Privacy Impact Assessment
for the

EPIC Seizure System (ESS)

August 4, 2006

Contact Point
El Paso Intelligence Center
Information Management Systems
Drug Enforcement Administration
915-760-2000

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

DEA PRIVACY IMPACT ASSESSMENT

Part One: Is a PIA required?

Instructions for Questions 1-4: If you answer "yes" to any of Questions 1-3 and Question 4, go on to the next question. If you answer "no" to all of Questions 1-4, please briefly describe the IT system that is at issue, and submit this document for review under the PIA process.

1. Are you developing or procuring a new IT system or project that collects, maintains, or disseminates information:

   a. about U.S. citizens or aliens lawfully admitted for permanent residence; and
   b. that does NOT pertain only to government employees or contractors?
   Yes.

2. Are you initiating a new electronic collection of information under the Paperwork Reduction Act?[1]
   No.

3. Are you making a change to an existing IT system that creates new privacy risks? For example:

   a. Are you applying a new technology to an existing system that significantly changes how information is managed in the system?
   Yes.

   b. Are you making a change in business processes:

      i. that merges, centralizes, matches or otherwise significantly manipulates existing databases?
      No.

      ii. that results in significant new uses or disclosures of information or incorporation into the system of additional information?
      No.

   c. If this information has been collected previously:

      i. Are new or significantly larger groups of people being impacted?

[1] This includes new electronic collections of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government). See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.

No. DEA is not collecting new data about additional people.

ii. Is new data being added resulting in new privacy concerns?
No.

iii. Is data being added from a commercial or public source?
Yes.

4. Is this information individually identifiable? (Does this pertain to specific individuals who can be identified either directly or in conjunction with other data?) If no, submit this document for review under the PIA process. If yes, continue to the next question.
Yes.

Instructions for Questions 5-6: If you answer "yes" to any of Questions 5-6, submit the required documentation for review under the PIA process. If you answer "no" to a question, continue on to the next question.

5. Has a PIA or similar evaluation been conducted? If yes, does the existing PIA address the questions in Part Two? If yes, submit the existing PIA with this document for review under the PIA process. If no, continue to the next question.
Yes. An evaluation was conducted for the prior system, Pathfinder, on which the ESS is based, but it does not address the questions in Part Two.

6. Is this a national security system as defined at 40 U.S.C. 11103? If yes, please attach verification and submit this document for review under the PIA process. If no, continue to Part Two.
No.

Part Two: Preliminary PIA (Routine database systems)

1. Please provide a general description of the system, including the purpose of the system.
The El Paso Intelligence Center Seizure System (ESS) is a data collection system that incorporates two previous systems, the Clandestine Laboratory Seizure System (system notice Justice/DEA-002) and the Automated Intelligence Records System (Pathfinder) (system notice Justice/DEA-INS-111) for the purpose of combining both previously existing systems into a single collection of records.

The principal purpose of the ESS is to ensure that law enforcement entities can more effectively investigate, disrupt and deter criminal activities by providing authorized law enforcement personnel access to data maintained in this system by means of a secure Internet connection. The ESS provides a single point of entry to vetted users to submit a request for information from relevant data sources available to the ESS. Results obtained through a search of ESS databases are provided in near real time to the user.

The ESS data collection contains drug, alien, weapons and other criminal law enforcement information. The information contained in this system consists of sensitive but unclassified law enforcement data collected and produced by the following agencies: the El Paso Intelligence Center (EPIC); the Department of Homeland Security (DHS); the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the Federal Aviation Administration (FAA); the Federal Bureau of Prisons (BOP); the United States Marshals Service (USMS); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); and public and other information obtained from commercial databases.

The system also contains sensitive but unclassified criminal law enforcement information submitted by federal, state and local law enforcement officers concerning drug, currency, firearms trafficking, and alien smuggling records associated with drug-related and other criminal activities.

Records consist of suspect and tracking files on people, vessels, aircraft, organizations, and vehicles and include identifying information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). The system also consists of audit logs that contain information regarding queries made of the system.

2. Volume of records that will be stored in the system.
Estimated Total Number of Records as of August 1, 2006 is 270,000.

Possible number of persons impacted is approximately 270,000 at this time. Many of the records might duplicate information or consist of multiple entries about individuals, and all records do not necessarily contain references to individuals.

The number of records is expected to increase, and the number of individuals who will be impacted will increase as well.

4. What is the purpose for which the system data will be used, including how it will be used and who will use it?
The system data is provided to vetted law enforcement users for the purpose of identifying previous criminal offenses, identifying individuals subject to the criminal justice process, or conducting counter-drug, criminal or intelligence investigations in order to provide investigative information for the DEA, and other law enforcement agencies, in the discharge of their law enforcement duties and responsibilities.

Each participating source data agency will contribute information to ESS. Additional contributing agencies to the ESS may be added at a later time. Federal, state, local, tribal and foreign law enforcement entities will use ESS to make queries of structured and unstructured data.

5. What are the sources of the information?

ESS data sources consist of the following systems:

- **DEA/EPIC's National Seizure System;**
- **DEA's Narcotics and Dangerous Drugs Information System (NADDIS);**
- **BOP's SENTRY;**
- **DHS's Treasury Enforcement Communication System (TECS II), Central Index System (CIS), and Merchant Mariner Lookout Log (MMLL);**
- **FAA's Aircraft Registry and Airman Certification System (ARS); and**
- **Western States Information Network (WSIN).**

Additional contributing law enforcement agencies may be approved in the future.

Other data sources are (1) DEA intelligence and investigative records; (2) reports, investigative and intelligence reports from other participating and associated federal and state member agencies; and (3) records and reports of foreign law enforcement and regulatory agencies.

Third party data sources include public and non-public data sources (e.g., commercial databases).

6. With whom will the information be shared outside of the Department?

Information from ESS may be disclosed:

(1) To federal, state, local, tribal and foreign law enforcement agencies to facilitate the investigation and prosecution of illegal drug trafficking activities general law enforcement individuals and agencies;

(2) To law enforcement individuals and organizations in the course of investigations where necessary to elicit information pertinent to counter-drug, counter-terrorism, weapons, alien, and drug-money investigations;

(3) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function related to this system of records;

(4) To a former employee of the Department for purposes of: responding to an official inquiry by a federal, state, or local government entity or professional licensing authority in accordance with applicable regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility;

(5) To the news media and the complying with 28 CFR 50.2 when applicable, unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy;

(6) To any criminal, civil, or regulatory law enforcement authority whether federal, state, local, territorial, tribal, or foreign where the information is relevant to the recipient entity's law enforcement responsibilities;

(7) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record;

(8) To the National Archives and Records Administration (NARA) for purposes of management inspections conducted under the authority of 44 U.S.C. 2904 and 2906; and,

(9) In an appropriate proceeding before a court or administrative or regulatory body when records are determined by the Department of Justice to be arguably relevant to the proceeding.

(10) To agencies of the U.S. Intelligence Community.

7. Is providing information voluntary by the individuals? If yes, are individuals informed that they may decline to provide information?
No. The information pertaining to individuals is based on their suspected involvement with illegal drug trafficking activities, criminal case investigations or other law enforcement concerns.

8. Do individuals have an opportunity to consent to particular uses of the information? If yes, how can individuals grant consent?
No. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data that was lawfully gathered and maintained based on law enforcement authority and individuals may not have an opportunity to consent to particular uses of that information.

9. How will the information be secured (e.g., administrative and technological controls)?
Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including DEA's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only personnel who maintain the system and other users who are members of law enforcement agencies and who have undergone background and criminal history checks will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their duties.

Several administrative and technological controls secure the information contained within ESS. The Security Administrator, the System Administrator, and the User Access Manager are three major components of the ESS administration. The Security Administrators are responsible for viewing, monitoring, and archiving security logs and audit trails. The System Administrators are responsible for the maintenance and operation of the system as a whole, including backing up the system and its recovery. The User Access Managers are responsible for adding, changing, or deleting users and their system access privileges. The determination of appropriate users and assignment of passwords are other administrative controls in place.

The ESS repository is physically protected in compliance with Department of Justice guidelines for Information Technology Security (DOJ 2640.2E) pertaining to both physical and environmental security. Hardware and electronic media used in the ESS is protected in accordance with the sensitivity of the data, which the system is authorized to process, store, or transmit.

ESS is also protected by boundary protection devices (e.g., firewalls) at identified points of interface with networks or systems (e.g., ADNET). The ESS also employs virus protection software and encryption technology during transmission to ensure data security.

10. Is this information covered by a Privacy Act System of Records Notice? If yes, provide the Federal Register Citation. If not, is one being created?
Yes. Federal Register, Volume 71, No. 122, June 26, 2006, 36362-36364.

11. Is this information covered by a Computer Matching Agreement? If yes, please attach.
No.

12. Is this a Major Information System as defined in OMB Circular A-130 and A-11 (Section 300-4). If yes, please include identifying information and complete Part Three.
Yes. As defined, a "Major information system" embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, or its (v) significant role in the administration of an agency's programs, finances, property or other resources.

The ESS requires special management and attention because of its importance to the agency mission since ESS supports the law enforcement information sharing strategy and mission of the DOJ.

13. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

Information in ESS is discloseable only in accordance with federal law, including the Freedom of Information Act and the Privacy Act.

User limitations were created to ensure that ESS is used for law enforcement purposes only, and only law enforcement individuals with a "need to know" the information contained within the system will have access to the ESS. All applicants for ESS must either have a background check on file with their agency or must undergo a background check. In addition, the above-mentioned security controls, both administrative and technological, controls were developed and implemented in order to reduce the risk of unauthorized access to the data.

14. Is this system of such significance or sensitivity (i.e., medical records, taxpayer information, etc.), or is the impact on privacy such that the system requires special consideration of privacy risks? If yes, please briefly explain and complete Part Three.

Yes. ESS will contain information lawfully collected and maintained as a result of criminal law enforcement investigations. These records may include sensitive personal information regarding a person's possible involvement in criminal activity.

Part Three: Further Analysis (Major Information Systems, etc.)

1. Please briefly describe the impact on privacy.

The ESS will contain a range of information about U.S. citizens, non-U.S. citizens and other persons who are referred to in criminal investigations or matters of concern to the contributing source data agencies. Examples of information in the system include: suspected criminal activity, financial records, medical records, and other personal information (i.e. address, phone, social security number, etc.). All of this information will be shared internally within DOJ and externally with other federal, state, local, tribal and foreign law enforcement authorities. This information has already been lawfully collected as part of law enforcement activities. The ESS will assist in disseminating the information to other law enforcement agencies for the purpose of improving the enforcement of U.S. laws.

If an investigator or analyst determines that the information in ESS may be relevant to an investigation, he/she may request permission from the contributing agency to utilize the information.

Due to the volume of records and the type of information being shared, privacy rights' of individuals could be impacted if the system is misused or unauthorized persons gain access. The impact on the privacy of individuals, however, will be the same as the impact of any current case analysis and investigation that includes the same data obtained from the source law enforcement agencies.

2. Please describe the alternatives to design, collection, and handling of the information that would have a lesser impact on privacy and the rationale for not selecting each such alternative, as well as the final decision.

There are two possible alternatives to handling of this information that would have lesser impact on the privacy of individuals. The first would be to not create a system like ESS. Based on the needs of the law enforcement community to share investigative information in order to protect citizens from criminal and terrorist activity, this is not a practical alternative.

The second alternative would be to create a system that provides the similar functionality for use by EPIC internal personnel only and not provide the data electronically to authorized external law enforcement agents. This would mean maintaining the current protocol of having authorized law enforcement personnel contact EPIC directly with their requests for information. EPIC would continue to provide information from available databases to the requester.

However, because speed is often an important element in apprehending a criminal or preventing a criminal act, the second alternative limits EPIC's ability to respond to an increasing volume of authorized law enforcement agents' requests for information and may limit law enforcement's ability to effectively combat crime. In order to expedite the information sharing process across varying federal, state, local, tribal law enforcement entities and effectively investigate criminal activity, it is necessary to create a system such as ESS.

3. What measures are in place to mitigate identified risks?

Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including DEA's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Only personnel who maintain the system and other users who are members of law enforcement agencies have undergone background checks will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their duties.

DEA has implemented administrative and technological security controls and measures to protect the information collected by the government, both while in storage and in transit. These measures are designed to thwart unauthorized access and inappropriate disclosure. Other administrative and technological controls are described in more detail in Part Two, Question 9.

ESS includes robust audit capabilities. ESS security staff will periodically review the audit logs to ensure appropriate access to and use of information.

The MOUs between DEA/EPIC and other law enforcement entities external to DEA outline policies and procedures for the handling of information. The policies and procedures cover the actions of source data agencies (e.g., data accuracy), as well as how recipients can use the shared data.

The MOUs that enable the use of ESS also include sanctions for misuse of the system and/or data. Sanctions can be applied to an individual or an entire agency, depending on the circumstances and severity of the misuse.

4. How will data be collected from sources other than Department records and individuals and be verified for accuracy?
   Source data agencies have the duty, sole responsibility, and accountability to make reasonable efforts to ensure that information in ESS is accurate, complete, timely, and relevant.

   Each agency is responsible for ensuring and verifying the accuracy of the information it is providing to the ESS. Designated individuals within the source data agency verify the information within that particular agency.

5. How will data be checked for completeness?
   The information will be checked for completeness by the source data agency during its reviews.

6. Is the data current? How do you know?

   Yes. Each contributing agency is responsible for ensuring that all of their incoming information to ESS is current. Each agency is also responsible for updating their system data records as new information becomes available.

7. Are the data elements described in detail and documented? If yes, what is the name of the document? If not, please do so.
   Yes. Data elements are described in the document "NSS 2.0 Datadictionary 010306.doc". Additional documentation will be available as the system continues to evolve.

8. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
   Information in this system is safeguarded in accordance with applicable laws, rules, and policies, including DEA's automated systems security and access policies. Records and technical equipment are maintained in buildings with restricted access. Passwords, password protection identification features, and other system protection methods also restrict access to information in this system. Other administrative and technological controls are described in more detail in Part Two, Question 9.

Only users who are members of law enforcement agencies, who have undergone background checks will be permitted access to the system; and such access is limited to those who have an official need for access in order to perform their professional duties.

All individuals working on the design, development, or deployment of the ESS will have personnel security clearances commensurate with the level of information stored in the repository.

The MOUs that enable the use of ESS also include sanctions for misuse of the system and/or data. Sanctions can be applied to an individual or an entire agency, depending on the circumstances and severity of the misuse.

9. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Please explain. **Not applicable.**

10. How will the data be retrieved? Can it be retrieved by a personal identifier? If yes, explain.

    Data will be retrieved from ESS based on a user making a query of particular information and the system providing a response containing the requested information. Records can be retrieved by the name and/or other identifier(s) of the individual.

11. What are the potential effects on the due process rights of individuals of: consolidation and linkage of files and systems; derivation of data; accelerated information processing and decision making; use of new technologies?

    The development and use of ESS does not adversely impact the due process rights of individuals. Law enforcement agencies have always been able to share information with other law enforcement agencies as appropriate. ESS facilitates this sharing and makes it more efficient by consolidating access through a single point of entry. The use of data conducted by investigators does not change. Investigators and law enforcement authorities will use the information to investigate and potentially prosecute any criminal suspects. If an investigator or analyst determines that the information developed as a result of a query is relevant to an investigation, the information can be used to assist with an investigation. As individuals have no right to prevent the appropriate sharing of information between law enforcement agencies, the use of ESS does not impact the due process rights of individuals.

    Because the data in the system will be made available to a larger group of law enforcement officers, officers who formerly had minimal access to sensitive law enforcement information originating from other law enforcement agencies may now have access to the information quickly and easily. The impact on the privacy of individuals, however, will be the same as the impact of any current case analysis and investigation that includes the same data obtained manually from other law enforcement agencies. Any possible implication on an individual's due process rights

would occur as a result of a criminal prosecution and procedures, not as a result of the ability to query the data in ESS.

12. How are negative effects to be mitigated? **This is not applicable. DEA has determined that there is no adverse impact on the due process rights of individuals caused by the operation and use of the ESS system.**

13. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)? **DEA will restrict access to ESS to authorized law enforcement personnel with a need for access such as supervisors, law enforcement agents/officers, and task force members associated with agencies that have signed the MOU. In addition, limited access to ESS will be provided to system administration and system security personnel for purposes of conducting system operation and maintenance tasks. All such personnel (either government employees or contractors/subcontractors) shall be vetted and cleared for system access and their access shall be monitored and audited.**

14. How will the determination be made as to who will have access to the data?
The Director of EPIC will determine who can have access to information in the ESS.

Access to ESS data by system administrators and/or system security officers will be limited to only that needed to perform these functions and will be documented in the MOU regarding ESS.

15. Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes. Criteria, procedures, controls and responsibilities are documented in the MOUs between DEA/EPIC and other law enforcement entities and in ESS security documentation.

16. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access? **ESS has an audit capability that will log the date, time, subject, and originating account of all user queries. These audit logs are kept for five years, and the ESS security staff is responsible for reviewing them.**

Users will also be notified of potential sanctions for misuse of the system or any data obtained from the system.

17. Do other systems share data or have access to data in this system? If yes, explain.
Yes. Other systems share data with this system. See response in Part Two Question Five.

18. Who will be responsible for protecting the privacy interests of individuals affected by the interface?

All users and the participating agencies of ESS will be responsible for protecting the privacy interest of individuals identified in the system. Each agency is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the system and/or the data contained within.

19. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
Yes. Generally, the agencies that have entered the MOU with DEA/EPIC will share or have access to ESS.

20. Who is responsible for assuring proper use of the data?
The contributing agency has the sole responsibility to ensure that information in ESS was not contributed or maintained in violation of any applicable law by the contributing agency.

All users and participating agencies of ESS will be responsible for ensuring appropriate use of information made available through the system. Each partner agency is responsible for the actions of its users, and sanctions will be applied for intentional or repeated misuse of the system and/or the data contained within.

The contributing agency has the sole responsibility to ensure that information in ESS was not contributed, maintained in violation of any applicable federal, state, or local law by the contributing agency.

21. What are the retention periods of data in this system?
Records in this system in all formats are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

There is no retention period for the data in this system. Each contributing agency is responsible for its own data. The agencies control what is updated, added, modified or deleted. No information is removed unless it is deleted by the contributing agency.

22. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
Records in this system in all formats are maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration.

Each contributing agency is responsible for its data and controls what is deleted. No information is removed unless it is deleted by the contributing agency.

23. Is the system using technologies in ways that the Department has not previously employed? If yes, how does the use of this technology affect individual privacy?
Yes.

EPIC will be sharing Sensitive But Unclassified (SBU) criminal law enforcement information with other federal, state, local, tribal and foreign law enforcement agencies. ESS will provide a single point of access over secure Internet through which authorized law enforcement agents will access the information. The system will assist agents and officers to compare records and analyze the contents of those records to determine similarities or other relationships between criminal acts and the people suspected of committing these acts.

If abused or misused, the ESS could have a negative impact on an individuals' privacy. The contributing agencies have agreed to policies and procedures to mitigate any risks.

24. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.
No. The ESS will provide the capability to identify individuals, addresses and vehicles whose attributes meet the results of a query and provide information on the individuals, addresses and vehicles if that information is contained in the data responsive to the query. However, the system has no mechanism for monitoring the real-time actions, the identification or the location of individuals.

25. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain and indicate what controls will be used to prevent unauthorized monitoring.

No. See response for Part Three, Question 24 above.

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