Privacy Impact Assessment
for the

PlanETS

August 22, 2006

Contact Point
Concorde Program Management Office
Drug Enforcement Administration/Office of Information Systems
202-307-1000

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

Introduction

The Plan Enforcement Tracking System (PlanETS) is a web-based application that provides for geographical-based processing and analysis for the Drug Enforcement Administration (DEA) operations. The system captures the operational aspects that are required prior to an enforcement or surveillance action. The operational plan is completed prior to an enforcement action and provides detailed information regarding the planned enforcement activity. Data is collected and saved for record. Agents use a printout of the operation at the enforcement location.

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?

PlanETS collects personal information of those individuals involved with Operation Safety Plans. Individuals involved are law enforcement officers, e.g. DEA special agents, TFO (NYPD, FBI, ICE), and targets / suspects of the operation. The data collected include:

- A complete narrative describing the operation plan, which may include personally identifiable data elements.
- Information about suspects, including:
  - Name (with aliases).
  - Date of birth / age (and alternate DOB).
  - Race, gender, hair/eye color, height, weight, description.
  - Addresses associated with suspect, including description, photograph and phone number.
  - Vehicles associated with suspect, including license plate and photograph.
  - Warrants, criminal history and gang affiliations.
  - Photographs.
  - ID numbers assigned by local, state and federal law enforcement.

- Information about operation locations
  - Address and/or description.
  - Address and/or description of staging location.
  - Map, property type (residence, business), phone number and photograph.
  - Warrants and Identification (ID) numbers assigned by local, state and federal law enforcement.
  - Closest hospitals and police precinct, with name and phone numbers of precinct contacts.
- Information about agents participating in the operation:
  - Name, phone numbers and vehicle.
  - Call sign, Agency, Team and role assignment.
- Information about under cover (UC) or confidential sources (CS) involved in the operation:
  - Name (for under cover personnel)
  - UC Number (for confidential sources)
  - Description, phone numbers, vehicle and assigned equipment.
- Information about attorneys assigned to the case:
  - Name, type Assistant United States Attorney or Assistant District Attorney (AUSA/ADA), district, contact phone numbers and date contacted.
- Information about contacts with other law enforcement agencies about reverse operations (where the agents pose as drug dealers):
  - Name, agency, phone numbers and date contacted.
  - Name, agency and phone number of agent contacting other agencies.
- Information about supervisors approving the operation plan:
  - Name, title, phone number and date of approval.

1.2 From whom is the information collected?

The main source of the information PlanETS collects is from DEA agents and/or members of Task Forces charged with running the operation(s), to include Group Supervisor and Assistant Special Agents in Charge (ASACs). Information may also be collected from NYPD, the New York State Police

(NYSP), other federal law enforcement agencies participating in the NYFD Strike Force and other state/local agencies working in conjunction with the NYFD.

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?

PlanETS requires the collection of personal information to accurately identify all persons, both suspects and operational personnel, associated with the operation. This is done to ensure that the agents running the operation have the most complete picture possible of all aspects of the operation for safety as well as accountability purposes. The data collected is also used to establish a timeline of notifications to other law enforcement agencies, and can discover conflicts with other ongoing operations or incidents. This PlanETS is a deconfliction system with other LEAs.

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 by PlanETS is used by the DEA agents participating in the operation in the form of a printed Operation Plan report. The Operation Plan report uses this personal information in the text of the plan, along with photographs of suspects, vehicles and locations, and maps of the operation location based on the location data collected. Operational plans involved are safety related plans in order to protect and inform LEAs involved, so that they can receive detailed information about individuals and information about the facility involved. The PlanETS information is also used to create a map for the Base Operations dispatchers to see all ongoing operations, and for dispatching, ending and canceling operations. PlanETS information is provided to GS and ASAC supervisors via the Operation Plan web forms and the Base Operations map so that they can communicate with team members and/or call-ins from other federal, state or local law enforcement officers regarding tactical law enforcement activities on the subject(s) in the reports. The information is also used by the FBI, and other federal agencies assigned to the NYFD Strike Force, as well as the NYPD and the NYSP to de-conflict with other enforcement operations that may be active or pending in close vicinity or the same location.

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 the New York Division FBI Office.

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?

The information is shared with the NYPD and the NYSP (working with the NYFD Task Force), all federal agencies associated with the NYFD Strike Force and any state/local agencies participating in joint investigations with any of the offices in the NYFD.

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.

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

No.

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?

No.

Section 8.0
Technical Access and Security

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

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 PlanETS system

Risk: Low

Mitigation / Countermeasures:

- Authentication controls. Initial access to the PlanETS online system is limited to authorized users with active PlanETS 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 PlanETS after a successful Firebird authentication. An unauthorized user would have to have knowledge of both userid/password combinations in order to gain access to PlanETS.
- Role-based access controls. Access to specific data is restricted by user classification (Regular User, Dispatcher, System Administrator) as well as by membership in specific enforcement groups. This enforces access control to information with privacy implication to members of an enforcement group, their supervisors and the Base Command operators that dispatch the operations. Additionally, the detail level of the information available is limited by the user classification.
- Access and changes to PlanETS data can be tracked through database logging and auditing. Auditing logs are checked on a routine basis and monitored by system administrators.
- PlanETS user accounts can be created, updated, enabled and disabled only be authorized administrators. In order to perform these functions, individual must be identified as a System Administrator. The authorization shall come from the ASAC. Access to specific data is restricted by user classification (Regular User, Dispatcher, System Administrator) as well as by membership in specific enforcement groups.
- PlanETS 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 systems for DOJ 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.

.

Threat: Unauthorized Disclosure of Operation Plan Report Print-Out

Risk: Low

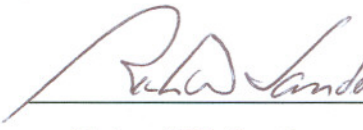
Mitigation / Countermeasures:

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

Conclusion

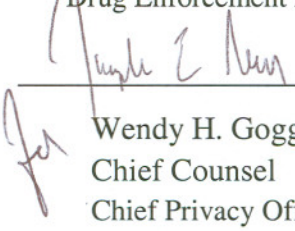
Recognizing that access to sensitive Operation Plan information should be limited for security and privacy reasons, the PlanETS system was designed to limit access by password protected login accounts, user type definitions and compartmentalization by enforcement group membership.

Responsible Officials



_____<<Signature>> 09/07/06 <<Date>>

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



_____<<Signature>> Sep 6, 2006 <<Date>>

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

Approval Signature Page

_____<<Signature>> _____<<Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

Responsible Officials

_____ <<Signature>> _____ <<Date>>

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

_____ <<Signature>> _____ <<Date>>

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

Approval Signature Page

_____ <<Signature>> 10/6/06 <<Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice