Privacy Impact Assessment
for the

Investigative Management Program and Case Tracking System (IMPACT)

February 4, 2008

Contact Point
Office of Information Systems
Drug Enforcement Administration
202-307-1000

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

Introduction

Investigative Management Program and Case Tracking System (IMPACT) is a web-based case management system to replace the existing "paper-based" system. The principal business goal for the system is to improve mission performance and achieve greater operational efficiency relative to the establishment, recording, accessibility, and analysis of information pertaining to DEA investigative activities.

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 to be collected is:

- Name
- Date of Birth
- Alias Names
- Social Security Number (SSN)
- Place of Birth
- Citizenship
- Alien Status
- Race
- Ethnicity
- Sex
- Color Hair
- Height
- Color Eyes
- Weight
- Address
- Phone Number
- Identifying Characteristics

- Employer Information (Company Name and Address, Phone Number, Position Title, Supervisor Name and Supervisor Phone Number)
- Passport Number
- Name on Passport
- Driver's License Number
- Name on License
- Family Information

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 system's information is being collected for the establishment, recording, accessibility, and analysis of information pertaining to DEA investigative activities.

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

21 U.S.C. § 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.

The risks identified are the risk of unauthorized access to or use of defendant/suspect personal information and the risk of unauthorized theft of back-up tapes. Access to the building where the system is housed is protected by physical building security, including security guards, access badges, and security cameras. Access to the system itself is protected by authentication controls, role-based access controls, and system auditing.

Access to individual electronic case files will be limited to those authorized personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file. Sworn law enforcement officers are the only individuals who are given access to the system. These individuals have accepted the rules of behavior regarding the proper handling of DEA paperwork and data, which mitigates the risk of unauthorized use or disclosure of the information. To further prevent unauthorized use by employees, audit logs are kept and checked at regular intervals. Users of all DEA systems must certify on a yearly basis by completing DEA security awareness training.

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 is used to support the investigation and prosecution of drug cases and related offenses.

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)?

Disposition standards for system records will be implemented in accordance with approved records retention schedules.

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.

The system has authentication controls and role-based access controls. Auditing is used to track user logs. A process exists for both user provisioning and cancellation of accounts in a timely fashion. Additionally, users of all DEA systems must certify themselves on a yearly basis by completing DEA Security Awareness Training.

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 is shared with US Attorneys and, on a need-to-know basis, it is shared with these Federal Law Enforcement Agencies: Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Federal Bureau of Investigation (FBI), US Marshals, and Federal Bureau of Prisons (BOP). It is also shared with local Task Force Officers (TFOs) who have been assigned to DEA's High Intensity Drug Trafficking Area (HIDTA) offices. These officers have been deputized as DEA federal agents.

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

All information collected may be shared with the entities listed in question 4.1 to support the continued investigation of alleged drug offenses and the prosecution of those cases and related offenses in courts. The personally identifiable information of confidential informants is not shared.

4.3 How is the information transmitted or disclosed?

Information is provided in hard-copy form via a tracked courier.

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

No components outside of DEA have direct access to the system. Law enforcement officers and Group Assistants are the only individuals who are given access to this information. These individuals have accepted the rules of behavior regarding the proper handling of DEA paperwork and data, which mitigates the risk of unauthorized use or disclosure of the information. Each user is required to review and acknowledge the DEA IT Rules of Behavior annually as part of the online IT security training. Given the limited distribution of the information in the system, the absence of access to the system itself, and the understanding of the rules of behavior, privacy risks are limited.

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?

On a need-to-know basis, the data may be shared with select Federal, State, Local, and Tribal law enforcement officers.

5.2 What information is shared and for what purpose?

Case information is shared. The purpose of sharing this information is to further other case investigations and to prosecute drug and related offenses in courts.

5.3 How is the information transmitted or disclosed?

Information is shared in hard-copy form via a tracked courier.

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

No. Data is given only to trusted law enforcement officers. These officers have accepted the rules of behavior regarding the proper handling of DEA paperwork and data.

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

Data is given only to trusted law enforcement officers. DEA does not monitor training activities for users from agencies outside DEA.

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

No. There are no provisions in place for auditing law enforcement recipients' uses of system information.

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

A risk of unauthorized disclosure of defendant/suspect personal information was identified. DEA law enforcement officers and Group Assistants are the only individuals who are given direct access to this information. These individuals, and the trusted law enforcement officers with whom they share this information, have accepted the rules of behavior regarding the proper handling of DEA paperwork and data, which mitigate the risk of unauthorized use or disclosure of the information. Given the limited distribution of the information in the system, the absence of access to the system itself, and the understanding of the rules of behavior, privacy risks are limited.

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

- Regular User - Full editing capabilities only to his own case information.
- Supervisor - Full editing capabilities to case information for all DEA Special Agents and TFOs within his group.
- Group Assistant - Full editing capabilities to case information for all DEA Special Agents and TFOs within the group.
- System Administrator – Full editing capabilities to all case information for all groups and can also add, remove, and edit user profiles.

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.

Contractors will not have access to the IMPACT application.

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?

It is determined at the Group Supervisor level which end-users can do case work and administrative work. This procedure is documented in the User's Manual.

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

Access to specific data is restricted by user classification (Group Assistant, System Administrator, Supervisor, and Regular User), as well as by membership in specific enforcement groups. This enforces access control to 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.

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 access to servers. The information is kept on a closed network. Authorized users have accepted rules of behavior, which include the proper handling of sensitive DEA paperwork and data. Users of all DEA systems must certify on a yearly basis by completing DEA security awareness training. Changes to roles and permissions are captured in audit logs.

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) local area network (LAN) called Firebird. Multi-layered security is in effect by virtue of the fact that users must first log on to Firebird and then log into the system successfully. 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 (Group Assistant, System Administrator, Supervisor, and Regular User) 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.

The system is hosted within the DEA's Firebird SBU LAN, which 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 scrutinized annually with 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?

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.

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 and each project, including this one, 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?

These 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 were designated to ensure that only certain subsets of data can be viewed.

Conclusion

Recognizing that access to case information should be limited for security and privacy reasons, this system was designed to limit access by password protected login accounts, user type definitions, and compartmentalization by enforcement group membership. Privacy risks in the system are controlled and minimized by separation of users, compartmentalization of functions, and monitoring/oversight activities. Due to security concerns associated with the system's data, significant security controls have been implemented.

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