Privacy Impact Assessment
for the

DEA Diversion Control

Controlled Substances Ordering System (CSOS)

August 31, 2006

Contact Point
Drug Enforcement Administration
Office of Diversion Control
202-307-1000

Reviewing Official
Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

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 legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. The DEA, Office of Diversion, E-commerce Section, operates the Controlled Substance Ordering System (CSOS) whose purpose is to issue and revoke digital signatures to DEA Registrants (manufactures, distributors, and pharmacies who order controlled substances) to digitally sign electronic orders for controlled substances. To this end, this system 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, electronic files ("digital certificates") are generated by the system and downloaded by the applicant (a "Subscriber"). These certificates contain only public information and are exchanged between trading partners in business-to-business transactions and are 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.

Section 1.0
The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

CSOS digital certificate applications are received by the DEA. These applications are paper-based and are not transmitted electronically. The data received in the applications include:

1) The applicant's name;
2) Business address;
3) Approved drug schedules;
4) Company's DEA registration number;
5) Business telephone number;
6) Business e-mail address;
7) Social Security Number;
8) A copy of a Government issued photo ID;
9) An identifier selected by the applicant;
10) A copy of the DEA registration; and

11) A copy of powers of attorney granting signing authorization for the registrant, if applicable.

1.2 From whom is the information collected?

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 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 2.0
The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The DEA requests specific and sufficient identity information to confirm the identity and ordering authority of the applicant. The information collected is equivalent to what is already being collected as a part of the initial (manual) registration process that must occur prior to the digital certificate enrollment process.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The Controlled Substances Act (CSA), Title II of the Comprehensive Drug Abuse Prevention and Control Act of 1970 authorizes the DEA to collect this information.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The following risks were identified with respect to privacy and the information collected:

1. **Risk to unauthorized disclosure of the Subscriber's SSN.** DEA identified a risk of unauthorized disclosure of the SSN that might lead to identity theft. 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. 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.

2. **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 (Certificate Authorities, or, CAs), presents an increased risk to Subscriber identity theft, as well as to the diversion of controlled substances. To mitigate this risk, 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.

Section 3.0
Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The information collected is used to establish the eligibility and identity of the applicant for a DEA CSOS digital certificate.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No, the system is not used to perform data analysis or data mining. No information is added to the applicant's DEA Registration information.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The information 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.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Under requirements established by the Federal Bridge Certification Authority (FBCA's) Policy Authority that governs government public key infrastructures (PKIs), the data is retained for a minimum period of 10 years, 6 months. The National Archives and Records Administration (NARA) has approved CSOS' retention schedule.

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

System records are safeguarded in accordance with the requirements of the Privacy Act of 1974, 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 a secured facility, disposal performed under two-person control, and comprehensive training on the procedures for handling sensitive information is provided to staff. 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 personally identifiable data, as defined under the Privacy Act, are marked and the original documentation is stored in a safe with limited access. Data backups are marked with Privacy Act data indicators and are transported under multi-person control to a secured-facility for archival. An authorized accrediting firm accredits the system using the Webtrust for Certification Authorities (CA) criteria. Accreditation has been performed to certify that these practices are handled in accordance with those stated in the CPS and are consistent with industry "best practices" and government requirements.

Section 4.0
Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

CSOS data is not shared with other internal components of the Department.

4.2 For each recipient component or office, what information is shared and for what purpose?

Not applicable, CSOS does not share information with other Agency components.

4.3 How is the information transmitted or disclosed?

Not applicable.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Not applicable.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

CSOS does not share information with external recipients.

5.2 What information is shared and for what purpose?

Not applicable.

5.3 How is the information transmitted or disclosed?

Not applicable.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Not applicable. CSOS does not share data.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

Not applicable. CSOS does not share data.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Not applicable. CSOS does not share data.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Not applicable. CSOS does not share data.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

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

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes, applicants are provided the opportunity to decline providing the information prior to submitting their application. Additionally the P3P-compliant policy at the site 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.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Applicants can choose not to submit their SSN, leaving that field blank on the application, at which point a made-up number is assigned.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

No additional risks, other than those already addressed, were identified.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Only the individual subscriber whose information pertains to them is allowed to make a request for information change except cases of POAs where the Registrant must approve the information change. 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 system of records is 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.

Detailed instructions for making requests for access to records are provided on the CSOS website. In response to a proper request for access, CSOS will notify the requesting individual subscriber whether

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.

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), and

e) Copies of available documentary evidence supporting the request.

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 date 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 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 within (10) days to any 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.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

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.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

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

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The individual supplies the information collected for the database, therefore, the individual may contest information through the same process as described above to amend inaccurate information.

Section 8.0
Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The Operations staff is 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 as well. 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 manufacturers, distributors, teaching institutions, exporters, and pharmacies.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Yes. (Appendix B includes the contractors' Statement of Work (SOW)).

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, 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.

8.4 What procedures are in place to determine which users may access the system and are they documented?

An 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 Operations Manager and the Security Officer.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Account management actions are monitored by the Security Officers 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.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

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 logical 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.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

New user training is provided to new employees based on their role. This training addresses all of the policy requirements associated with the CSOS system – including a section of training that addresses handling private Subscriber information.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. The last C&A was performed August 2005.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Threat: Unauthorized Access to the system

Risk: Low

Mitigation / Countermeasures:

Authentication controls. An unauthorized user would have to have knowledge of both userid/password combinations in order to gain access to the system.

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 is activated for the database to track the user logs.

A process exists for both user provisioning and cancellation of accounts in a timely fashion.

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

Threat: Unauthorized Disclosure of Reports Print-Out

Risk: Low

Mitigation / Countermeasures:

Reports can only be printed out by authorized users. Authorized users have accepted rules of behavior which include the proper handling of sensitive DEA paperwork and SBU data, whether it is a physical printout or access to the system.

Section 9.0
Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Primary system goals included an increase in speed of transaction times, lower costs per transaction, and greater electronic security. The electronic security services include authentication of sending party, integrity of communications and legal strength non-repudiation. At the time of development of the system, an extensive survey was performed of competing technologies that could meet these requirements; however there were no technologies that could compete with PKI in providing the required levels of functionality and security. DEA continues to assess new technologies that may achieve system goals as they are developed.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

A five-pronged methodology was used in conducting the original analysis. First, interviews were conducted with selected DEA and industry representatives. Then a review was conducted of documents recommended by DEA and industry. Next, visits to sites recommended by DEA and Industry were scheduled and conducted. Then there was follow-up of the leads and sources developed during the first three efforts, and finally questionnaires were submitted to selected industry representatives. Analysis of all this information identified the integrity, privacy, and security requirements of the proposed system.

The results of this analysis were posted to a product-specific website and presented at industry meetings before final adoption.

9.3 What design choices were made to enhance privacy?

The privacy of Subscriber data is dependant 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, a camera that records administrator actions, 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 Internet connection is essential and is protected by routers, firewalls, and intrusion detection systems; but wireless connectivity and remote connectivity are expressly forbidden in the system security plan.

Careful consideration was also given to the design of the procedures by which the data would be processed. 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 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.

Conclusion

Privacy of sensitive data has been a primary concern for both DEA and industry since the idea for the system was first conceived. As stated previously, DEA and industry worked together at inception to identify privacy requirements for the system, and those principles have been implemented throughout the system. The system's PKI technology, as well as the hardware and software that implements it, was selected because it offered the best opportunity to achieve the goals of electronic data privacy and security. The designs of both the network containing sensitive data and the procedures for handling the data have been optimized to protect data privacy and security. Changes to the system are managed and approved on a scheduled basis in order to maintain an optimal privacy and security posture for the system. Personnel have been screened to reduce the likelihood of insider compromise. Privacy risks have been identified in the formal risk assessment process required for certification as well as in the annual OMB business case analysis. Risks that are identified during these processes are mitigated and reported; new risks are added as old risks are mitigated, and strategies to reduce or mitigate risks are reviewed and updated on a regular basis. The managerial, personnel, and technical controls interoperate to ensure the highest possible level of support is achieved for the privacy of the data contained in the system.

Responsible Officials

_____/s/_____<<Signature>> _____<<Date>>

Richard W. Sanders
Assistant Administrator
Chief Privacy Officer
Drug Enforcement Administration

_____/s/_____<<Signature>> _____<<Date>>

Wendy H. Goggin
Chief Counsel
Chief Privacy Official
Drug Enforcement Administration

Approval Signature Page

_____/s/_____<<Signature>> _____<<Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice