Privacy Impact Assessment
for the

Priority Target Activity Resource and Reporting System

February 13, 2008

Contact Point
Office of Information Systems
Drug Enforcement Administration
301-307-1000

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 353-8878

Introduction

The basic concept of priority targeting is to identify, target, investigate, and disrupt or dismantle the most significant international, national, regional and local impact drug trafficking and/or money laundering organizations having a significant impact on drug availability within the United States.

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?

The information collected about suspected criminals and their families may include their names, phone numbers, addresses, bank account numbers, vehicle identification numbers (VINs), and the results of investigative efforts concerning their suspected criminal activity.

1.2 From whom is the information collected?

The information may be obtained from suspects, co-conspirators, witnesses, and other investigative sources.

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 information is collected to assist in the enforcement of the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the U.S., or any other competent jurisdiction, those organizations and principal members of organizations involved in the growing, manufacturing, or distribution of controlled substances appearing in or destined for illicit traffic in the U.S.; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances in the domestic and international markets.

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

21 U.S.C. Section 801 et seq, 28 U.S.C. § 534 and 28 C.F.R. §§ 0.100 and 0.101 authorize the collection of 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.

Identified privacy risks are unauthorized access to and use of information regarding individuals suspected of involvement in drug trafficking and/or money laundering. The steps taken to mitigate these risks include authentication controls and role based access controls. For more information, please see the responses to questions 8.5, 8.6, 8.9, and 9.3.

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 system is used to identify and track designated Priority Target Organizations (PTOs) so both operational and financial expenditures can be captured in a single database. Data pulled from the system assists DEA management in assessing established goals, measuring performance, and reporting accomplishments.

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

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

DEA conducts thorough investigations, which ensure the accuracy of the information in the system. DEA adds new and updated investigative information to the system as that information is obtained. Additionally, supervisors review and approve the information that agents enter into the system.

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)?

Data in this system is retained indefinitely and presently unscheduled for final disposition. A draft records retention schedule, proposing 25 years retention, is under development, and will be forwarded to NARA for approval by September 2009.

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.

1. Users of all DEA systems must certify themselves on a yearly basis by completing DEA Security Awareness Training.
2. The system utilizes strict access controls at both the database and application layers using the principle of least privilege to provide access on an as-needed basis.
3. Data at rest in the database are encrypted.
4. Roles are designated to ensure that users view only the appropriate subsets of data.

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?

The information may be shared with the DOJ Executive Office of the Organized Crime Drug Enforcement Task Forces (OCDETF).

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

The Information described in response to question 1.1 maybe shared with OCDETF to further comprehensive and effective law enforcement.

4.3 How is the information transmitted or disclosed?

Information is provided in hard-copy form. It is hand carried by DOJ personnel. No outside carriers are involved.

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

Only authorized DEA employees have direct access to this system. This restricted access eliminates the risk of unauthorized access. When information from the system is shared with OCDETF, it is hand carried to sworn law enforcement officers of OCDETF by DEA employees who have accepted the rules of behavior regarding the proper handling of DEA paper work and data. This practice mitigates the risk of unauthorized use or disclosure of the information.

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?

None

5.2 What information is shared and for what purpose?

N/A

5.3 How is the information transmitted or disclosed?

N/A

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

N/A

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

N/A

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

N/A

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

N/A

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?

DEA has published a Privacy Act System of Records Notice (SORN) for DEA's investigative records. No other notice was provided, and no other notice is required to be provided because the information in this system is collected during law enforcement activities.

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

Individuals about whom information in this law enforcement system is collected have neither an opportunity nor a right to decline to provide information. Exceptions to this general rule include information collected directly from individuals afforded rights under the Fifth Amendment and from individuals who may lawfully assert a privilege (e.g. attorney-client privilege, spousal privilege). Individuals from whom DEA requests information for this law enforcement system may decline to provide information.

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?

Individuals about whom information in this law enforcement system is collected have no opportunity to consent to particular uses of the information they provided. Individuals from whom information in this law enforcement system is collected have no opportunity to consent to particular uses of the information provided.

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

The privacy risk identified would be the failure of persons to know their information may be collected and what it will be used for. DEA has published a Privacy Act System of Records Notice (SORN) for DEA's investigative records. The information in this notice includes entities with which and situations when DEA may share investigative records. This notice, therefore, mitigates the risk that the individual will not know why the information is being collected or how the information will be used. No other notice was provided, and no other notice is required to be provided because the information in this system is collected during law enforcement activities and it is not practicable for any other notice to be given during these activities.

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?

Individuals may make a request for access to their records under the Freedom of Information Act. Individuals may make a request for access to or amendment of their records under the Privacy Act. However, this system is exempt from the access and amendment provisions of the Privacy Act pursuant to 5 U.S.C. § 552a (j)(2) and (k)(1).

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

Notice of individuals' rights under the Freedom of Information Act (FOIA) is given in Departmental regulations describing the procedures for making a FOIA request. Notice of individuals' rights under the Privacy Act is given through publication in the Federal Register of a System of Records Notice and in Departmental regulations stating Privacy Act exemptions and describing the procedures for making access/amendment requests.

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

No

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.

N/A

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?

- Special Agent / Case Agent (SA) – Full editing capabilities;
- Group Supervisor (GS) – Full editing capabilities;
- *** REVIEWER1 – Full editing capabilities;
- Assistant Special Agent-in-Charge (ASAC) – Full editing capabilities;
- *** REVIEWER2 – Full editing capabilities;
- *** Associate Special Agent-in-Charge (ASSOCSAC) – Full editing capabilities;
- *** REVIEWER3 – Full editing capabilities;
- Special Agent-in-Charge (SAC) – Full editing capabilities;
- Operations Management (OM) – Read only capabilities;
- Office of Domestic Operations - Approval (HQ) – Read only capabilities;
- Office of Domestic Operations – Coordination (HQX) – Read only capabilities;
- Office of Resource Management - Evaluation and Planning (FRE) – Read only capabilities;
- Intelligence Analyst (IA) – Read only capabilities;
- Program Analyst (PA) – Full editing capabilities; and
- Division/Region/HQS Admin Role - Read only capabilities.
- ***** =** Optional User Role

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.

No

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

Yes. The system determines the user's role based upon the user profile that is stored in the database. When a user has successfully logged in, the system retains the user's role and adjusts the functionality as appropriate to that role.

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

The users and their privileges are maintained by Division/Region/HQ Administrative Roles.

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

The system has role-based access controls. Access to specific data is restricted by user classification. The detail level of the information available is limited by the user classification. The system retains the user's role and adjusts the functionality as appropriate to that role. User roles are clearly and specifically defined providing for the various levels of access.

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

- User accounts are Strong Password Protected,
- Oracle auditing is turned on,
- There is no open physical access to servers,
- There is limited admin user access to servers,
- The system resides on a closed network.
- Authorized users have accepted rules of behavior, which include the proper handling of sensitive DEA paperwork and data.

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

Users of all DEA systems must certify themselves on a yearly basis by completing DEA Security Awareness Training.

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

Yes. The system is hosted within the DEA's Firebird SBU LAN and Firebird is fully Certified and Accredited (C&A) according to generally accepted guidelines for C&A of DOJ systems and re-accredited every 3 years. Certification was completed October 10, 2006.

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. Initial access to the online system is limited to certified users with active system accounts on a closed Sensitive But Unclassified (SBU) network local area network (LAN) called Firebird. Multi-layered security is in effect by virtue of the fact that users must first logon to Firebird and then access the system after a successful Firebird authentication. An unauthorized user would have to have knowledge of both userid/password combinations in order to gain access to the system.

The system has role-based access controls. Access to specific data is restricted by user classification.

The detail level of the information available is limited by the user classification. The system retains the user's role and adjusts the functionality as appropriate to that role. User roles are clearly and specifically defined providing for the various levels of access.

Database auditing has been turned on and currently tracks 160 events. Auditing logs are checked on a routine basis and monitored by system administrators.

The system is hosted within the DEA's Firebird SBU LAN and Firebird is fully Certified and Accredited (C&A) according to generally accepted guidelines for C&A of DOJ systems and re-accredited every 3 years. In addition, the system is also scrutinized annually with system self-assessments that verify and validate that the appropriate security measures are being effectively deployed.

All of the system's personal data are encrypted and stored in the database via a non-propriety and standard encryption algorithm.

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?

Yes. Technology evaluations are a function of the Enterprise Architecture (EA) and technologies are selected among a host of criteria, including security requirements. This system is considered a part of the EA and therefore inherits the EA technologies. All technologies are vetted by the office of the Chief Technology Officer (CTO) through a defined and repeatable process for the selection of alternatives.

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

1) Data integrity. Data integrity is maintained through best practices approaches for data management. This includes efforts for data standardization (entities/relationships), data structure (relational integrity model), and manual validation processes that exist to ensure the integrity of the data at the source of entry. Also, data integrity is further secured via input validation to forms in the development code.

2) Privacy. Privacy is analyzed via C&A requirements as part of the application of security controls under NIST SP800-53. Decisions are made based on the need to address "secret" or "private" data such as SSN, DOB, etc. Once those data elements are defined, encryption of those items is included as a database function for data at rest.

3) Security. Security is a required part of the project plan for each DEA project, including this one. The plan addresses and includes security in the technical approach portion of the plan. Security and privacy are both reviewed and analyzed as part of the

overall Web Infrastructure C&A for each system (minor application) with an annual self assessment. Finally, the Office of Security programs routinely provides independent auditing against DEA security policies, which provides ongoing risk mitigation to any discovered vulnerabilities as an independent entity outside of the project office.

9.3 What design choices were made to enhance privacy?

1) Utilization of strict access controls at both the database and application layers using the principle of least privilege to provide access on an as-needed basis. 2) Encryption of the data at rest in the database. 3) Roles are designed to ensure that only certain subsets of data can be viewed.

Conclusion

Recognizing that access to priority target information should be limited for security and privacy reasons, the system was designed to limit access by password protected login accounts, user type definitions and compartmentalization by enforcement group membership.

Responsible Officials

_____/s/_____ _____

James D. Craig
Assistant Administrator
Chief Privacy Officer
Drug Enforcement Administration

_____/s/_____ _____

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

Approval Signature Page

_____/s/_____ _____

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer
Department of Justice