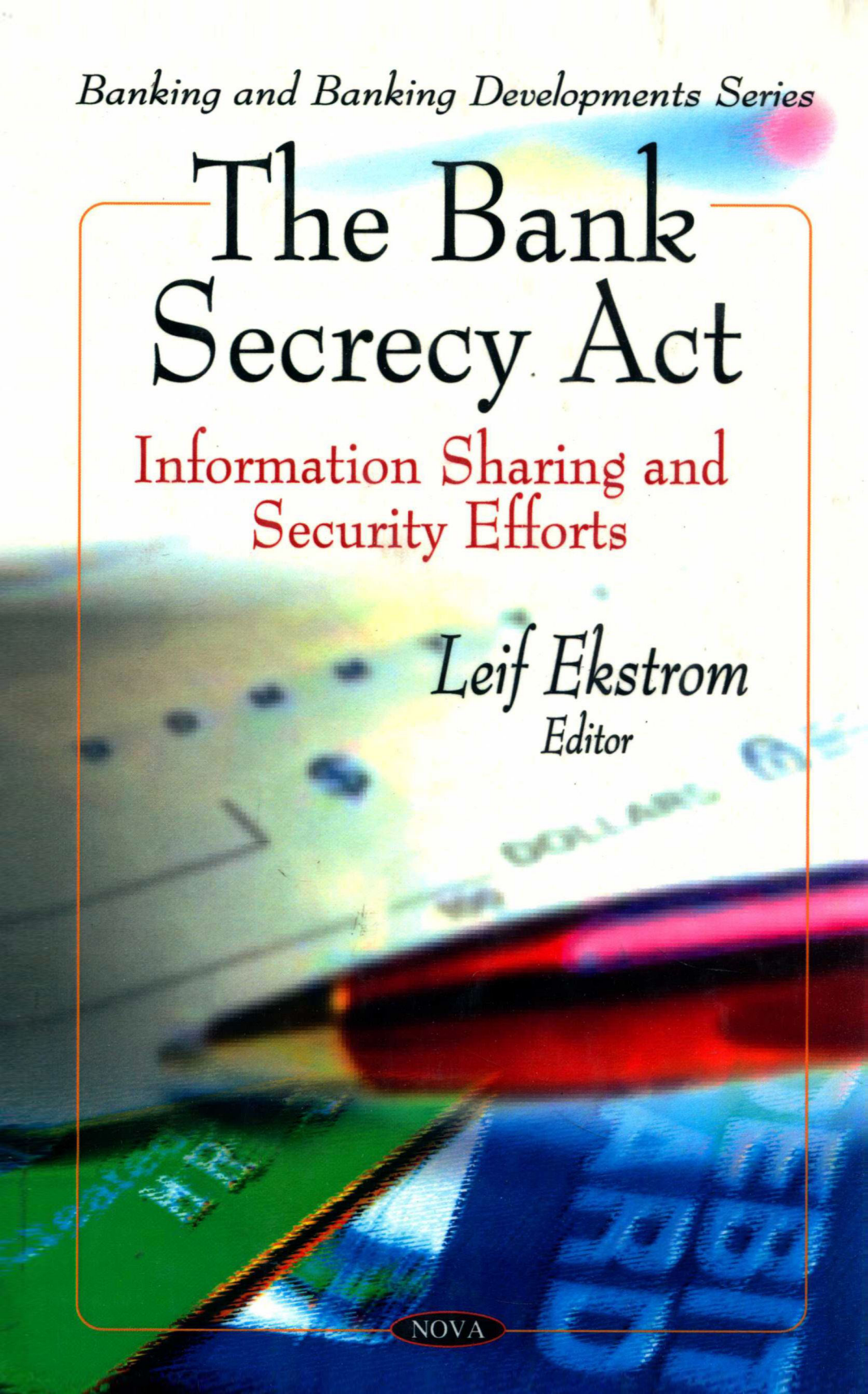
Banking and Banking Developments Series

The Bank Secrecy Act

Information Sharing and Security Efforts

Leif Ekstrom
Editor



NOVA

BANKING AND BANKING DEVELOPMENTS SERIES

THE BANK SECRECY ACT: INFORMATION SHARING AND SECURITY EFFORTS

LEIF EKSTROM
EDITOR

Nova Science Publishers, Inc.
New York

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

The Bank Secrecy Act : information sharing and security efforts / editor, Leif Ekstrom.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-60741-983-9 (hardcover : alk. paper)
1. United States. Currency and Foreign Transactions Reporting Act 2. Banks and banking--Records and correspondence--Law and legislation--United States. 3. Banks and banking--Security measures--United States. 4. Confidential communications--Banking--United States. 5. Banking law--United States. I. Ekstrom, Leif.
KF1030.R3B36 2009
346.73'082--dc22

2009036567

Published by Nova Science Publishers, Inc. ✦ New York

BANKING AND BANKING DEVELOPMENTS SERIES

THE BANK SECRECY ACT: INFORMATION SHARING AND SECURITY EFFORTS

BANKING AND BANKING DEVELOPMENTS SERIES

Financial Institutions in Turmoil
Carl D. Aspelin (Editor)
2010. ISBN: 978-1-60692-044-2

Finance and Banking Developments
Charles V. Karsone (Editor)
2010. ISBN: 978-1-60876-329-0

The Bank Secrecy Act : Information Sharing and Security Efforts
Leif Ekstrom (Editor)
2010. ISBN: 978-1-60741-983-9

PREFACE

This book explores the Bank Secrecy Act (BSA), which is a legislative framework for combating money laundering. The Financial Crimes Enforcement Network (FinCEN) is responsible for the administration of the BSA regulatory structure, and has delegated examination responsibility to the federal banking regulators. This book describes how BSA compliance and enforcement responsibilities are distributed, how agencies other than FinCEN are implementing those responsibilities and the evaluation of their coordination efforts. This book also discusses security policies and controls for systems at three organizations to evaluate whether security controls effectively protect the confidentiality, integrity and availability of the information and systems that support FinCEN's mission.This book consists of public documents which have been located, gathered, combined, reformatted, and enhanced with a subject index, selectively edited and bound to provide easy access

Chapter 1 - The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, relies extensively on its own computer systems, as well as those at the Internal Revenue Service (IRS) and the Treasury Communications System (TCS), to administer the Bank Secrecy Act (BSA) and fulfill its mission of safeguarding the U.S. financial system from financial crimes. Effective information security controls over these systems are essential to ensuring that BSA data, which contains sensitive financial information used by law enforcement agencies to prosecute financial crime, is protected from inappropriate or deliberate misuse, improper disclosure, or destruction.

GAO evaluated whether security controls that effectively protect the confidentiality, integrity, and availability of the information and systems that

support FinCEN's mission have been implemented. To do this, GAO examined security policies and controls for systems at three organizations.

Chapter 2 - The legislative framework for combating money laundering began with the Bank Secrecy Act (BSA) in 1970 and most recently expanded in 2001with the USA PATRIOT Act. The Financial Crimes Enforcement Network (FinCEN) administers BSA and relies on multiple federal and state agencies to ensure financial institution compliance. GAO was asked to (1) describe how BSA compliance and enforcement responsibilities are distributed, (2) describe how agencies other than FinCEN are implementing those responsibilities and evaluate their coordination efforts, and (3) evaluate how FinCEN is implementing its BSA responsibilities. Among other things, GAO reviewed legislation, past GAO and Treasury reports, and agreements and guidance from all relevant agencies; and interviewed agency, association, and financial institution officials.

CONTENTS

In: The Bank Secrecy Act: Information Sharing... ISBN: 978-1-60741-983-9
Editor: Leif Ekstrom

Chapter 1

INFORMATION SECURITY: FURTHER ACTIONS NEEDED TO ADDRESS RISKS TO BANK SECRECY ACT DATA

U. S. Government Accountability Office

WHY GAO DID THIS STUDY

The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, relies extensively on its own computer systems, as well as those at the Internal Revenue Service (IRS) and the Treasury Communications System (TCS), to administer the Bank Secrecy Act (BSA) and fulfill its mission of safeguarding the U.S. financial system from financial crimes. Effective information security controls over these systems are essential to ensuring that BSA data, which contains sensitive financial information used by law enforcement agencies to prosecute financial crime, is protected from inappropriate or deliberate misuse, improper disclosure, or destruction.

GAO evaluated whether security controls that effectively protect the confidentiality, integrity, and availability of the information and systems that support FinCEN's mission have been implemented. To do this, GAO examined security policies and controls for systems at three organizations.

WHAT GAO RECOMMENDS

GAO recommends that the Secretary of the Treasury direct the FinCEN Director to take several actions to fully implement an effective agencywide information security program. In commenting on a draft of this report, Treasury agreed to develop a detailed corrective action plan for each of the recommendations.

WHAT GAO FOUND

FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission; however, significant information security weaknesses remain in protecting the confidentiality, integrity, and availability of these systems and information. The three organizations implemented many information security controls to protect the information and systems that support FinCEN's mission. For example, IRS controlled changes to a key application and FinCEN segregated areas of its network. Nonetheless, the organizations had inconsistently applied or not fully implemented controls to prevent, limit, or detect unauthorized access to this information and these systems. For example, the organizations did not always (1) implement user and password management controls for properly identifying and authenticating users, (2) restrict user access to data to only what was required for performing job functions, (3) adequately encrypt data, (4) protect the external and internal boundaries on its systems, and (5) log user activity on databases. Furthermore, weaknesses in which systems were insecurely configured and patches were not applied to critical systems also existed. As a result, sensitive information used by the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing is at an increased risk of unauthorized use, modification, or disclosure.

A key reason for many of the weaknesses was that FinCEN and IRS had not fully implemented key information security program activities. For example, FinCEN did not always include detailed implementation guidance in its policies and procedures and adequately test and evaluate information security controls. Furthermore, GAO has previously reported that IRS did not sufficiently verify whether remedial actions were implemented or effective in mitigating vulnerabilities and recommended that it implement a revised remedial action verification process.

ABBREVIATIONS

BSA	Bank Secrecy Act
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TCS	Treasury Communications System
Treasury	Department of the Treasury
WebCBRS	Web-based Currency and Banking Retrieval System

January 30, 2009

The Honorable Barney Frank
Chairman

The Honorable Spencer Bachus
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable William Lacy Clay
House of Representatives

The Honorable Stephen F. Lynch
House of Representatives

As the administrator of the Bank Secrecy Act (BSA),[1] the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury (Treasury), is tasked with the mission of safeguarding the U.S. financial system from money laundering, terrorist financing, and other abuses. In fulfilling this mission, FinCEN performs analysis in support of law enforcement; issues regulations and enforces compliance with the BSA; facilitates information-sharing of BSA data; and coordinates with foreign counterparts.

FinCEN relies extensively on its own information systems, as well as on systems located at the Treasury components of the Internal Revenue Service (IRS) and the Treasury Communications System (TCS) to manage, store, and disseminate the data that financial institutions are required to report under the

BSA. These data contain sensitive information, including transaction amounts, account numbers, and social security numbers, and are used by law enforcement agencies investigating financial crimes, including terrorist financing and money laundering. The computer systems that support FinCEN's mission must be properly protected through strong information security controls[2] because a security breach could place sensitive financial and personally identifiable information at risk and allow criminals to subvert law enforcement's ability to detect illegal activity.

Our objective was to determine whether information security controls have been implemented that effectively protect the confidentiality, integrity, and availability of the information and systems that support FinCEN's mission. To accomplish this objective, we examined the information security controls at FinCEN and two organizations that operate systems or process and store data on its behalf—specifically, TCS and IRS. We concentrated our evaluation on the applications, databases, and network and mainframe infrastructure that support FinCEN's mission. We performed our review at FinCEN and TCS facilities in the Washington, D.C., metropolitan area and at an IRS computing center.

We conducted this performance audit from March 2008 to January 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. For more details on our objective, scope, and methodology, see appendix I.

RESULTS IN BRIEF

Although FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission, significant weaknesses existed that impaired their ability to ensure the confidentiality, integrity, and availability of these information and systems. The organizations have implemented many security controls to protect the information and systems. For example, FinCEN employed controls to segregate areas of its network and restrict access to sensitive areas, and IRS controlled changes to a key application in its BSA processing environment. However, weaknesses existed that placed sensitive

data at risk of unauthorized disclosure. The organizations did not always consistently apply or fully implement controls to prevent, limit, or detect unauthorized access to devices or systems. For example, the organizations had not consistently or fully (1) implemented user and password management controls for properly identifying and authenticating users, (2) restricted user access to data to permit only the access needed to perform job functions, (3) encrypted data, (4) protected external and internal boundaries, and (5) logged user activity on key systems. Shortcomings also existed in managing system configurations, patching systems, and planning for service continuity. As a result, increased risk exists that unauthorized individuals could read, copy, delete, add, and modify data and disrupt service on systems supporting FinCEN's mission.

A key reason for many of the weaknesses was that FinCEN and IRS had not fully implemented key information security program activities. For example, FinCEN did not always include detailed implementation guidance in its policies and procedures or adequately test and evaluate information security controls. Furthermore, IRS did not sufficiently verify whether actions taken to remedy or mitigate known vulnerabilities were fully implemented or effective.

To help strengthen information security controls over the information and systems supporting FinCEN's mission, we are making five recommendations to the Secretary of the Treasury to direct the Director of FinCEN to fully implement key information security program activities. We also are making 88 recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses at FinCEN, TCS, and IRS.

In commenting on a draft of this report, Treasury's Deputy Assistant Secretary for Information Systems and Chief Information Officer stated that securely maintaining BSA information contributes to the department's goal of promoting the nation's security through strengthened financial systems. He also stated that Treasury will provide a detailed corrective action plan for each of the recommendations and noted that many of the actions required to address the recommendations are already completed or under way.

BACKGROUND

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where

the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, they also pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Our previous reports, and those by inspectors general, describe serious and widespread information security control deficiencies that continue to place federal assets at risk of inadvertent or deliberate misuse, mission-critical information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,[3] a designation that remains in force today.[4]

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and systems within federal agencies.[5] FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risks; developing and implementing security plans, policies, and procedures; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

The BSA and FinCEN

The BSA, enacted by Congress in 1970, authorizes the Secretary of the Treasury to issue regulations requiring financial institutions to retain records and file reports useful in criminal, tax, and regulatory investigations. Following the September 11, 2001, terrorist attacks, Congress passed the USA PATRIOT Act, which, among other things, amended the BSA to expand the number of industries subject to BSA regulation and required financial institutions to establish proactive anti-money laundering programs to combat

terrorist financing.[6] In addition, the USA PATRIOT Act expanded reporting requirements and allowed the records and reports collected under the BSA to be used in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

As the administrator of the BSA, FinCEN, a bureau within Treasury, is tasked with the mission of safeguarding the U.S. financial system from money laundering, terrorist financing, and other abuses. In fulfilling this mission, FinCEN plays four key roles: (1) performing analysis in support of law enforcement; (2) issuing regulations and enforcing compliance; (3) facilitating information-sharing of BSA data; and (4) coordinating with foreign counterparts. Providing analysis was FinCEN's original mission when it was established in 1990, a role that it continues to perform. In its capacity as regulator, FinCEN develops regulations and delegates authority to eight other federal agencies to perform compliance examinations for BSA reporting requirements for referral to FinCEN, which retains enforcement authority. In terms of information-sharing, sections 361 and 362 of the USA PATRIOT Act mandate that FinCEN create and maintain networks to enable electronic filing of BSA reports and facilitate dissemination of the data to law enforcement and regulatory agencies. In addition, FinCEN participates in and promotes international collaboration and information-sharing among its foreign counterparts to detect and deter illicit financial activities. Between fiscal years 2002 and 2007, FinCEN's budget grew from $47.5 million to $73.2 million. According to FinCEN, this growth has taken place primarily because of the expansion of its regulatory functions.

Information That Supports FinCEN's Mission

FinCEN relies on information submitted under BSA reporting requirements to fulfill its mission. Specifically, FinCEN collects information submitted and disseminates it to law enforcement and regulatory agencies. The information primarily consists of Currency Transaction Reports and Suspicious Activity Reports that are filed by financial institutions. Currency Transaction Reports must be filed for any account cash withdrawals and deposits, currency exchanges, and wire transfers purchased with cash exceeding $10,000. Suspicious Activity Reports must be filed by financial institutions if a transaction involves or aggregates a minimum threshold[7] of funds or other assets and the institution knows, suspects, or has reason to suspect that the transaction is a violation of law. Law enforcement agencies use the information in these reports in combination with other information that they collect to link individuals and their activities, hinder activities, and

prosecute criminals. Financial regulators, such as the Federal Deposit Insurance Corporation and the National Credit Union Administration, use the information to examine financial institutions for compliance with the BSA.

Currency Transaction Reports and Suspicious Activity Reports contain highly sensitive, detailed information about the financial activity of private individuals[8] that is intended to help federal, state, and local law enforcement agencies in their investigations and, thus, potentially hinder criminal activity. Inappropriate disclosure, modification, or misuse of this information could undermine the ability of the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing.

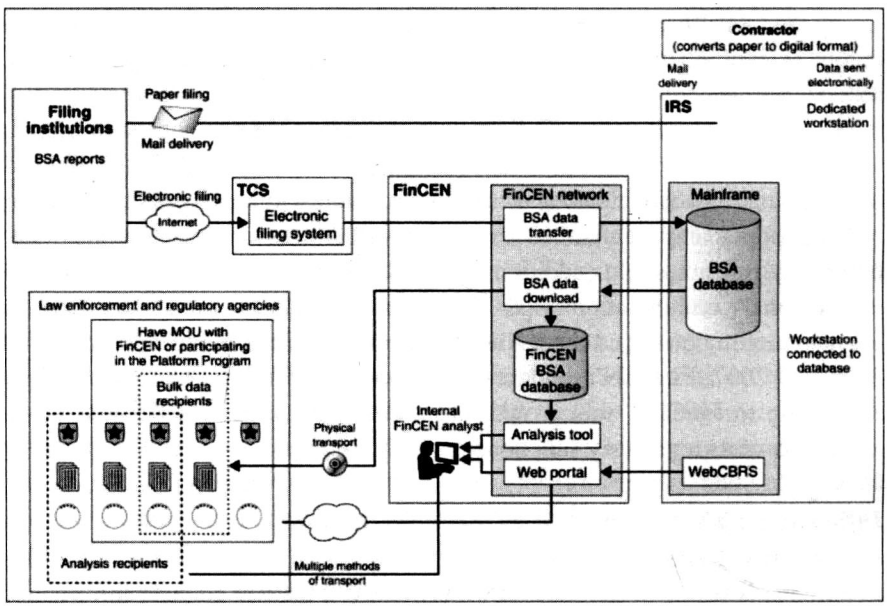


Figure 1 BSA Environment Operational Relationships and Data Flow

Information Systems That Support FinCEN's Mission

Information systems located at FinCEN, TCS, and IRS comprise the overall computing environment where BSA information is collected, processed, stored, disseminated, and protected in support of FinCEN's mission. In its own computing environment, FinCEN maintains a Web portal by which law enforcement agencies, regulatory agencies, and FinCEN employees access BSA data. It also has an analysis tool that it uses to provide analyses to law enforcement customers and a database containing a copy of the

BSA database maintained by IRS. These systems reside on FinCEN's network infrastructure. Additional systems are operated at TCS, including the electronic filing system and the supporting TCS network infrastructure. FinCEN's electronic filing system is operated on the TCS network under a hosting agreement. FinCEN also relies on systems operated by IRS, including the BSA database and the Web-based Currency Banking and Retrieval System (WebCBRS). WebCBRS and the database reside on a mainframe computer and supporting network infrastructure at an IRS computing facility

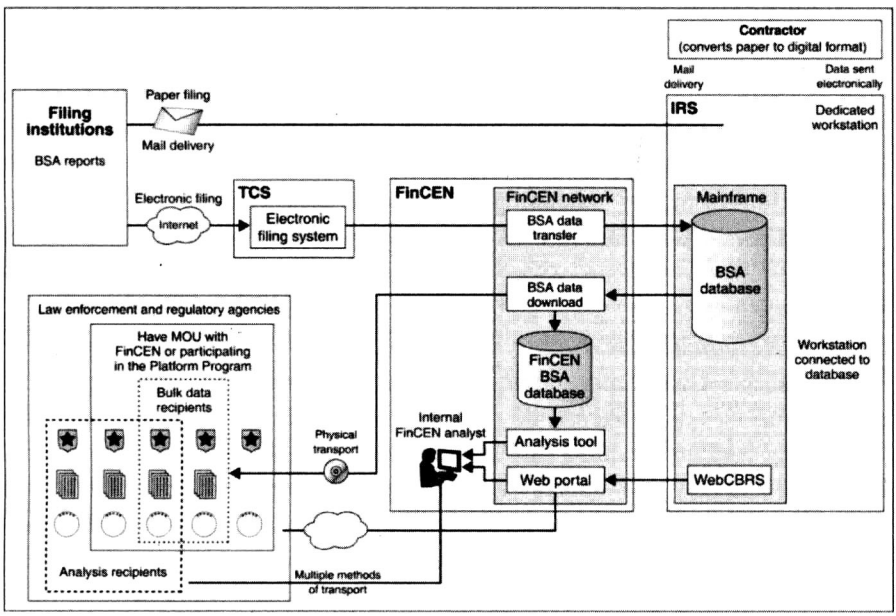


Figure 1. BSA Environment Operational Relationships and Data Flow

Information Flow in the BSA Environment

The information in BSA reports submitted by financial institutions comprise the data that is stored in the BSA database at IRS. Most reports[9] are submitted electronically, either singly or in batch form, over the Internet to the electronic filing system; FinCEN moves this data through its network infrastructure and passes them to IRS. Reports submitted in paper form are mailed directly to IRS; they are then forwarded to a contractor, who converts the reports into digital format and returns them electronically. IRS personnel then manually upload the data to the database.