Secure Outreach
Privacy Impact Assessment (PIA)

June, 2008

Page Break

Secure Outreach
Privacy Impact Assessment

Table of Contents

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."

SECTION A CONTACT INFORMATION

- **NAME OF SYSTEM**
  Secure Outreach

- **UNIQUE SYSTEM IDENTIFIER**
  015-04-01-12-01-1001-24-115-045

- **CONTACT INFORMATION**

  System Owner: Ken Obrien, Assistant Director FinCEN Office of BSA Data Services
  Telephone Number: 703-905-5168

  System Manager: Richard Whitney, FinCEN Secure Outreach Project Manager and COTR
  Telephone Number: 703-905-3596

  Privacy Act Officer: Gregory A. Smith, FinCEN Privacy Act Officer
  Telephone Number: 703-905-5034

  Chief Information System Security Officer: Greg Sohn
  Email: InfoAssure@fincen.gov

SECTION B SYSTEM APPLICATION/GENERAL INFORMATION

The Secure Outreach Project is part of the larger “BSA Data Services” organization within the Financial Crimes Enforcement Network (FinCEN) that collects and distributes Bank Secrecy Act (BSA) data to law enforcement and regulators. The Secure Outreach system provides Federal, state and local law enforcement, and regulatory users with a Treasury approved secure Internet connection to the Currency and Banking Reporting System (CBRS). The Secure Outreach web also provides a secure e-mail system. Also available at the website is a variety of information, such as training modules, state coordinator lists, relevant news and important system information. Secure Outreach is an operational system undergoing incremental and maintenance enhancements.

The Secure Outreach system provides a secure portal to sensitive, but unclassified BSA data, stored at a different website, but it does not store any of that data within itself. Classified data is not processed on the system. BSA data consists of data submitted by banks and other entities on forms such as form 8300, CMIR, CTRs, FBAR, RMSB, FinCEN form 110, and SARs (Full definition of all the form is provided at www.fincen.gov/reg_bsaforms.html). Secure Outreach is accessible by public Internet by those law enforcement and regulatory personnel with valid authentication. Secure Outreach does store authentication and contact information used to verify users' identity. Since users work for agencies like the Federal Bureau of Investigation (FBI), and the Drug Enforcement Agency (DEA), this user information is considered highly sensitive and is only available on a need-to-know basis.

The information contained in BSA databases (external to Secure Outreach) 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 C.F.R. Part 103. The authority to administer 31C.F.R. Part 103 has been delegated to FinCEN.

SECTION C DATA IN THE SYSTEM

The categories of individuals covered in the system include law enforcement users, financial regulatory users, and personnel in the FinCEN organization. The information collected is:

Name (Last, First, and Middle):
Agency and/or Agency Memorandum of Understanding (MOU) group:
Title:
Address:
Phone:
E-mail:
Date of Birth (DOB):
Social Security #:
Mother's First Name:
Supervisor:
Supervisor Title:
Supervisor Phone:
Supervisor E-mail:
BSA Direct Web Based Training status

The source for the information in the system is the information submitted on IRS form 5081 by the individuals in question. Supervisors of the individual's organization must approve the submittal. Selected contact information may be updated by the help desk in response to end user calls. Training progress is automatically recorded by the website's program.

Other information in the system pertains to group and special user access rights. For example, agency coordinators have the ability to generate extra reports.

Accuracy of the information associated with the users is dependent on the end user submittal of the information on the IRS form 5081 and validation by an appointed agency coordinator. Users can update selected information directly on Secure Outreach or can update their information with a call to the help desk.

The system acts as a portal to CBRS, so no public data is stored on the system.

SECTION D ATTRIBUTES OF THE DATA

Secure Outreach acts as a portal to CBRS. Secure Outreach itself does not retrieve general personal data to general end users or produce reports on individuals. End users can only view and edit their own contact information and title. End users can view, but not change their supervisor information. Addition and modification of user data is limited to the Secure Outreach help desk" and is limited to corrections based on phone calls with the users.

Help desk personnel have read access to user authentication data (DOB, mother's first name, and social security number) and contact data for the purposes of verbally identifying a user prior to a password reset and for filling call log tickets.

SECTION E MAINTENANCE AND ADMINISTRATIVE CONTROLS

The current policy is not to delete any users from the directory server data store, only to deactivate them. If and when the number of users exceeds the capacity of the system alternatives for separately archiving them will be examined. In addition, all systems are backed up to tape and stored offsite at a Government facility. In the case of a disaster, a replacement site would be activated from tape backup. Over twelve months of data is retained on tape. Note: the directory server maintains a replicate copy in real-time. Procedures for tapes are included in the administrators' operations manual.

Secure Outreach has employed standard proven technology and the current system is not a radical departure from anything that was done in earlier versions. It does not employ smart cards, caller-id or software that monitors individual users. Secure Outreach does utilize a centralized identity management infrastructure that ensures that only authenticated and authorized users are able to access the Secure Outreach portal, secure email and CBRS its BSA data. All users must authenticate to Secure Outreach before they may access the BSA Direct system. Secure Outreach requires users to authenticate via a secure login screen requiring username and password and protected by 128-bit secure socket layer (SSL) encryption. All communication between the user and BSA Direct continues to be protected by at least 128-bit SSL encryption.

End-user access to Secure Outreach is through password protected SSL/Transport Layer Security (TLS) Internet sessions. High level security controls are employed to meet OMB requirements, Federal Information Security Management Act (FISMA) requirements, and guidance:

Audit trail information in Secure Outreach consists of login and log off timestamps of users. All other audit data is stored on a separate system (Refer to CBRS for more details:

http://www.irs.gov/privacy/article/0,,id=134898,00.html). This is only used as a portal to enter CBRS.

Pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, as amended, records filed through Bank Secrecy Act (BSA) are covered by FinCEN's Privacy Act system of record notices, which were last published in their entirety on February 19, 2002, at 67 Fed. Reg. 7492, 67 Fed. Reg. 7496, and 67 Fed. Reg. 7498, respectively. Treasury/DO .212 and Treasury/DO .213 were subsequently amended on May 24, 2002, at 67 Fed. Reg. 36669. On November 25, 2003, FinCEN gave notice of proposed alterations to its three existing systems of record notice (SORN)entitled Treasury/DO .200--FinCEN Data Base--Treasury/DO, Treasury/DO .212--Suspicious Activity Reporting System--Treasury/DO, and Treasury/DO. 213-Bank Secrecy Act Reports System--Treasury/DO. No modification to the SORN is expected.

SECTION F ACCESS TO DATA

The general public cannot access the Secure Outreach system. It can only be accessed by authorized FinCEN personnel, as well as authorized personnel from designated federal, state, and, local law enforcement, intelligence, and regulatory agencies that have signed a MOU with FinCEN to allow access to the BSA information. The organization and corresponding MOU determine the type of accesses permitted to a user. The help desk maintains procedures for entering users into the system. The certified registrants are required to complete web-based security and legal training once every two years. All users are kept fully aware of their individual responsibilities regarding security procedures and regulations. All personnel receive an indoctrination that provides an understanding of the sensitivity of information, the threats to the computer and communications system, and the methods and requirements for controlling access to information and the system processing it. The indoctrination also includes information on how users can get help when having difficulty with the system and procedures for reporting security incidents.

The system shares limited data with the Gatedev control panel program and databases, which are only accessible internally. Secure Outreach stores training data in the Gatedev system and obtains status reports on the IRS's CBRS system. Both Gatedev and Secure Outreach fall under the umbrella of the BSA Data Services organization. Secure Outreach's internal data is not shared outside of the BSA Data Services organization.

Contractors operate the Secure Outreach system. All Secure Outreach personnel, i.e., all staff with system or information access, shall have a completed background investigation prior to having access to the system, and are required to acknowledge by signature, their agreement to adhere to FinCEN security policies and procedures prior to working on the contract. This includes signing a nondisclosure agreement and a yearly security awareness document. The contract includes specific security requirements required by law (FISMA, OMB, and Treasury). Senior help desk personnel enter new individuals into the system via a special administrative interface, which only they have access. Help desk personnel have their own administrative Web interface for reset using passwords and a linked in client server system for call logging. System administrators have access to the Sun Access Manager and the Directory Server (which is the main data store) only from a secured computer room.

The Secure Outreach COTR is responsible for the conduct and activities of the Contractor. FinCEN's ISSO provides security oversight for the Contractor and collaborates with the Program Manager on required security procedures and implementation. FinCEN security officials are allowed unrestricted access to conduct security site surveys and to perform duties associated with information systems security and information security oversight. FinCEN’s ISSO and Secure Outreach COTR will perform on-site system security reviews frequently for any signs of unauthorized system use/access attempts and indications of anomalous system or user behavior.

It has been determined that the results of this PIA do not require any additional technology or process changes to Secure Outreach.

The Following Officials Have Approved this Document

PIA REVIEWED BY PRIVACY ACT OFFICER, FINCEN:

SIGNATURE DATE

PIA REVIEWED BY SYSTEM OWNER, FINCEN:

SIGNATURE DATE

PIA REVIEWED BY CHIEF INFORMATION SECURITY OFFICER, FINCEN:

SIGNATURE DATE