

## **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**

ITI - Information Technology Infrastructure

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

Refer to <http://www.treasury.gov/foia/privacy/issuances/fincen05.html> for the SORN information

### **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 ITI GSS supports and provides telecommunication, network services, and Data Center services to support the FinCEN mission. The ITI GSS also provides access and services for remote and traveling users such as through protected communications and laptop computers. Applications utilizing ITI GSS infrastructure allow for the retrieval and analysis of BSA information.

### **SECTION C      DATA IN THE SYSTEM**

1. Name
2. Address
3. Social Security Number or TIN number
4. Bank Secrecy Act (BSA) Information

User information (User ID, password, privilege level, Permissions granted) is needed to authenticate users and verify user levels and the need of that individual to access data in the system.

BSA data collected by the IRS is used to assist other agencies in identifying illegal activities associated with funding/supporting terrorist activities, money laundering, and other activities that could adversely affect the security of the United States.

## **SECTION D      ATTRIBUTES OF THE DATA**

Refer to Section C.

## **SECTION E      ACCURACY, TIMELINESS, AND RELIABILITY**

Data is submitted to the IRS who performs any data integrity verification.

## **SECTION F      MAINTENANCE AND ADMINISTRATIVE CONTROLS**

The following information is captured in the audit trails:

1. User Id
2. User Location
3. Time
4. Date
5. Login
6. Logoff
7. Terms Searched

Infrastructure firewalls and (Intrusion Detection System) IDS's have been implemented to monitor any anomalies in the network. Active Directory (AD) login has been enabled on the workstations and servers to audit user actions as well as application level login. The purpose of this capability is to ensure that no unauthorized users access the FinCEN ITI. In addition, two factor authentication is used for remote access along with mobile device encryption.

BSA data is maintained for 10 years. Data is purged from the system database. Areas are overwritten in time.

## **SECTION G      ACCESS TO DATA**

Authenticated users can retrieve and view Bank Secrecy Act (BSA) data for subjects of interest. Personnel associated with specific offices or programs; contractors, users, managers, etc. Access to specific applications or network resources are granted by System Administrators based on Management request using the Fin018. Security clearance level is verified by the Office of Security, the Information System Security Office maintains a copy of the manual Fin18 until access is revoked by manager or user departs. Access is controlled by System Administrator; user roles and permissions can be assigned by the system administrator based on the individual login and level of access required (roles assigned to the user). For FINCEN users, a FIN018 form

has to be initiated by the manager of the employee before access is granted to the systems. Refer to Question 8, for the FIN018 process.

The IRS at DCC supplies all BSA data to FinCEN. The retrieval systems also query the FinCEN Analytical Case Management System, the FinCEN XXXX XXXX and the XXXX XXXX XXXX. These types of access are granted through Memorandum of Understanding/Agreement (MOU/MOA).

**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.