FINANCIAL CRIMES ENFORCEMENT NETWORK
PRIVACY IMPACT ASSESSMENT

Pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Chapter 36), the following organizational privacy management information is provided in this Privacy Impact Assessment (PIA) analysis of how information is handled: (a) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (c) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

- **NAME OF SYSTEM**

314(a) SISS: Secure Information Sharing System

- **UNIQUE SYSTEM IDENTIFIER**

SECTION A CONTACT INFORMATION

Director, FinCEN
P.O. Box 39, Vienna, VA 22183-0039
E-mail: InfoAssure@fincen.gov

SECTION B SYSTEM APPLICATION/GENERAL INFORMATION

This section of the Privacy Impact Assessment (PIA) describes the application and the method used to collect, process, and store information. Additionally, it includes information about the business functions the system supports.

The 314(a) Major Application (MA) provides financial institutions the capability to electronically access subject lists submitted by federal law enforcement and to electronically indicate positive matches on any person or business on that subject list through a secure Internet network. 314(a) also provides a secure messaging system that allows FinCEN to communicate and disseminate information such as advisories and reports on the latest trends in money laundering or terrorist financing to the financial industry.

SECTION C DATA IN THE SYSTEM

The data in the system includes Name, Date of Birth and Addresses (and other identifying information about persons of interest. The data supports sharing of information between federal law enforcement and the financial industry as covered by the Patriot Act Section 314(a).

SECTION D ATTRIBUTES OF THE DATA

Refer to Section C.

SECTION E ACCURACY, TIMELINESS, AND RELIABILITY

Point of contact data is verified by federal regulators. It is the responsibility of referring law enforcement agents to provide accurate subject information.

SECTION F MAINTENANCE AND ADMINISTRATIVE CONTROLS

Data is removed every four weeks from the secure website as a new transmission is rotated in, and is erased from the database. Backup tapes are fully encrypted. Database auditing is done on the system. There is a comprehensive audit trail of every user and employee that logs into the system and every action taken within the system. Infrastructure IDS's and firewalls monitor any anomalies within the network. The purpose for this auditing is to ensure that only authorized users have access and make queries to the system. Persistent cookies are not used to monitor users of the system.

SECTION G ACCESS TO DATA

Cleared FinCEN employees, contractors, TCS contractors, and the financial industry have access to the data. On a bi-weekly basis, FinCEN receives a point of contact listing from the federal regulators. Individuals on those listings are designated as eligible to access the system. The data can only be retrieved by a designated point of contact via a user name and password. The data is not retrievable via a personal identifier. Data can be retrieved by an established user name and password via the secure website.

Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

N/A. The data gathered is for subjects of interest for law enforcement requestors.

SECTION H BUSINESS PROCESSES AND TECHNOLOGY

Will the conduct of this PIA result in circumstances that will require changes to the current business processes involving this system? If so, explain. No.

Will the completion of this PIA potentially result in technology changes for the system? If so, explain. No.