Drug Enforcement Administration

Privacy Impact Assessment
for the
Controlled Substance Ordering System (CSOS)

Issued by:
James Robert Bryden
Senior Component Official for Privacy
Drug Enforcement Adminstration

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

Date approved: August 7, 2023

(May 2022 DOJ PIA Template)

[THIS PAGE INTENTIONALLY LEFT BLANK]

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 Drug Enforcement Administration (DEA) regulates the manufacture, distribution and dispensing of controlled substances in the United States. This regulatory control is designed to prevent the diversion of controlled substances into "other than legitimate medical, scientific, research, or industrial channels" (e.g., the non-medical use of controlled substances for purposes not intended by the prescriber); and also, to ensure that there is a sufficient supply of controlled substances for legitimate purposes.

The DEA Information System Division, Diversion Technology Section (TGD), operates the Controlled Substance Ordering System (CSOS), whose purpose is to issue, manage, and revoke digital certificates to DEA Registrants (manufacturers, distributors, and pharmacies who order controlled substances). Registrants use these certificates to digitally sign electronic orders for controlled substances. To this end, CSOS processes applications from DEA Registrants and their personnel who have been assigned power of attorney (POA) to order controlled substances for that company. Based on the information provided by the Registrant and correlated with DEA Registration databases, digital certificates are generated by the system and downloaded by the applicant (a "Subscriber"). Certificates contain only public information, are exchanged between trading partners in business-to-business transactions, and used as a part of the digital signature process to affirm the identity of the purchaser and the substances that the purchaser is authorized by the DEA to order from the trading partner.

Information is collected directly from the applicant (the DEA Registrant or designated personnel applying for a digital certificate) and is correlated to information stored in DEA's Registration database to obtain information about the controlled substance schedules (types of drugs) that the Registrant has been pre-authorized by DEA to order. A commercial data aggregator, ChoicePoint Government Services, is used to confirm that an individual is indeed employed by the organization. In the absence of aggregator verification, confirmation is obtained through a call to the organization.

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.

The purpose of CSOS is to provide each DEA Registrant a digital certificate used to electronically sign controlled substance orders using Public Key Infrastructure (PKI) technology[1], that is an electronic equivalent of the DEA official order Form 222, the official DEA form used by DEA Registrants when

[1] PKI provides the infrastructure for managing public keys used to encrypt data.

ordering controlled substances which that DEA issues pursuant to its authority under 21 U.S.C. § 828(a). CSOS physically controls and securely stores information in the system irrespective of whether the information consists of paper or digital media. The Controlled Substances Act (CSA) prohibits distribution of Schedule I and II controlled substances except in response to a written order from the purchaser on a DEA Form 222. . DEA issues Form 222 to registrants for this purpose, preprinting on each form the registrant's name, registered location, DEA registration number, schedules, and business activity. DEA serially numbers the forms, requiring registrants to maintain and account for all forms issued. Executed and unexecuted Forms 222 are held by the registrant and must be available for DEA inspection. The Controlled Substances Act requires that executed Forms 222 be maintained for two years, *see* 21 U.S.C. § 828(c).

When ordering a Schedule I or II substance, the purchaser must provide two copies of the Form 222 to the supplier and retain one copy. Upon filling the order, the supplier must annotate both copies of the form with details of the controlled substances distributed, retain one copy as the official record of the distribution, and send the second copy of the annotated Form 222 to DEA. Upon receipt of the order, the purchasers must also annotate their copy, noting the quantity of controlled substances received and date of receipt.

The Certification Authority (CA) issues digital certificates to approved Registrants. In CSOS, subscribers create an electronic Form 222 order using CSOS-enabled ordering software. The order is digitally signed using the registrant's CSOS issued certificate. The paper DEA Form 222 is not required for electronic ordering. DEA manages the CA, controlling the content, disbursement, and tracking of DEA Form 222 and therefore assumes responsibility for the form's electronic variant.

There are 3 types of Registrations: Form 251 filled out for a Registrant, Form 252 for a Coordinator, Form 253 for a Power of Attorney. DEA will enter the registration information in private extensions fields within the digital certificates that are issued to registrants and Powers of Attorney (POA) in the same manner that DEA pre-prints the registration information on the paper order forms issued to registrants and POA.

CSOS certificates provide the means of completing the Scheduled substance ordering process electronically. The CSOS framework was designed to provide trust services to DEA registered manufacturers, distributors, pharmacies, and other DEA Form 222 users. The framework consists of Government managed systems with integrated PKI enabled software covering the following elements:

1) Certification Authority (CA) (Root CA and Subordinate CA used to issue PKI certificates to Registrants)
2) Public Facing Directory (Lightweight Directory Access Protocol (LDAP)[2] directory providing certificate status information e.g., Certificate Revocation List (CRL) information),
3) Application Servers hosting Commercial Off the Shelf (COTS) software
4) Database Servers hosting the User Registration information

[2] LDAP is a protocol that allows applications to query information easily.

The information collected by CSOS via the appropriate registration form is used to establish the eligibility and identity of an applicant for a DEA CSOS digital certificate.[3] The DEA requests specific and sufficient identity information to confirm the identity and ordering authority of the applicant for the digital certificate. This identity information is collected on an online form, which is then transferred to a printable PDF of either a CSOS 251, 252, 253, or 254, which must be printed and mailed to the DEA by the subscriber.

The following personally identifying information (PII) is collected on the online form:

- Applicant's First Name
- Last Name
- MI
- SSN
- Business Phone Number
- Email Address
- DEA Number
- DEA Reg Name
- Mother's Maiden Name
- Business Address
- City
- State
- Zip
- CSOS Coordinator Last Name
- CSOS Coordinator First name
- Photocopies of two (2) forms of identification, one (1) of which must be a government-issued ID
- Photocopy of the applicant's DEA registration certificate
- A copy of powers of attorney granting signing authorization for the registrant, if applicable.

CSOS does not analyze data to assist users in identifying previously unknown areas of note, concern, or pattern—otherwise known as datamining. No other information is added to that entered by the applicant in his or her DEA Registration forms. All paper records obtained through the application process are retained for (3) months, and then destroyed. Digital images of paper records are retained for 10 years.

Please note that PII is collected and processed in several processes within CSOS.

1. **Initial Certificate Enrollment**

Application processes are established for the identification of DEA Registrants, CSOS Coordinators and CSOS Subscribers. CSOS Subscribers are DEA registrants listed in good standing in the Controlled Substance Act (CSA) database, or holders of a valid power of attorney for those registrants, and shall enter into a binding agreement with the CSOS CA. Subscriber applications are submitted to a CSOS

[3] Eligibility background information regarding the applicant is kept on a separate system from CSOS.

Coordinator, who are applicants that have completed a Coordinator application (Form 252). A CSOS Coordinator is responsible for the initial verification of the Subscriber's identity and authorization for a CSOS certificate and submission of the application package to the CSOS Registration Authority (RA) who is a DEA employee or contractor. CSOS Coordinator and Subscriber applications and instructions can be found at DEA's website at https://www.deaecom.gov.

CSOS Coordinator Registration Process - A notarized CSOS Coordinator or DEA Registrant application must be received along with or prior to any CSOS Power of Attorney (POA) certificate applications. Registrants and POAs applying as the CSOS Coordinator shall be given the option to receive a CSOS certificate on the CSOS Coordinator application form.

The CSOS RA must receive a CSOS Coordinator application in advance of, or concurrently with, the submission of CSOS Subscriber certificate applications. CSOS Coordinators shall submit the following information/credentials to the CSOS RA for identity verification:

- A signed and notarized CSOS Coordinator application obtained from the CSOS website at https://www.deaecom.gov containing the signature of the individual who signed the most recent application for DEA Registration or the individual authorized to sign the most recent application for DEA Registration authorizing that individual to represent the organization in the capacity of the CSOS Coordinator;

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;

- A copy of a current DEA registration certificate (Form 223) of the applicant or the most recent application for DEA registration;

- For individuals with POA to sign orders, a copy of the power of attorney form as specified in Code of Federal Regulations (CFR).

CSOS Subscriber Registration Process - Authentication of CSOS Subscriber identity shall be performed by the local organization and requires the identification of a CSOS Coordinator, who serves as the Local Registration Authority (LRA) and organizational point of contact for CSOS issues. Subscribers shall submit the following information/credentials to their designated CSOS Coordinator for identity verification:

- A CSOS Certificate application, signed by the applicant, stating that the applicant has read and understands the terms of the Certificate Policy (CP) and has agreed to the statement of Subscriber obligations that the Certification Authority provided and acknowledging acceptance of Section 843(a)(4)(A) of Title 21, United States Code, which states that any person who knowingly or intentionally furnishes false or fraudulent information in the application is subject to imprisonment for not more than four years, a fine of not more than $30,000.00 or both;

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;

- For individuals with POA to sign orders, a copy of the power of attorney form as specified in CFR.

The CSOS Coordinator shall complete Section 3 of the Subscriber's application, providing the following information in the Subscriber's packet:

- Signed Affirmation of Identity Verification in accordance with the DEA Registrant Agreement and Section 843(a)(4)(A) of Title 21, United States Code;

- The CSOS Coordinator's first and last name, signature and date signed as the individual who has performed Subscriber identity verification;

- Copies of the identification documents, application and letter assigning POA furnished by the Subscriber.

Upon receipt of the packet from the CSOS Coordinator, the CSOS RA shall validate that the application information is complete and consistent with the information received by the Registrant. All supporting documentation shall be scanned and entered into the system, including the unique identifying information from the identification documents. The CSOS RA shall also verify that the application was received from an approved CSOS Coordinator by matching the data and signatures against information in the CSA database supplied by DEA and using the previously submitted CSOS Coordinator's application data and signature.

2. Information Changes

Information changes are accomplished by the RA Operator completing one of three forms; the Coordinator Change form, the Organization Change form, or the Subscriber Update form. The Coordinator Change form applies only when a Coordinator resigns, or the Coordinator's role has changed. If the Organization's name or address has changed, the RA Operator completes the Organization Change form. The RA Operator also completes the Subscriber Update form to update Subscriber information, this includes: the Social Security number, telephone number, security code and the coordinator's business address. The system notifies the Subscriber and the Requestor that the subscriber's information has changed through e-mail notification that includes each item that was updated. The System notifies the Requestor that information has changed by e-mail notification.

3. Certificate Revocation

Where applicable, a CSA Revocation Report will be generated by the system and reviewed by a DEA Investigator. As CSA records are inserted into the CSA database, the system will determine if the DEA Registration participates in CSOS, whether the data that has changed, and inserts the changed record into the CSA Revocation Report. A 60-day notification is provided to each certificate holder of the pending revocation. The Coordinator is provided with a list of the individuals who may renew electronically and a lists of those who must re-renew via the initial enrollment procedures.

4. Certificate Renewal

PII is also handled by the system for the purpose of renewal notification. The system will automatically notify Subscribers of pending certificate expiration. The script identifies CSOS certificates that will expire 45 days from the current date, determines the method for which the certificate shall be renewed, notifies the Subscriber of the pending expiration and provides the CSOS Coordinator the information required to renew each certificate.

All information submitted to CSOS is verified against DEA's Registration database, which contains information on which companies have been approved as DEA Registrants and which controlled substances the Registrant is authorized by the DEA to handle. Employment verification is performed first through a cross-check against a commercial data aggregator's records. In the event that the aggregator provides conflicting information, or fails to find information on the individual, the employer listed on the application is directly contacted to verify employment.

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
X	Statute	Controlled Substances Act (CSA), Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970, 21 U.S.C. § 801 et seq.
	Executive Order	
X	Federal Regulation	Title 21, Code of Federal Regulations, part 1300 to the end
	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.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	C	All marked PII categories apply only to members of the public (USPER) and relate to each of the following numbered CSOS Forms: CSOS 251, 252, 253, 254
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	CSOS 251, 252, 253, 254
Tax Identification Number (TIN)			
Driver's license	X	C	CSOS 251, 252, 253
Alien registration number			
Passport number			
Mother's maiden name	X	C	CSOS 251, 252, 253
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	C	CSOS 251, 252, 253
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			

(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
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			
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			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C	CSOS 251, 252, 253
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **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	The CSOS system permits auditing only of the input actions of members of the public, not DEA access to such data.
- **User passwords/codes**			

(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
- **IP address**	X	C	The CSOS system permits auditing only of the input actions of members of the public, not DEA access to such data.
- **Date/time of access**	X	C	The CSOS system permits auditing only of the input actions of members of the public, not DEA access to such data.
- **Queries run**			
- **Content of files accessed/reviewed**			
- **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	X	Email	X		
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		Private sector	X

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		X	CSOS PII data is available only to authorized DEA employees who access that data as part of their job responsibilities and have a legitimate a need to know to that information. Further, as covered in CSOS Privacy Policy, private information will not be sold, rented, leased, or intentionally disclosed in any manner to any person without prior written consent, unless otherwise required by law, or except as may be necessary for the performance of CSOS services.
DOJ Components				
Federal entities	X			This information may be shared with a member of Congress or to a congressional staff member in response to a request from the person who is the subject of the record. This information may also be shared with federal agencies responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the DEA Diversion Control becomes aware of a violation or potential violation of civil or criminal law or regulation.

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.**
				Further, as covered in CSOS Privacy Policy - private information will not be sold, rented, leased, or intentionally disclosed in any manner to any person without prior written consent, unless otherwise required by law, or except as may be necessary for the performance of CSOS services.
State, local, tribal gov't entities	X			This information may be shared with state or local agencies along with state medical and licensing boards responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the DEA Diversion Control becomes aware of a violation or potential violation of civil or criminal law or regulation. Further, as covered in CSOS Privacy Policy - private information will not be sold, rented, leased, or intentionally disclosed in any manner to any person without prior written consent, unless otherwise required by law, or except as may be necessary for the performance of CSOS services.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				

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.**
Other (specify):				

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

Not applicable. CSOS does not share information with the public.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

General notice of the existence, contents, and uses of CSOS is provided by the publication of this PIA and the relevant SORN. The applicable SORN is JUSTICE/DEA-005, "Controlled Substances Act Registration Records (CSA)," 52 Fed. Reg. 47182, 208 (Dec. 11, 1987), 66 Fed. Reg. 8425 (Jan 31, 2001), 82 FR 24147 (May, 25 2017). In addition, before filling out CSOS applications 251, 252 and 253, subscribers must first read and agree to the following:

- CSOS Registrant Agreement (CSOS 251 and 252)
- CSOS Subscriber Agreement (CSOS 251, 252, and 253)
- CSOS Privacy Policy (CSOS 251, 252, and 253)

Further, a Privacy Policy is available on the CSOS website, available at http://www.deaecom.gov/privpol.html. The CSOS Web site is P3P-compliant to be automatically read by browsers, consistent with OMB Memorandum M-03-22.

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.

Certificate application is voluntary, and the information provided by the applicant is used solely to establish eligibility/identity for issuance of the certificate. For instance, applicants can choose not to

submit their SSN, leaving that field blank on the application, at which point a randomly generated number is issued for applicants and maintained by the CSOS Registration authority staff. Therefore, if the individual provides this information, it is assumed that they have provided positive consent to the use of this information in the manner described, including any disclosure of information as outlined in the CSOS Privacy Policy.

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.

Detailed instructions for making requests for access to records are provided on the CSOS website, in the Privacy Policy, and are located in the Certificate Practices Statement (CPS) also located on the CSOS website. Only the individual subscriber whose information pertains to them is allowed to make a request for information change except cases of Power of Attorney (POA) where the Registrant must approve the information change through a Helpdesk ticket. Information that may be reviewed includes only that information pertaining to the individual subscriber submitting the request that is maintained by the DEA in a "system of records" (a grouping of records under the control of the DEA from which information can be retrieved by means of the individual subscriber's name or an identifying number assigned to the individual subscriber).

In response to a proper request for access, CSOS will notify the requesting individual subscriber the CSOS system of records contains any records pertaining to him or her, and if so, the manner in which those records may be reviewed. [4] The following discusses how a request to amend a CSOS record is processed. Requests for an amendment must include:

a) The name of the individual subscriber requesting the amendment,
b) A description of the item or items to be amended,
c) The specific reason for the amendment,
d) The type of amendment action sought (e.g. deletion, correction or addition)
e) Copies of available documentary evidence supporting the request.

The individual can also call the CSOS Help Desk at 1-877-DEAECOM for assistance.

DEA maintains a record of each request for amendment that it receives, including the date and time the request was received, the name of the record, and information provided in support of the request. DEA will provide to the requesting individual subscriber written or e-mail acknowledgment of the receipt of his/her request for amendment within ten (10) working days of the dale of receipt of that request. DEA will also notify the CSOS CA of the receipt of a request for amendment of a record, in writing or by e-mail, within ten (10) working days of the date of receipt of that request. A copy of the

[4] However, Controlled Substance Act Registration Records under SORN Justice/DEA-005 are subject to an exemption from certain Privacy Act access rights under 5 U.S.C. 552a(k) pursuant to regulation 28 C.F.R. § 16.98 (a)-(b), to the extent requests involve investigatory material compiled for law enforcement purposes.

acknowledgment and the notice to the CSOS CA will be made a part of the record of the request for amendment.

DEA will make any appropriate corrections to any record or portion thereof that are required to ensure that the record is accurate, relevant, timely, and/or complete within twenty (20) working days of the date of receipt of a request for amendment of that record. A copy of the corrections made, if any, will be made a part of the record of the request for amendment and a copy of which will be forwarded to the CSOS RA. Written or e-mail notification of the correction will also be provided to a person or agency to whom that record was previously disclosed, and a copy of that notification will be made a part of the record. CSOS will notify the individual Subscriber making the request in writing or by e-mail of any amendments that are made to the record. A copy of the notification will be made a part of the record of the request for amendment.

Lastly, the Freedom of Information Act (FOIA) and/or Privacy Act (PA) is available as well.[5] DEA's public facing website contains a FOIA/PA webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The FOIA/PA website also contains procedures for filing a request for record correction or amendment to DEA. Further, the CSOS website allows the user to automatically evaluate information for consistency to their browser settings, as well as review the privacy policy, if they choose to do so at that time.

Section 6: 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).

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):** An Approval to Operate was issued on 4/14/23. at date of submission. **If an ATO has not been completed, but is underway, provide status or expected completion date:**
	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: There are no POAMs related to privacy controls.

[5] See https://www.dea.gov/foia.

	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:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** CSOS is system with FIPS 199 categorization of Moderate. CSOS physically controls and securely stores information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media. CSOS protects information system media until the media are destroyed or sanitized using approved equipment, techniques and procedures. CSOS protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled. The SSP specifies the approved release procedure for the media of a given system. For Medium and High systems, storage media is physically controlled and safeguarded in the manner prescribed for the most-sensitive designation, or highest classification level, and category of data ever recorded on it until destroyed or sanitized using approved procedures. National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev 5), Security and Privacy Controls for Information Systems and Organizations are reviewed on an Annual Basis and have been assessed and validated. CSOS received an Approval to Operate on 4/14/23 via a formal memorandum approving the security and privacy plan and authorizing the system to operate for a specified period of time.
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 Security Information and Event Management (SIEM) tool[6] forwards collected logs for further evaluation and review by separate DEA security group.

[6] A SIEM tool provides the ability to gather security data from information system components and present that data as actionable information via a single interface. See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf.

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 privacy training specific to this system is required.

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***

CSOS has the following key privacy and security administrative, technical, or physical controls:

- Authentication controls. An unauthorized user would have to have knowledge of both userID/password combinations in order to gain access to the system. A process also exists for both user provisioning and cancellation of accounts in a timely fashion.

- Role-based access controls. Access to specific data is restricted by user classification as well as by membership in specific enforcement groups. This enforces access control of information with privacy implications to members of an enforcement group and their supervisors. Additionally, the detail level of the information available is limited by the user classification.

- Auditing. Auditing is activated for the database to track the user logs.

- Annual system self-assessments that verify and validate that the appropriate security measures are being effectively deployed.

CSOS is categorized at a MODERATE level of security assurance according to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Accordingly, the following NIST 800-53[7] security and privacy controls are applied to CSOS in order to protect privacy and reduce the risk of unauthorized access and disclosure:

[7] NIST 800-53, Revision 5, can be found here: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

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: (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.	In order to access CSOS, 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 CSOS applications online receive notices regarding authorized information use, privacy accommodations, and references to applicable laws regarding the collection of data. The privacy policy for CSOS can be viewed here: https://www.deaecom.gov/privpol.html

NIST 800-53 Control Number	Requirement	Implementation
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 e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	TGD designates a Content Manager who is responsible for reviewing and posting updates to the publicly accessible portions of CSOS. The Content Manager performs periodic reviews of content posted to the publicly accessible portions of CSOS 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.
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).	Non-organization personnel have no direct, persistent access to CSOS data. Non-organizational access to CSOS data must be in compliance with the stipulations in section 4.2 of the CSOS PIA.
PL-5 Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The CSOS PIA complies with guidance in OMB Memorandum M-03-22.

NIST 800-53 Control Number	Requirement	Implementation
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 new threats and vulnerabilities), or other conditions that may impact the security state of the system	Risk Assessments are conducted annually at minimum on TGD-managed systems, including CSOS. These assessments are documented, reviewed and approved by organizational management. Deviations from security controls are documented and reviewed quarterly at minimum, until resolved.

Additionally, the Operations Manual describes the controlled procedures for creating a new employee account and assigning them to an approved role. All new account actions on the system must have the written approval of the Program Manager and Section Chief. Account management actions including the actual assignments of roles and rules are verified according to established security and auditing procedures. Account management actions and monitored by the System Administration Team on a daily basis to ensure that unauthorized users are not added to the system, or permissions elevated to provide existing users with unauthorized levels of access. Role separation is an inherent feature of any government PKI and, as such, processes that ensure this role separation and account creation integrity are audited by an external entity.

Privacy Risk: The system may be compromised without sufficient and robust physical, technical, and administrative privacy and security controls for handling and protecting PII.

Mitigation: This risk in mitigated: As detailed above, there are several types of security and privacy controls active on the CSOS. Role-based access controls are being utilized to reduce the risk of unauthorized access and disclosure. The Operations staff are authorized to maintain the system and is divided into five groups with each group having distinct responsibilities. It includes the following management positions: Operations Manager, CA Manager, Registration Authority (RA) Manager, Help Desk Manager, System Security Manager, and System Administration Manager. Each group includes supporting staff.

Only RA staff have access to the Subscriber information in the RA database. RA staff has read and write access, however the majority of data entry is performed by a scripted workflow process that reduces the number of personnel that have to handle the record, as well as reduces the likelihood of data entry errors.

The Engineering staff has access to the system in order to support development of system solutions and include an Engineering Manager, several team leaders, and engineers. External businesses who do not access the system directly but who use CSOS certificates or access CSOS certificate information include those who conduct transactions using prescriptions, such as hospitals, medical practitioners, pharmacies, and narcotic treatment programs. External users also include controlled substance manufactures, distributors, teaching institutions, exporters, and pharmacies. DEA contractors will have access to the system.

The Internet connection for CSOS is essential, and is protected by routers, firewalls, and intrusion prevention systems. Secure Sockets Layer (SSL) encryption[8] is implemented to secure data in transit. No remote connections exist within CSOS and are expressly prohibited as documented in the system security plan. Careful consideration was also given to the design of the procedures by which the data would be processed.

System records are safeguarded in accordance with the requirements of OMB Circular A-130, Appendices I and III and Sections 2.8 and 5 of the CSOS Certificate Practices Statement (CPS) located at www.deaecom.gov/csos_cps.pdf. Technical, administrative, and personnel security measures include procedural and access controls to limit accessibility to data, storage in secure DEA space, disposal performed under two-person control, and comprehensive staff training on the procedures for handling sensitive information.

The privacy of user information stored in the private network's database is protected from vulnerability by multiple technical controls in the operating system, routers, firewalls, and intrusion detection systems. All systems that handle data in identifiable form are marked, and the original documentation stored in a secured container with limited access. Data backups are marked with data indicators, and transported under multi-person control to a secured facility for archiving.

CSOS implements Data at Rest encryption protection, requiring one or more of the following: 1. confidentiality protection; and/or 2. integrity protection. The information system implements the protection of the: 1. confidentiality of organization-defined information at rest; and 2. integrity of organization-defined information at rest.

Privacy Risk: Monitoring, testing and evaluation of privacy and security controls may be insufficient or too infrequent.

---

[8] SSL provides privacy and data integrity between two communicating applications, see https://csrc.nist.gov/glossary/term/secure_sockets_layer.

Mitigation: This risk is mitigated. As noted in the table at 6.1, 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 in real time using Qualys – vulnerability scanning tool. Staff review system reports and review security findings. Findings are mitigated in accordance by the DOJ Vulnerability Management Plan (VMP).

Privacy Risk: DEA may not appropriately audit, document, and review compliance of its PII rules on this system.

Mitigation: This risk is mitigated. The CSOS system is subject to auditing to ensure integrity and compliance.

Additionally, Group Policy Objects (GPOs) are established to log all actions performed by a System Administrator at the CSOS system, including all account management actions. Administrators do not have access into the RA database. GPOs also are set to notify on attempted access to protected folders by unauthorized users. GPOs are set to reapply themselves on a regular basis to ensure that an Administrator does not change the settings. All logs containing System Administrator actions are stored on a protected log server that requires two-person control for the removal of the logs onto tamper evident media that is then reviewed each day by the Security Officer to ensure that the proper documentation accompanies any changes to user roles or additions of personnel to the system.

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.)

Paper data is retained for three (3) months, and then disposed of in regulation burn bins. The retention of digital data included in CSOS is 10 years/6 months. The records are scheduled under NARA retention schedule N1-170-04-7.

Section 7: Privacy Act

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

_____ No. ___X__ Yes.

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

JUSTICE/DEA-005, "Controlled Substances Act Registration Records (CSA)," 52 Fed. Reg. 47182, 208 (Dec. 11, 1987), 66 Fed. Reg. 8425 (Jan 31, 2001), 82 Fed. Reg. 24147 (May, 25 2017).

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: Risk of aggregated data facilitating identity theft or diversion. All of the information collected and contained within the digital certificate, with the exception of the individual's SSN, is considered "public" information. Even so, DEA recognizes that the aggregation of this information in an electronic public repository, as is the case with most digital certificate issuing authorities (CAs), presents an increased risk to Subscriber identity theft as well as to the diversion of controlled substances.

Mitigation. This risk is mitigated because DEA has chosen not to publish copies of digital certificates in their public repository. While this process increases the burden for individuals who accept digitally signed transactions (necessitating that the Subscriber exchange the certificate with their trading partner in advance of the transactions), it serves to prevent identity aggregation.

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

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 because the privacy of Subscriber 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, two-person control at sensitive servers and logs, were all designed into the system. The network design has also been enhanced to defend the privacy of this subscriber data; the subscriber 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; even paper submitted by applicants is kept under lock and key for up to three (3) months until it is destroyed. Personnel who access the sensitive data do so in a secluded section of the secure area. These personnel maintain additional privacy practices at their workstations, and lock their workstations and paperwork when out of their own area. All users of the system are prohibited from copying sensitive data to laptops or other mobile hardware.

Additionally, an independent Auditor conducts an annual Compliance Audit on CSOS using the Federal PKI Compliance Audit Guidelines. The Auditor reviews CSOS policies and practices to identify material weaknesses. Annual Compliance Audit activities involve verifying DEA CSOS operations are consistent with those stated in the Certification Practice Statement (CPS) and are consistent with industry "best practices" and government requirements. Additionally, as part of the C&A of CSOS, DEA Cybersecurity Services (TCV) personnel assess whether CSOS complies with DOJ/DEA security requirements, NIST SP 800-53 controls, and regulations in accordance with the Federal Information Security Management Act (FISMA), as well as best security practices.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: There is a risk of unauthorized disclosure stemming from Information Sharing of data in CSOS.

Mitigation: This risk is mitigated because Subscriber information from this system may only be disclosed to the following parties, via mail:

- Federal, state or local agencies along with state medical and licensing boards responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order when the Diversion Control Division (DC) becomes aware of a violation or potential violation of civil or criminal law or regulation.
- A member of Congress or to a congressional staff member in response to a request from the person who is the subject of the record.
- A DEA employee, an expert consultant, or contractor of DEA in the performance of a federal duty to which the information is relevant.
- Persons registered under the Controlled Substances Act (P.L. 91-513) for the purpose of verifying the registration of customers and practitioners.

Further, system personnel undergo annual privacy, contingency and incident response, and cyber-security training.

Privacy Risk: Unauthorized disclosure of the SSN that might lead to identity theft.

Mitigation: To mitigate this risk, CSOS implements specific access controls to limit the handling of the applications containing the SSN, as well as strong access controls on the database in which the SSN is stored. Data at rest encryption is implemented on the Registration database containing User personal information (e.g., SSN) to prevent unauthorized disclosure or modification. The database is not accessible outside of the DEA facility and the paper applications are stored in a locked cabinet in a secured area inside the DEA facility, which is itself secured by card or biometric physical-access controls. The applications are shredded under two-person control during disposal. Personnel are trained not to disclose the SSN, even during telephone conversations with the Subscriber and the digital certificate does not contain the SSN.