Privacy Impact Assessment
for the

National Drug Intelligence Center

SENTRY System

March 29, 2007

<u>Contact Point</u>
David J. Bonski
Chief, Technical Services Branch and Chief Information Officer
National Drug Intelligence Center
319 Washington Street, 5th Floor
Johnstown, PA 15901
(814) 532-4795

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

Privacy Impact Assessment

SENTRY System
National Drug Intelligence Center eGov Initiative

Introduction

The National Drug Intelligence Center (NDIC) SENTRY System is an Internet-based collection and dissemination system designed to help identify new, synthetic drug-related behaviors at an early stage, evaluate their importance, and track their development. The SENTRY application is a component of the NDIC eGov Initiative (NEI). SENTRY will focus on synthetic drugs that are primarily produced via a chemical process, such as LSD (lysergic acid diethylamide), MDMA (3, 4-methylenedioxymethamphetamine, also known as ecstasy), and methamphetamine. The system also will monitor prescription drugs, over-the-counter medications, botanical substances and extracts, and chemicals and products involved in the manufacturing of synthetic drugs. The ultimate goal of SENTRY is to inform and alert the counterdrug community to address problems at an early stage.

SENTRY is operated by NDIC in coordination with the Office of National Drug Control Policy (ONDCP) and the National Institute on Drug Abuse (NIDA). SENTRY supports the ONDCP National Synthetic Drugs Action Plan.

SENTRY consist of an external public-facing website used to collect and disseminate information on emerging synthetic drug issues form registered users and an internal relational database used to process and analyze information obtained through the external website.

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

1.1 What information is to be collected?

Two types of information are collected through SENTRY: User registration information and descriptions of new or unusual synthetic drug-related activity provided by registered users.

User Registration Information – Agencies interested in becoming an authorized SENTRY user must provide agency contact information, including agency name, contact/user name, contact/user position, address, telephone number, and e-mail address.
Drug Activity Information – Approved authorized SENTRY users provide anecdotal information describing new or unusual synthetic drug-related activity.

1.2 From whom is the information collected?

It is anticipated that a network of correctional officers, drug diversion investigators, emergency medical personnel, forensic chemists, juvenile detention officers, law enforcement officers, medical toxicologists, school nurses, school resource officers, teachers, school administrators, physicians, emergency medical personnel, medical examiners, and treatment providers will become approved, authorized users and provide information through SENTRY.

Section 2.0 – The Purpose of the System and the Information Collected and Stored within the System

2.1 Why is the information being collected?

SENTRY is an Internet-based collection and dissemination system designed to help identify new synthetic drug-related behaviors at an early stage, evaluate their likely importance, and track their development. Information collected through SENTRY also will be shared, in aggregate form, with federal, state, and local counterdrug agencies to assist proactive responses to emerging synthetic drug-related behaviors and trends.

Section 3.0 – Uses of the System and the Information

3.1 Describe all uses of the information.

NDIC will use information obtained through SENTRY, combine it with additional information, and produce and disseminate Drug Alert Watch and Drug Alert Warning reports. A Drug Alert Watch report will be issued when a pattern of synthetic drug-related activity is first identified. The Drug Alert Watch report relies heavily on qualitative (nonnumeric anecdotal) information obtained from NDIC's wide network of partners. Once a pattern is established, NDIC will continue collecting and evaluating additional information. If and when a trend is detected, a Drug Alert Warning will combine this same qualitative information collected in the Drug Alert Watch phase with additional quantitative information collected by NDIC analysts and partner agencies.

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

4.1 With which internal components of the Department of Justice (DOJ) is the information shared?

Within DOJ, SENTRY information will likely be shared with the Drug Enforcement Administration (DEA), although no formal data-sharing agreement currently exists with DEA. SENTRY information also may be shared with other DOJ components involved in drug enforcement activities that request the information.

Section 5.0 – External Sharing and Disclosure

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

Outside of DOJ, SENTRY information will be shared with the ONDCP in the Executive Office of the President and NIDA in the Department of Health and Human Services. Other federal agencies involved in drug enforcement, treatment, or research that request SENTRY data may also be given access to SENTRY information. SENTRY information will be shared with local agencies on a case-by-case basis when an authorized user requests that NDIC facilitate contact with another user.

Section 6.0 – Notice

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

Agencies voluntarily become authorized SENTRY users and are under no obligation to use the system to report 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?

Information provided through SENTRY will be available, in aggregate form, through the Geographical Information System (GIS) capabilities of SENTRY. NDIC does, however, only use the first three digits of the zip code to generate this information to prevent identification of specific respondents. SENTRY information will be shared with state and local agencies on a case-by-case basis when an authorized user requests that NDIC facilitate contact with another user. NDIC will telephone the submitter of the information and inform them that another user of the system would like to speak with them. If this is agreeable, NDIC will supply the submitter’s contact information to the requestor via telephone. Only with the consent of the SENTRY user who provides the data will PII obtained through SENTRY be provided to the requestor.

Section 8.0 – Technical Access and Security

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

The SENTRY system consists of a public-facing web site and an Intranet-based web site. The purpose of the external site is to collect information from known registered users, and the purpose of the internal site is for the analytical processing of information submitted from the external site.

The public-facing website will contain the following user groups or roles:

- General User – NDIC will maintain (create, update, delete) all accounts, and only those people who have submitted the proper information to NDIC will be granted access. These users have the ability to submit information and view NDIC news items and bulletins.
- Web Administrator – This group/role consists of NDIC employees who have been granted the ability to create, modify, and delete site content (bulletins and news items).
- User Administrator – This group/role consists of NDIC employees who have been granted the ability to create, modify, and delete external user accounts.
- Administrator – This group/role consists of NDIC employees who manage users and content.

Access to the internal site will be limited to NDIC employees. The internal site will contain the following user groups or roles:

- Analyst – NDIC employee (Intelligence Analyst) who creates, updates, and deletes content related to the information submitted from the external site.
- Administrator – NDIC employee who has the ability to create, update, and delete all site content.

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 system from a user standpoint. Contractors will help Government staff design, develop and test the SENTRY application. Once the Government conducts final acceptance testing and formally receives the application, Government support staff will deploy the external and internal web sites. Government employees will provide general support and lifecycle maintenance. All maintenance support decisions will be made by

Government employees. NDIC does have a general support subcontract for technical services, and some system administration support by a contractor may be required. The scope of the support subcontract includes software development and life-cycle technical support.

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

Yes. See question 8.1.

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

The internal web site will use Operating System authentication and NDIC will follow NDIC documented Account Administration Policy for adding, modifying, and creating users in addition to granting and denying access to resources.

To the general user community, NDIC will explain the process for participating in the SENTRY application. To participate as a General User on the public-facing website, the requester must provide the following information typed on agency letterhead:

- Name of agency or organization
- Name and title of requester
- Requester's role within the agency
- Complete mailing address
- E-mail address
- Telephone number
- Fax number

This information should be faxed to NDIC and an NDIC employee will contact the requester within 7 business days with their login information.

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

For the Internal website we follow our Account Management Policy, in which each request for access must be signed off by the requester's supervisor and access granted by NDIC's Security Office account representative. For the external public-facing web site, please see the response to question 8.4 above.

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

NDIC uses levels of safeguards to prevent the misuse of data. First, user access is limited and must be approved before any access to the system is granted for either the Internal or External websites. Second, users will be granted only the access required to perform their job functions. Privileges are grouped into roles, and these roles are assigned based on job function. Third, the application segregates information access - there are two web sites and two databases - external users are only granted access to a small portion of data in one database only. Fourth, all records are stamped with the date/time and user who created the record and the date/time and user who modifies the record. Fifth, important information is audited. For example, an audit log tracks login and logout events. Finally, the audit information will be periodically reviewed.

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

Being a DOJ component, all NDIC employees and contractors are required to complete Computer Security Awareness Training (CSAT) annually. Incorporated into the CSAT training is privacy training.

NDIC employees will be involved in the development, testing, and deployment of the SENTRY system. Privacy-related information will be addressed in all stages. NDIC users will receive training prior to the release of the system.

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

NDIC will support design, development and testing of the SENTRY system on our Justice Network Segment (JNS). The Internal website will be hosted on this network. This network is Certified and Accredited and has a Certification and Accreditations (C&A) status of Authority to Operate (ATO). The ATO for JNS was issued on March 7, 2006.

NDIC will deploy the public-facing website on our NEI network. This network is Certified and Accredited and has a C&A status of Authority to Operate (ATO). The ATO for NEI was issued on February 24, 2005.

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

Potential Privacy Risk: Unauthorized Access to the SENTRY system

Risk Level: Low

Risk Mitigation:

- Physical and Logical Access Control - Information in the SENTRY system is safeguarded in accordance with NDIC's Information Technology (I.T.) Security policies. Records and computer systems are maintained in buildings with restricted access. Passwords and password-protection mechanisms also restrict access to information in this system. Only personnel who develop and maintain the system and other users who are intelligence analysts will be permitted access to the system. This access is limited to those individuals who have an official need for access in order to perform their duties.

- Authentication Controls -Access to the SENTRY system is limited to authorized users with active SENTRY accounts on a closed Sensitive But Unclassified (SBU) network called the NDIC NEI.

  NEI is fully Certified and Accredited (C&A) in accordance with DOJ‘s FISMA guidelines. Administrative and technical controls are described in more detail in the C&A package for the NEI network.

- Role-Based Controls - Access to specific data is restricted by user classification. This enforces access control to information with privacy considerations given to registered users, NDIC analysts, technical staff, and users from other participating agencies.

Potential Privacy Risk: Compromise of Information As a Result of Information Sharing with Other Participating Agencies

Risk Level: Low

Risk Mitigation: The sharing of information collected by the SENTRY system with other government agencies will be done in accordance with Memorandums of Understanding (MOUs) that will be established with these agencies. The protection of information collected and shared will be delineated as a condition in these MOUs. All users, technical staff, and other individuals from participating agencies will be responsible for protecting the privacy interest of information collected by this system.

Conclusion

Privacy considerations for the SENTRY system are protected through the fundamental design of the system. There is an external web site with its own community of users and protections, and there is an internal web site with a different community of users and protections. The business rules for each group of users are based on specified roles and on what individual users are required to do with the information that is collected.

Responsible Officials

___David J. Bonski_____________ Signature ___4/6/07_________ Date

David J. Bonski
Chief, Technical Service Branch
Chief Information Officer
National Drug Intelligence Center

____Thomas W. Padden________ Signature ____4/10/07________ Date

Thomas W. Padden
Acting Chief Counsel
Chief Privacy Official
National Drug Intelligence Center

Approval Signature Page

___Kenneth P. Mortensen_____ Signature ___5/2/2008_________ Date

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