Drug Enforcement Administration

Privacy Impact Assessment
for the
Registrant Information Consolidated System

Issued by:
Preston L. Grubbs, Senior Component Official for Privacy

Approved by: Erika Brown Lee, Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: June 4, 2014

(September 2012 DOJ PIA Form)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) posted at http://www.justice.gov/opcl/pia.htm.]

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

This privacy impact assessment (PIA) covers the Registrant Information Consolidated System (RICS), a group of applications that collect and maintain information – pursuant to the Controlled Substances Act of 1970 (CSA), as amended, and other authorities – about persons that handle or seek to handle controlled substances and listed chemicals.[1]

As background, the CSA and its implementing regulations generally 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 CSA and regulations also impose reporting and record-keeping requirements.[2]

The mission of the Drug Enforcement Administration (DEA), Office of Diversion Control (OD), is to prevent, detect, and investigate the diversion of pharmaceutical controlled substances and listed chemicals from legitimate sources and channels while ensuring an adequate and uninterrupted

[1] "Persons" include any individual, corporation, government or governmental subdivision or agency, business trust, partnership, association, or other legal entity.

[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."

supply for legitimate medical, commercial, and scientific needs.

RICS automates application, registration, compliance, and reporting, and it supports investigation and enforcement efforts. The following are examples of OD activities that RICS helps facilitate:

- Investigating 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;
- Collecting information about controlled substances that are subject to national drug production quotas and international treaty obligations;
- Collecting information about regulated sellers' compliance with the Combat Methamphetamine Epidemic Act of 2005 in order to assist prevention, detection, and investigation of the diversion of scheduled listed chemical products from legitimate channels;
- Receiving 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;
- Producing special reports required for statistical and analytical purposes to facilitate computerized monitoring and tracking of the distribution of controlled substances and listed chemicals;
- Verifying payment of registration fees;
- Supporting 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; and
- Tracking U.S. importation and exportation of controlled substances and listed chemicals.

Applicants and registrants[3] enter information into RICS, including information about their business/organization and processes. This information[4] includes:

- Applicant/registrant identification information (name of individual or business or organization; place of business address; name, phone number, and e-mail address of point of contact)
- Debt collection information (social security number of individual applicants/registrants; taxpayer identification number of business or organization applicants/registrants)
- DEA registration number (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)

[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).

- 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 (credit card number and expiration date; name of credit card holder). This information is collected for validation. Only the 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)
- User information (e.g., name, e-mail address, user ID, password)

After an applicant/registrant submits an application/renewal, a DEA investigator or registration program specialist will undertake to verify the validity of the information. Once an application is approved, the applicant/registrant receives a DEA registration number. This number becomes a key to accessing the applicant/registrant's information throughout all RICS applications (which are described in detail below).

RICS is comprised of several different applications, which are described below:

- **Controlled Substances Act application**: The CSA application is the RICS application that automates initial registration and renewals. Accordingly, it collects more personally identifiable information (PII) (including many of the items of information listed above) than the other RICS applications. Most of the PII that is maintained in RICS is stored in the database associated with the CSA application. The other RICS applications retrieve the PII stored in the CSA application database by querying the DEA registration number, which serves as a common identifier for all RICS applications.

  Information collected by the CSA application is used to assist DEA in verifying and approving applicants and 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 the CSA application. Information collected by the CSA application 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.

- **Drug Theft and Loss application (DTL)**: Registrants are required to notify DEA of the theft or significant loss of a controlled substance. DTL enables the reporting of such incidents to DEA over the internet.[5] Registrants access DTL by entering their name and DEA registration

[5] Background information about this legal requirement and related materials are available at http://www.deadiversion.usdoj.gov/21cfr_reports/theft/index.html.

number; entry of this information enables DTL to download information about the registrant from the CSA application. DTL 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 DTL 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). Accordingly, routine queries of DTL consist of filtering information on the following data elements: DEA registration number; national drug code of substance stolen or lost; method of theft (e.g., armed robbery); drug schedule; and carrier (which is applicable only if the theft or loss occurred during transit).

- **Combat Methamphetamine Epidemic Act (CMEA) self-certification application**: The Combat Methamphetamine Epidemic Act of 2005, which amends 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.[6] The CMEA allows sellers to self-certify online. While this self-certification is separate from registration to handle controlled substances or List I chemicals under the CSA (via the CSA application), the CMEA application downloads information about regulated sellers that are also controlled substance registrants from the CSA application by querying the CSA application with the seller's DEA registration number. The CMEA application 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.

  DEA uses the CMEA application for the main purpose of ensuring compliance with the self-certification requirement of the Act. For example, if during a site visit a DEA investigator notices that a pharmacy is selling a scheduled listed chemical product, the investigator can query the CMEA application to determine whether the pharmacy has submitted a self-certification. The CMEA application is queried by reference to DEA registration number, certificate ID number, name of seller, state, and zip code. Searching by these fields yields virtually all the information about a seller that the CMEA application has either directly collected from regulated sellers or that it has downloaded from the CSA application.

- **Automated Reports and Consolidated Orders System (ARCOS)**: The Controlled Substances Act requires manufacturers and distributors of certain controlled substances to

---

[6] The text of the Combat Methamphetamine Epidemic Act and related materials are available at http://www.deadiversion.usdoj.gov/meth/index.html#cmea.

report certain transactions of such substances to the Attorney General.[7] ARCOS monitors 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, mid-level practitioners, 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. The information is also used by investigators and prosecutors to strengthen criminal, administrative, and civil cases.

ARCOS downloads several items of information about registrants by querying the CSA application by reference to DEA registration number. As indicated above, ARCOS also collects information about transactions of controlled substances (e.g., date of transaction, name of buyer, contact information of buyer, type and quantity of substance) and assigns authentication information to manufacturers and distributors. ARCOS is often queried by DEA by reference to DEA registration number or name of manufacturer or distributor. For example, if a DEA investigator wants to find out if a certain buyer is purchasing an excessive quantity of a controlled substance, the investigator can query ARCOS by reference to the buyer's DEA registration number.

- **Chemical Transaction Analysis System (CTRANS)**: CTRANS is the name given to the following group of subsystems. The information contained in these 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.

    - Chemical Handlers Enforcement Module System (CHEMS): CHEMS consolidates information about handlers of listed chemicals and transactions involving listed chemicals from a variety of sources for reporting and analytical purposes in order to support investigations. Sources of information include the CSA application; invoices; import/export declarations; and investigator notes and reports. Information maintained by CHEMS includes registration information retrieved from the CSA application; CHEMS ID (an identification number unique CHEMS 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. For example, if a DEA investigator receives a tip about a chemical manufacturer who is using a non-registered supplier to receive a listed

[7] Background information about this legal requirement and related materials are available at http://www.deadiversion.usdoj.gov/arcos/index.html.

chemical, the investigator can query CHEMS by the name of the supplier or manufacturer to determine if any other investigative activities have been pursued against them. CHEMS is routinely queried by reference to name of handler, state, and zip code.

- Chemical Import/Export (CHIMEX) and Controlled Substances Import/Export (CSIMEX) applications: CHIMEX and CSIMEX collect and maintain information about imports and exports of controlled substances and 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. §§ 952, 953, and 971, and with 21 C.F.R. Parts 1312 and 1313.[8] 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 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). These applications are routinely queried by reference to DEA registration number or name. These queries retrieve much of the information associated with those identifiers.

- Mail Order System (MOS): 21 U.S.C. § 830(b)(3) generally requires that regulated persons who engage in a transaction with a non-regulated person or who engages in an export transaction involving ephedrine, pseudoephedrine, or phenylpropanolamine, and which uses or attempts to use the U.S. Postal Service or any private or commercial carrier, must report such transaction to the Attorney General. MOS enables such persons to complete these reports online. The system retrieves information about reporters from the CSA application using DEA registration number, where applicable. It collects transaction information (including the name and address of non-regulated person(s) and information about the substances involved in the transaction) directly from the reporters. In doing so, MOS allows DEA to track such transactions and supports diversion control efforts and investigations. For example, if a DEA investigator suspects that a buyer may be bypassing physical pharmacies to receive ephedrine through the mail, a query by the buyer's name or address could assist the investigator in determining if an excessive amount of the substance is being shipped to the buyer, even if the supply comes from different sources. A search of the buyer's name or address retrieves all of the transaction information associated with those fields.

- Port Import/Export Reporting System (PIERS): PIERS maintains information about imports and exports of listed chemicals (by water only), and it is used by DEA for multiple purposes. First, DEA uses PIERS to detect emerging trends concerning

[8] For more information about these requirements, see http://www.deadiversion.usdoj.gov/21cfr_reports/chemicals/index.html and http://www.deadiversion.usdoj.gov/imp_exp/index.html.

chemicals of interest. Second, PIERS helps DEA investigators ensure compliance with reporting requirements. For example, if an investigator suspects that a chemical importer is not completing required forms, the investigator may query both PIERS and CHIMEX by reference to the importer's name in order to determine if there are any discrepancies between the information in the two systems. PIERS obtains information solely from the Journal of Commerce. This information includes names and contact information of parties to the transaction and carriers, as well as shipping information and chemical information.

- **Quotas application**: As background, each year DEA establishes quotas for the total annual needs for controlled substances in schedules I and II, 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 application using DEA registration number. The Quotas application 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). Collection of this information helps DEA evaluate registrants' past supply and use of substances, and analyze registrants' estimated future use of substances. DEA routinely queries the Quotas application by reference to registrant name and DEA registration number. These queries retrieve most information in the system associated with those identifiers.[9]

- **Bulk Chemical Manufacturers Reporting application (BCMR)**: As stated 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 report, 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. The term "bulk manufacturer" does not include 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 BCMR 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.[10]

---

[9] For more information on quotas, see http://www.deadiversion.usdoj.gov/quotas/index.html.

[10] For more information on bulk chemical manufacturer reports, see http://www.deadiversion.usdoj.gov/chem_prog/bulk_chem_manufacturer.htm.

DEA personnel with access to the system may access and query RICS applications. The ability to add, modify, delete, or otherwise edit information in the system requires that the user receive a role, user ID, and password. The user's access and capabilities are commensurate with the user's role and need for information. A DEA user may only be granted access to the system once a supervisor approves of the access and formally requests login credentials.

RICS is accessible on the OD Web site (ODWeb) and on the Registrant Support Network (RSN). ODWeb is an external, internet-accessible platform where applicants and registrants can log in to and use RICS, whereas RSN is an internal platform where DEA authorized users access and use RICS. ODWEB and RSN are categorized as general support systems. RICS is categorized as a major application which inherits the security posture and controls of the systems on which it is installed.

Information collected and maintained by RICS is shared, and transmitted from the system, as described below in section 4.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID	X	Driver's license		Financial transaction	X
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card	X		
Other identifying numbers (specify): DEA registration number; state license number; certificate ID; session ID (a technical identifier for the connection between the user's computer and the server)					

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth		Financial info	
Alias		Address	X	Medical information	
Gender		Telephone number	X	Military service	
Age		Email address	X	Physical characteristics	
Race/ethnicity		Education	X	Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	

Work-related data					
Work address	X	Business associates			
Other work-related data (specify): Information about controlled substances and listed chemicals handled by registrant (e.g., type, quantity, usage, transaction information); information about registrant businesses and organizations (e.g., number of employees, state license information, business activities, controlled substances and listed chemicals handled); liability information, such as whether a registrant has ever been convicted of a felony related to a controlled substance or List I chemical); financial information such as credit card number, credit card expiration date, etc., for payment of registration fees.					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run	X	Contents of files	
Other system/audit data (specify): Password					

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax	X	Online	X
Telephone		Email			
Other (specify): Some registrants may choose to complete paper forms of RICS applications. Paper forms are mailed to DEA headquarters, where authorized DEA personnel enter the information into RICS through a direct connection to the application. Registrants are strongly encouraged to utilize the online applications.					

Government sources					
Within the Component	X	Other DOJ components		Other federal entities	
State, local, tribal		Foreign			
Other (specify): RICS maintains some notes and comments from DEA users					

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

Non-government sources		
Other (specify):	Media source is Journal of Commerce (PIERS only).	

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

One potential threat to privacy that exists in light of the information collected is that the system will collect more information than necessary in light of the purposes of the system. This potential threat is mitigated because DEA is only authorized to collect information specified by law, and there are human controls in place to ensure that RICS is only collecting authorized information. Specifically, information collected by the system is reviewed by the Office of Diversion Control Technology Section Program Management Office (PMO) for its applicability to the scope of the Office's mission.

Another potential threat to privacy that exists in light of the information collected and the sources of the information is the collection of inaccurate information. This potential threat is mitigated because most of the information in RICS is entered by the persons that are the subjects of the information. As mentioned above, the CSA application collects more PII than other RICS applications, and the other RICS applications retrieve this PII from the CSA application (and it is automatically populated into other applications' fields); this reduces the risk of human error inherent in entering information at multiple locations. Moreover, information entered into the system is reviewed and verified by DEA personnel before a registration application is approved. RICS also includes automated verifications and checks to maintain uniform, error-free data. Information submitted is subjected to a variety of automated validation and edit routines before the information is added to RICS. Incorrect information is returned to the submitter for correction.

Other potential threats to privacy include improper access to data (which, among other things, threatens the integrity of the data) and unauthorized disclosure of the data. These threats are mitigated by the implementation of the following security features and safeguards: certification and accreditation in accordance with Federal Information Security Management Act requirements; requirements at the account-creation stage (e.g., supervisor request and permission); authentication controls (including strong passwords); role-based access controls (e.g., 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 (including audit trails, which keep track of who modifies records); encryption of data at rest and in transit; monthly patches and vulnerability tests; presence of firewalls (segregating the external ODWEB from the internal RSN); timely provisioning and cancellation of user accounts through regular reviews; and physical security features in place at the location where RICS data is stored. In addition, system administrators have security clearances and receive general privacy training and training on rules of

behavior; RICS information is designated within DEA as administratively controlled information, which must be protected from unauthorized disclosure, alteration, and destruction; and RICS is in compliance with DOJ IT Security Standards.

Finally, it is worth noting that much of the information collected by RICS is publicly available, inasmuch as regulated individuals, businesses, and organizations will often post their names, DEA registration numbers, and other information on their web sites or at their places of business.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
X	For litigation (to the extent that investigations and enforcement efforts reach litigation)		
X	Other (specify): To ensure compliance with registration, record-keeping, and reporting requirements contained in Title 21 of the U.S. Code and Title 21 of the Code of Federal Regulations.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Please see the response to question 1, above, for a detailed explanation of each RICS application, the information collected by the applications, and how the applications use the information.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	CSA, 21 U.S.C. § 801 *et seq*. Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1)) (taxpayer ID number)

	Executive Order	
X	Federal Regulation	21 C.F.R. Parts 1300-1316[11]
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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.[12]

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.

OD continues to work with the DEA Records Management Unit on appropriate retention policies.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

A potential threat to privacy as a result of DEA's use of the information in RICS is misuse of the information, including unauthorized disclosure of the information. A description of the measures and safeguards DEA has implemented to mitigate this risk is included in the response to question 2.3. The measures and safeguards specifically designed to prevent misuse of information include:

- Requirement that DEA users of RICS agree to DEA IT rules of behavior
- Role-based access controls

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

[12] 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 8 years from the date of the approval. On the other hand, 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 10 years and then destroyed after 55 years from the date of the coded action.

- Maintenance of audit logs (which track modifications of records, among other things)
- Designation of RICS 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
- General privacy training for system users and administrators

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

As an initial matter, note that DEA requires the authorized recipients listed below that seek information from RICS to make a formal request for such information before DEA will make the disclosure.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components[13]	X			
Federal entities		X		Reports regarding registrant information are provided to authorized and validated federal government entities.
State, local, tribal gov't entities		X		Reports on registrant information and populations are provided to authorized and validated state government entities.
Public				
Private sector				
Foreign governments				

[13] Information in RICS is not routinely shared with other DOJ components. However, if a law enforcement component such as the FBI or a U.S. Attorney's Office requests information about a specific applicant or registrant, such information may be shared with that component for the purpose of furthering investigation of the applicant or registrant, in accordance with the procedures and requirements described in the response to question 4.2.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Foreign entities (UN International Narcotics Control Board)				Through the UN Pre-Export Notification Online system[14]
Other (specify):			X	Some registrant information[15] is shared with other registrants via authorized log in to the OD Website.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

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 RICS, 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:

- 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 RICS 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 as well as DEA approval of the desktop computer that will be used to access the network.
  - Obtain a user account for RICS itself. DEA strictly controls a component's level of access to information in RICS. In addition, users from other components will only have read-only access to RICS. Information is transmitted through a secure connection to the user's workstation.

RICS information is shared with the following entities external to the Department of Justice:

- The Department of Commerce National Technical Information Service (NTIS)

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

[15] Information disclosed is restricted to the information which is publicly available on the DEA Registration Certificate. See section 4.2.5 for a list of elements disclosed. This information is typically used to determine whether the registrant is authorized to handle controlled substances.

- State regulatory agencies (e.g., medical boards)
- The Department of Health and Human Services
- The International Narcotics Control Board
- Registrants

Recipients external to DOJ who receive information from RICS applications must demonstrate a need to know the information requested as well as proper credentials. After their credentials are reviewed, they are permitted to download or view information pertinent to their request.

Information shared with NTIS, authorized state personnel, and the Department of Health and Human Services is protected through a secure connection to the Office of Diversion Website. Authorized users provide a username and password and may download a text file with the information required.

Registrant information shared with other registrants is protected by validation on the OD Website. Information is transmitted through a secure connection.

For more information on the security features and safeguards that have been implemented, see the response to question 2.3.

An examination of each of the DOJ-external entities which receives RICS information is included in the sections following:

4.2.1 NTIS

Information in CSA is routinely shared with the Department of Commerce National Technical Information Service (NTIS). The following data is disclosed:

- Name of registrant
- Registrant's address
- Business Activity
- Authorized Drug Schedule
- DEA Registration Number
- Issuance Date
- Registration Expiration Date
- Fee Status

This information is gathered by NTIS, the national clearinghouse for information regarding technological and scientific matters, for distribution to members of the public. NTIS collects this information for the purpose of improving outreach to health care professionals, and to better help health care professionals comply with drug enforcement regulations. This sharing is required by statute (The American Technology Preeminence Act of 1992).

4.2.2 State Regulatory Agencies

Information in CSA is routinely shared with state regulatory agencies, such as state medical boards. The following data is disclosed:

- Name of registrant
- Registrant's address
- Business Activity
- Authorized Drug Schedule
- DEA Registration Number
- Issuance Date
- Registration Expiration Date
- 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.

4.2.3 Department of Health and Human Services

Information in CSA is routinely shared with the Department of Health and Human Services. The following data is disclosed:

- Name of registrant
- Registrant's address
- Business Activity
- Authorized Drug Schedule
- DEA Registration Number
- Registration Expiration Date
- Issuance Date
- Fee Status
- Registrant date of birth, if applicable
- 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.

4.2.4 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 to facilitate international treaty enforcement.

4.2.5 Registrants

Information in CSA is routinely shared with registrants. The following information is shared:

- DEA Registration Number
- Name

- Business Address
- Approved Drug Schedules
- Registration Expiration Date
- Issuance Date
- 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.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
X	Yes, notice is provided by other means.	Specify how: Notices addressing the authority for the collection of the information, the purposes for which the information is intended to be used, how the information may be disseminated, and the effects of not providing all or any part of the requested information are displayed on applications available on the OD Website.[16] Such notices are also available on hard copy paper forms.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

X	Yes, individuals have the opportunity to decline to provide information.	Specify how: Persons are not 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.
	No, individuals do not have the opportunity to decline to provide information.	Specify why not:

5.3 Indicate whether and how individuals have the opportunity to consent to

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

particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: The uses of information gathered by RICS are stipulated on the application's login page. Providing the information requested amounts to consent to those uses.
	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not:

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Notices addressing the authority for the collection of the information, the purposes for which the information is intended to be used, how the information may be disseminated, and the effects of not providing all or any part of the requested information are displayed on the applications on the OD Website. In addition, Privacy Act-protected information in RICS is covered by the system of records notices listed in section 7. This privacy impact assessment is also a form of notice. The risk of persons not knowing that their information is being collected and how it will be used is therefore minimal. These persons voluntarily provide this information to obtain a benefit from DEA – being licensed to handle controlled substances and List I chemicals. In addition, the notice on the website explains how DEA will use and share the information that persons choose to provide.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: Yes. December 2011 (Registrant Support Network); December 2010 (OD Website). If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Please see the answers to questions 2.3 and 4.2.

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 done to provision and/or cancel user accounts as appropriate.	
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Role-based access (as determined by DEA management based on users' duties); monitoring, auditing, and logging all user activity; intrusion detection functionality; other measures as discussed in answers to questions 2.3 and 4.2.	
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.	
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.	
X	The following training is required for authorized users to access or receive information in the system:	
	X	General information security training
		Training specific to the system for authorized users within the Department.
		Training specific to the system for authorized users outside of the component.
	X	Other (specify): Agreement to comply with DEA IT rules of behavior

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Descriptions of how the access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure are included in sections 2.3 and 4.2. In addition, note that the Registrant Support Network and the Office of Diversion Control Website systems (the two platforms on which RICS resides, as explained in section 1) are categorized as systems requiring a MODERATE level of security assurance according to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Accordingly, the following controls are applied to the systems on which RICS is housed in order to protect privacy and reduce the risk of unauthorized access and 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)	In order to access RICS 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.

NIST 800-53 Control Number	Requirement	Implementation
	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: (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 the authorized uses of the system.	Users interacting with RICS applications online receive notices regarding authorized information use, privacy accommodations, and references to applicable laws regarding the collection of data. The privacy statement for RICS online applications can be viewed here: http://www.deadiversion.usdoj.gov/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	The Office of Diversion Control, Technology Section, designates a Content Manager who is responsible for reviewing and posting updates to the publicly accessible portions of RICS. The Content Manager performs periodic reviews of content posted to the publicly accessible portions of RICS 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

NIST 800-53 Control Number	Requirement	Implementation
	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 e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	is restricted from public access or removed.
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 4.2 of this PIA establishes the non-organizational users with access to information on the system, and delineates the parameters for that access.
PL-5 Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The RICS PIA complies with guidance in OMB Memorandum M-03-22.
RA-3 Risk Assessment	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the 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	Risk Assessments are conducted annually at minimum on Office of Diversion Control systems, including the systems which house RICS applications. These assessments are documented, reviewed and approved by organizational management. Deviations from security controls are documented and reviewed quarterly at minimum, until resolved.

NIST 800-53 Control Number	Requirement	Implementation
	new threats and vulnerabilities), or other conditions that may impact the security state of the system.	

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: Privacy Act-protected information in RICS 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), and DOJ-002 (DOJ Computer Systems Activity and Access Records), 64 Fed. Reg.73585 (Dec. 30, 1999).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

The information collected and maintained by the CSA application is retrieved by DEA registration number. A search of the CSA application by reference to DEA registration number retrieves all of the information associated with that number. In addition, DEA users can produce reports on multiple registrants sorted by location, drug schedule, expiration date, business activity, etc. As explained above, most of the other RICS applications retrieve registration information from the CSA application by querying the CSA application by reference to DEA registration number.

In the Drug Theft and Loss application, routine queries performed by DEA users consist of filtering database records on the following fields: DEA registration number of the registrant reporting the theft or loss; national drug code of substance lost or stolen; type of loss or theft (e.g., armed robbery or lost in transit); drug schedule; carrier (if loss or theft occurred in transit).

In ARCOS, the following fields are routinely queried to filter for registrant information: DEA registration number and registrant name.

Routine queries of the CMEA application are done by reference to DEA registration number, name, state, and/or zip code.

In the subsystems that comprise CTRANS, information is retrieved by reference to registrants, names and addresses of parties to transactions of controlled substances or listed chemicals, controlled substance or listed chemical, state, and zip code.

Information in the Quotas application is routinely searched by reference to DEA registration number and registrant name.

In the BCMR application, information is routinely searched by reference to DEA registration number and registrant name.