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**

BSA E-Filing

- **UNIQUE SYSTEM IDENTIFIER (or Systems of Records Notification)**

Covered under: Treasury/FinCEN .003-Bank Secrecy Act Reports System (formerly Treasury/DO .213)

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.

Pursuant to the USA Patriot Act of 2001, the Financial Crimes Enforcement Network (FinCEN) was tasked with developing a highly secure network to allow filing institutions to electronically file certain Bank Secrecy Act (BSA) forms (reports). The BSA E-Filing system portal provides a third filing option to financial institutions for meeting their BSA reporting responsibilities and also makes the information available to law enforcement more rapidly. Prior to the introduction of BSA E-Filing, these filings were sent either on magnetic tape or on paper through the U.S. mail.

- The BSA E-Filing system can be viewed as having two basic components: (1) A system that will provide financial institutions the capability to electronically file their BSA data through a secure internet network. (2) 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.

SECTION C DATA IN THE SYSTEM

The categories of individuals covered in the system include individuals identified in reports filed under the Bank Secrecy Act and its implementing regulations at 31 CFR part 103, including customers of financial institutions, brokerages, casinos, and money services businesses. Data gathered include:

1. Name
2. Social Security Numbers,
3. Birth dates
4. Addresses
5. Bank account numbers
6. Occupation
7. Amount and Type of Transactions
8. Passport No. and Country
9. Financial Institution where the transaction occurred
10. Other account information to be stored at the Internal Revenue Service (IRS) Detroit Computing Center (DCC)
11. Other investigative data: XXXXXXXXXXXX

BSA E-Filing does not allow the retrieval of stored data submitted to the IRS DCC because it operates as a transmission system.

Note: The system is only a transmission system to the Bank Secrecy Act Reports System.

The information contained in BSA E-Filing is collected under the authority of the Bank Secrecy Act, the popular name for Titles I and II of Public Law 91-508, as amended, and codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5331. The regulations implementing the authority contained in the Bank Secrecy Act are found at 31 CFR Part 103. The authority to administer 31CFR Part 103 has been delegated to FinCEN.

Pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, records filed through BSA E-Filing are covered by FinCEN's Privacy Act system of records notices Treasury/FinCEN .003-Bank Secrecy Act Reports System--Treasury/FinCEN. A new system of records or further alteration to our existing system of records will not be required for BSA E-Filing.

The sources for the information in the system are from the records of participating organizations required to file reports with FinCEN, which include financial institutions, brokerages, casinos, and money services businesses. The majority of the information in the system is data taken from the individual and not from federal, state, tribal, and local agencies. Data may be collected from other third party sources when individuals conduct financial transactions on behalf of other individuals or institutions and need to file the information appropriately.

The data is not used by the system; BSA E-Filing is designed to bring in the bank secrecy act data faster and more efficiently through an Internet based electronic filing portal so the relevant and necessary data can be transmitted by the system to the IRS for storage at IRS DCC. The

system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected, but will be used solely for the electronic transmission of BSA forms to the IRS.

SECTION D ATTRIBUTES OF THE DATA

Refer to Section C.

SECTION E ACCURACY, TIMELINESS, AND RELIABILITY

The source of information to be collected from the customers of these organizations is specifically outlined on the BSA form each filing organization is required to have its customers complete. To ensure the data is complete and accurate, the system has error-checking and form validation functionality. The IRS will verify the accuracy of data collected from sources other than FinCEN and will send correspondence on incomplete or invalid data submitted on the electronically filed BSA form(s). Once the document is filed, each form is entered as an official legal document and cannot be changed. The data elements are specifically described in detail and documented in the data model provided in the document: BSA E-Filing Engineering Notebook.

SECTION F MAINTENANCE AND ADMINISTRATIVE CONTROLS

BSA E-Filing retains administrative data as follows:

Administrative Data Type	**Retention Time**
Acknowledgement Data	30 days after being opened or 60 days after being posted, whichever comes first
Alert Data	30 days after posting
Track Status Data	365 days after achieving 'Accepted' or 'Rejected' status

The data is deleted from the database using an automated program.

FinCEN's ISSO provides security oversight for the Contractor. The ISSO collaborates with the Program Manager on required security procedures and implementation - the Contractor adheres to and follows FinCEN ISSO directed security procedures and protocols. FinCEN security officials are allowed unrestricted access to contractor facilities to conduct security site surveys and to perform duties associated with information systems security and information security oversight. FinCEN’s ISSO and BSA E-Filing COTR perform on-site system security reviews frequently for any signs of unauthorized system use/access attempts and indications of anomalous system or user behavior.

The Treasury Chief Information Officer (CIO) has implemented a Treasury-wide CSIRC using the NETSEC program. Incidents are reported to GSA's FedCIRC via the Treasury’s TCSIRC.

The following are the minimum requirements that must be included in each Incident Response Process for FinCEN: Security Incidents - All security incidents (internal and external), breaches, vulnerabilities, and adverse information are to be reported immediately to a Supervisor, Security Officer, and/or the Director. On request, some incidents will be reported in writing to the Security Officer. If an incident involves sensitive information, personnel will ensure protection of that information first and then report it to the ISSO. Computer Security Incidents Reportable to the ISSO - The following computer security incidents must be immediately reported to the ISSO: (1) Malicious code accidentally or purposely infecting any IT system/network must be reported (2) Other information systems security-related incidents (3) Suspicion or known malicious infections or attacks on any IT system or network (4) Intrusion attempts or successful system access by an unauthorized person or entity.

In June 2003, FinCEN implemented its new Information Systems Security Policies. These policies include rules of behavior and consequences for violating bureau directives or policies set forth by the Director. FinCEN's CIO is the Designated Approving Authority (DAA) for all certification and accreditation (C&A) related matters. FinCEN's ISSO provides IT security management oversight (as well as maintains physical security and federal industrial security measures) for all of FinCEN's systems, networks, and contracted programs. In addition, the ISSO is responsible for implementing and executing FinCEN's IT security program with close coordination and collaboration with the CIO.

The E-Filing system maintains a system log allowing for the tracking of all user connectivity to the system. This log monitors the username, connection time, and connection length. Unauthorized access attempts can be monitored using this log file. The log also displays the number and type of filings the user submitted during their session.

SECTION G ACCESS TO DATA

BSA E-Filing does not allow the retrieval of stored data. The system is only used to file reports such as Suspicious Activity Report (SAR) and Currency Transaction Reports (CTR). Access to the system is determined by a user completing a form that is then verified by FinCEN. The verification is done by FinCEN contacting the Financial Institution of the user to verify that this user exists and has a need to access the system. Users who input data to the system include, financial institutions, and banks. Data from this system is inputted into the Bank Secrecy Act Reports System.

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

N/A.

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.