008 (Investigative Reporting and Filing System), 77 Fed. Reg. 21808 (April 11, 2012), DEA-020, Essential Chemical Reporting System, 52 Fed. Reg. 471219 (Dec. 11, 1987); and DOJ-002 (DOJ Computer Systems Activity and Access Records), 64 Fed. Reg.73585 (Dec. 30, 1999).

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?

a. Potential Threats Related to the Collection of the Information

Privacy Risk: A potential threat to privacy is that the system will collect unauthorized data or collect more data than required in light of the purposes of the system.

Mitigation: This potential threat is mitigated in that the DEA is authorized to collect this needed information as specified by law. Additionally, human controls are in place to ensure that RSN applications only collects authorized information and does not over-reach their permissions. Specifically, information collected by RSN applications is regularly reviewed by DC to ensure legal compliance, the continued relevance and applicability of information requested to the scope of Diversion's mission.

Privacy Risk: Another potential threat that exists to the privacy on the information collected and the sources of that information is the collection of inaccurate information.

Mitigation: This potential threat is mitigated, as information is entered into RSN applications by the entities that are the subjects of the information. The CSA application collects more personal identifying information (PII) than the other RSN applications and is the primary data source of the other RSN applications. This data integration scheme greatly reduces the risk of human error. Moreover, information entered into the system is manually reviewed and verified by DEA personnel before a registration application is approved. RSN also includes automated verifications and checks to maintain uniform, error-free data. Information submitted is subject to a variety of automated verification, validation and edit routines before the information is added. Incorrect information is returned to the submitter for correction.

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

Privacy Risk: Potential threats to privacy include improper access to data which threatens the integrity of the data.

Mitigation: These threats are mitigated by implementing security features and safeguards such as certification and accreditation in accordance with Federal Information Security Management Act requirements; requirements at the account-creation stage (i.e., supervisor request and permission); authentication controls to include strong identity verification mechanisms; role-based access controls (i.e., some users may have read-only access); user agreement with DEA IT Rules of Behavior; incorporation of "need-to-know" requirements and procedures designed to satisfy those requirements throughout the system; system auditing; encryption of data at rest and in transit; continuous patching and vulnerability testing; appropriate network segmentation; timely provisioning and cancellation of user accounts through regular reviews; and physical security features in place at the location where RSN data is stored. In addition, system administrators have security clearances and receive general privacy training and training on Rules of Behavior; RSN information is designated within DEA as administratively controlled information that must be protected from unauthorized disclosure, alteration, and destruction.

Privacy Risk: A potential threat to privacy as a result of DEA's use of the information in application housed within RSN is misuse of the information.

Mitigation: This risk is mitigated. A description of the measures and safeguards DEA has implemented to mitigate this risk is included in the response to the other risk identified in this section. However, the measures and safeguards specifically designed to prevent misuse of information include:

- Requirement that DEA users of RSN agree to DEA IT rules of behavior for general and privilege users;
- Role-based access controls
- Maintenance of audit logs (which track modifications of records, among other things);
- Designation of RSN information as administratively controlled information that must be protected from unauthorized disclosure, alteration, and destruction);
- Timely provisioning and cancellation of user accounts through regular reviews;
- Requirement of supervisor request and permission to receive login credentials;
- Authentication controls (including strong password);
- Incorporation of "need to know" requirements (and procedures designed to satisfy those requirements) throughout system;
- Monthly patches and vulnerability tests; and
- General privacy training for system users and administrators.

Privacy Risk: The system's administrative controls may be insufficient to prevent unauthorized individuals within DEA from accessing the system's PII without a need to know.

Mitigation: This risk is low and has been mitigated. NIST privacy controls have been assessed for RSN. Rev 5 Baseline has been reviewed and control assessment and validation has occurred; indicated within Security and Privacy Plan. The privacy of registrant data is dependent on ensuring that only authorized staff has access to the system data. To meet this requirement, smart-card and biometric access to the facility was designed into the system. The network design has also been enhanced to defend the privacy of this data; the data is segregated on a private network segment in order to enhance data privacy. In order to protect the privacy and security of its data, the system limits its connections to other systems.

The physical area in which the system is maintained is accessible only to individuals who have received clearance. Data from the system is not removed from the secured area where it is used. Personnel who access the sensitive data do so in a secluded section of the secure area. All users of the system are prohibited from copying sensitive data to non-government hardware.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Potential threats to privacy also include unauthorized disclosure of data which threatens the confidentiality of the data.

Mitigation: These threats are mitigated by the implementation of in-depth security technologies, features and practices such as:

- System Certification and Accreditation in accordance with Federal Information Security Management Act requirements;
- Requirements at the account-creation stage (i.e., supervisor request and permission);
- Robust Authentication to include strong Identity Control and Access Management that leverages Role-Based Access Control strategies (i.e., some users have elevated privilege access where others have read-only access) and "need-to-know" requirements and procedures.
- User Account provisioning, right-sizing, suspension and cancellations through automated alerts and regular reviews;
- User Agreement instruments coupled with DEA IT Rules of Behavior for both General Users and DEA Privileged Users;
- System security and performance auditing;
- Encryption of data when at rest, in processing, and in transit;
- Continuous Monitoring with timely patching and vulnerability testing;
- Network Segmentations appropriate for functionality and data classification, and
- Physical Security features in place at all locations where RNS application data is processed and stored.

In addition, system administrators have security clearances and receive general privacy training and training on Rules of Behavior; information collected by RSN applications is designated within DEA as administratively controlled information that must be protected from unauthorized disclosure, alteration, and destruction.

Further, in the event that a law enforcement component of the DOJ such as the FBI or a U.S. Attorney's Office requests information from RSN, there are procedures in place to ensure that there is an official need to know the information (e.g., to further an investigation of a particular registrant) and that DEA has approved the component's level of access to the information. There are also controls when non-DOJ components seek dissemination of the information. See controls at Section 4.1 above.