



# Audit Report



OIG-06-030

TERRORIST FINANCING/MONEY LAUNDERING: FinCEN Has Taken Steps to Better Analyze Bank Secrecy Act Data But Challenges Remain

May 18, 2006

Office of  
Inspector General  
Department of the Treasury



# Contents

---

<b>Audit Report</b> .....	3
Results in Brief .....	4
Background .....	6
Findings and Recommendations .....	10
FinCEN Is Performing More Complex Analysis in Line with PATRIOT Act Requirements but Needs to Better Plan and Measure the Effort .....	10
Recommendations .....	20
The FinCEN Database Cannot Be Relied On for Accurate and Complete Data .....	21
Recommendations .....	30
Improved Internal Controls Are Needed to Protect BSA and Other Data.....	32
Recommendations .....	35

## Appendices

Appendix 1:	Objectives, Scope, and Methodology .....	38
Appendix 2	FinCEN's Analytics Division .....	40
Appendix 3	Descriptions of Several Software Packages Used by FinCEN Analysts .....	43
Appendix 4:	Management Response .....	46
Appendix 5:	Major Contributors to This Report .....	51
Appendix 6:	Report Distribution .....	52

## Abbreviations

ASIS	Analytical System for Investigative Support
BSA	Bank Secrecy Act
CBRS	Currency and Banking Retrieval System
DEA	United States Drug Enforcement Administration
EDS	Electronic Data Systems
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit

---

HIFCA	High Intensity Money Laundering and Related Financial Crime Area
NACLC	National Agency Check with Local Record Check
IRS DCC	Internal Revenue Center Detroit Computing Center
PAR	Performance and Accountability Report
SAR	Suspicious Activity Report
SQS	Suspicious Activity Report Query System

---

*The Department of the Treasury  
Office of Inspector General*

May 18, 2006

Robert W. Werner  
Director  
Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network (FinCEN) was established in April 1990 to provide a government-wide, intelligence and analytical network to support the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes. In May 1994, FinCEN assumed responsibility for administering the Bank Secrecy Act (BSA), a law enacted to help deter, detect, and investigate money laundering. The USA PATRIOT Act of 2001 elevated FinCEN to bureau status and required FinCEN to furnish research, analytical, and informational services to financial institutions and appropriate law enforcement authorities to fight terrorism, organized crime, and money laundering.

The objective of our audit was to determine the extent to which FinCEN performed complex analyses of BSA and other data intended to provide law enforcement with new leads or clues regarding individuals, entities, and organizations engaging in terrorist acts or money laundering. The report also discusses issues we identified with FinCEN's case management information system, known as the FinCEN Database, and with certain weaknesses we identified with data security controls.

We conducted our fieldwork between September 2004 and July 2005 at FinCEN Headquarters in Vienna, Virginia and in Washington, D.C. We reviewed applicable laws and regulations related to FinCEN's duties and responsibilities. We also reviewed FinCEN's strategic plan, annual and performance and accountability reports, standard operating procedures, and studies related to case processing and data analysis. We interviewed officials from

---

FinCEN's Analytics Division and Client Liaison and Services Division<sup>1</sup> in Vienna, Virginia, and the Regulatory Policy and Program Division in Washington, D.C. We selected and reviewed a random sample of FinCEN Database cases from an electronic data file for fiscal years 2003, 2004, and the first quarter of 2005, and reviewed corresponding documentation to assess the status, completeness, and timeliness of FinCEN's products. We examined the analytical nature of FinCEN's products, and the methods, tools, and techniques FinCEN used to conduct its data analysis. A more detailed description of our objectives, scope, and methodology is provided as appendix 1.

## Results in Brief

FinCEN's strategic plan includes several key objectives for adding value to its analytical program. One objective in FinCEN's fiscal years 2006-8 plan was to adjust its support of law enforcement investigations by performing complex data mining and analysis.<sup>2</sup> FinCEN planned to increase its analytic products while reducing time spent in routine data retrieval. This strategy was designed to shift FinCEN's effort from routine data retrieval (reactive cases) to complex data mining (proactive cases). The Department of the Treasury's Office of Performance Budgeting (OPB) approved a measure for fiscal years 2005-6 to evaluate FinCEN's efforts: the percentage of FinCEN's customers finding FinCEN's analytical support valuable. In November 2005, the Department of the Treasury reported in its FY 2005 Performance and Accountability Report (PAR) that 73 percent of FinCEN's customers found the support valuable.

Though the results were favorable, this measure did not comprehensively assess FinCEN's complex data mining and analysis. We were unable to assess the support for fiscal year 2005 results, but by reviewing fiscal year 2004 customer response data, also largely favorable, we found that a large percentage of the input was related to the results of reactive case work and included very limited data related to proactive cases.

---

<sup>1</sup> This division was renamed to the Information and Technology Division following our audit.

<sup>2</sup> Data mining for FinCEN is the process of analyzing BSA, law enforcement, and commercial data to identify possible terrorist financing, money laundering, and other criminal activity.

---

FinCEN has taken steps to increase its use of analytic tools and methods for identifying trends and patterns in BSA data. However, we reviewed FinCEN's analytic data for fiscal years 2003 through the first quarter of 2005 and found that FinCEN had made limited progress in increasing its complex data mining and analysis (i.e., proactive case work). Proactive case work increased during this period, from 6 percent of FinCEN's analytical case work in 2003 to 10 percent in 2005 as reported in the Department of the Treasury's fiscal year 2005 PAR. Filling law enforcement requests for specific information, known as reactive case work, continued to be FinCEN's focus.

FinCEN's effort to conduct more complex analysis was hindered in 2004-5 by the release of all 63 of its contractor employees. These employees had been handling about a third of FinCEN's reactive case work and, upon release, this work was reassigned to FinCEN's analysts. The contractor employees were released by October 2004 because their employers did not complete FinCEN's required upgrade of the employees' security clearances. Because release of the contractor employees resulted in a case backlog, FinCEN informed law enforcement agencies in February 2005 that routine domestic data requests, both existing and future, would be processed only when FinCEN's analysts had time available. In March 2005, under a new contract, FinCEN began to rebuild the contractor staff, bringing on board 10 contractor employees with Top Secret clearances.

As we requested data on FinCEN's efforts and results, we found that the bureau did not have reliable management information to assess FinCEN's analytical work. FinCEN uses the FinCEN Database to determine the status of its products and to report the results of its case work in both its annual report and The Department of the Treasury PAR. Included in these reports are the number of investigative cases, subjects, and strategic analytic products. However, we found that the data were not always accurate or reliable. We also found that the Database did not always contain information about the timeliness of work or resources used. Data problems resulted from a combination of system weaknesses that made it difficult to develop summary data, and data recording errors that occurred when analysts did not record data in accordance with standard operating procedures. FinCEN also made

---

changes in how data were categorized from year to year, which required us to re-categorize certain data to ensure comparability.

In addition to data management issues, we found that certain internal controls over BSA and law enforcement data were weak and could allow these data to be compromised. First, as of July 2005, FinCEN had not scheduled 28 of 66 required on-site inspections due in fiscal year 2005, in accordance with its Gateway Inspection Policy and Procedure. Gateway is a system used by law enforcement to remotely access BSA data and FinCEN performs on-site inspections of user sites to determine whether system use is proper.<sup>3</sup> Second, FinCEN has neither a policy nor a methodology to review internal analyst queries for possible misuse or abuse or to prevent and detect browsing of BSA and law enforcement data. Although we did not identify inappropriate use, we believe internal users represent an inherent risk and that a policy and methodology for monitoring would be a beneficial control. Third, after FinCEN increased the security level requirement for its contractor employees, they were allowed to access sensitive but unclassified BSA and other data, even though they had not yet obtained the proper clearances.

We made several recommendations to FinCEN to improve the bureau's management of its analytical program, strengthen the case management system, and improve data security controls. The specific recommendations are presented in the body of the report. FinCEN concurred with our recommendations and has either completed action or established target dates for completion.

## **Background**

### **Section 361 of the USA PATRIOT Act**

On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107-56). Section 361 of the act added a new section 310 to Subchapter I of chapter 3, title 31, of the United States Code that defines FinCEN's duties to analyze BSA data and

---

<sup>3</sup> FinCEN provided data following our exit conference which showed the bureau completed these inspections during the last quarter of fiscal year 2005 (23) and the first quarter of 2006 (4).



---

disseminate the data to financial institutions and appropriate law enforcement authorities. These data are for use in identifying, preventing, and prosecuting terrorism, organized crime, and money laundering. In addition, the act requires FinCEN to determine emerging trends and methods in money laundering and to support intelligence activities against international terrorism.

### **FinCEN's Analytics Division**

As of January 2005, FinCEN employed 98 analysts in its Analytics Division, which is composed of the Office of Law Enforcement Support, Office of Regulatory Support, and Office of Global Support. Under a July 2004 reorganization, analysts are expected to handle all types of cases, including both routine data requests and proactive case work.<sup>4</sup> (See appendix 2 for organizations charts and descriptions of each office.) Intelligence research specialists and law enforcement staff support financial criminal investigations through research and analysis of information. FinCEN also employs contractor staff to do research, primarily for the routine request for information cases.

FinCEN's Analytics Division works closely with the bureau's Client Liaison and Services Division to coordinate these efforts. The Client Liaison and Services Division trains federal, state, and local agencies to access data via FinCEN's Gateway system, which gives users direct access to BSA reports, and monitors use of the system. When two or more agencies query the same subjects, the Division links the agencies, enabling them to coordinate their investigations.

### **Databases Used**

Several databases are available to FinCEN analysts conducting research and analysis.

- The FinCEN Database contains subjects or businesses FinCEN has researched in its commercial, financial, and law

---

<sup>4</sup> Before the reorganization, the Division was organized by the types of products produced, including tactical, strategic, or PATRIOT Act 314 requests. The Office of Investigative Support provided tactical support (focused on individuals and entities, i.e., subjects) and PATRIOT Act 314 requests (focused on information sharing between law enforcement and financial institutions) and the Office of Strategic Analysis offered analytical support (focused on particular topics, such as money laundering).

---

enforcement databases. This database includes investigative and intelligence cases, financial institution Hotline tip cases,<sup>5</sup> and strategic analysis cases; assigns a number for each entry; and contains data such as the number of subject(s), date of request, date entered, date started and ended, case status (such as open or closed), and case type. As such, the FinCEN Database not only provides FinCEN with the ability to track resources used to develop cases but also is an analytical resource for conducting research on new subjects.

- External financial, law enforcement, and commercial databases are used for responses to requests for research and for performing data analysis. Financial databases include the Currency and Banking Retrieval System (CBRS), which houses BSA Currency Transaction Reports for transactions greater than \$10,000 and Suspicious Activity Reports (SAR) from institutions citing suspicious financial transactions. Another financial database is the Currency and Banking Query System, which allows users to query narrative information contained in the SARs. The Treasury Enforcement Communications System contains useful law enforcement data and provides access to the National Crime Information Center and National Law Enforcement Telecommunications Center. Other law enforcement databases include the U.S. Drug Enforcement Administration Narcotics and Dangerous Drug Information System and U.S. Postal Inspection Database. Commercial databases, such as Dun and Bradstreet Worldbase, are also used.

### **Users of FinCEN's Analytical Data**

Users of FinCEN's analytical data include federal, state, local, and foreign law enforcement agencies. Other users include Congress,

---

<sup>5</sup> FinCEN's Financial Institution Hotline allows financial institutions to expeditiously contact FinCEN directly about any suspicious activity related to terrorism. If the tip involves an imminent threat, FinCEN instructs the financial institution to contact the nearest Federal Bureau of Investigation (FBI) office, and FinCEN forwards the information to other law enforcement agencies, such as the U.S. Office of Immigration and Customs Enforcement (ICE), Internal Revenue Service Criminal Investigative Division (IRS-CID), and Treasury's Office of Intelligence and Analysis. FinCEN then searches financial and law enforcement databases using names, accounts, addresses, and other identifiers provided from the Hotline tip and prepares a written report with results and conclusions for law enforcement. Hotline tip cases are not coded separately in the FinCEN Database.

---

FinCEN's Regulatory Policy and Programs Division, and federal bank regulatory agencies.

Certain regulatory and law enforcement agencies house individuals at FinCEN to conduct research. These are known as Platform Users and are generally short-term. Detailees or Representatives are similar, but use FinCEN data resources for longer periods of time.

*Gateway* users include employees of federal law enforcement agencies, state and local police, and states' attorneys general, district attorneys, bureaus of investigations, and departments of public safety who access BSA reports in the CBRS financial database from their own locations. Gateway, which is managed by the Client Liaison and Services Division, allows investigators to conduct their own research and analysis of BSA data, rather than relying on FinCEN's resources. Gateway has a feature that automatically signals FinCEN when two or more agencies have an interest in the same subject. This feature allows FinCEN to assist participating agencies in coordinating their investigations.

Users of FinCEN analytical data also include teams that consist of FinCEN analysts working on cases in federally designated high-intensity money laundering zones around the country, known as High Intensity Financial Crimes Areas (HIFCA). The purpose of these zones is to concentrate law enforcement efforts at the federal, state, and local level to combat money laundering.

### **BSA Direct**

FinCEN awarded a contract to Electronic Data Systems (EDS), a global information technology services company, to design, develop, implement, and provide Web-hosting and support services for a new information storage and delivery system called BSA Direct. FinCEN believes BSA Direct, which will replace the Gateway system, will enhance how data collected under the BSA are stored, accessed, and utilized. Through BSA Direct, FinCEN plans to provide authorized law enforcement and financial regulatory organizations with Web-based access to BSA data and improved analytical tools to ensure these data are fully and appropriately used, while preserving information security. On March 15, 2006, FinCEN's Director issued a temporary "stop work" order for BSA Direct and ordered FinCEN staff and BSA contractor, Electronic

---

Data Systems to pause for up to a 90-day period. He stated concerns with the project repeatedly failing to meet its performance milestones.<sup>6</sup>

## Findings and Recommendations

### Finding 1 **FinCEN Is Performing More Complex Analysis in Line with PATRIOT Act Requirements but Needs to Better Plan and Measure the Effort**

Since passage of the USA PATRIOT Act, FinCEN has attempted to conduct more complex investigative case analysis to better combat terrorist financing and money laundering threats. This is consistent with FinCEN's strategic plan, which directs FinCEN toward producing more analytical products in lieu of routine data retrieval. FinCEN established several performance measures to internally evaluate its analytical efforts, one of which—customer satisfaction with FinCEN's analytical products—was approved for the fiscal year 2005 PAR. According to FinCEN's 2005 PAR, 73 percent of respondents reported themselves satisfied on this measure. Though we did not assess the support for the 2005 results, our review of customer satisfaction data from fiscal year 2004 indicated that few customers responded and most of the responses dealt with routine data retrieval (*reactive* cases). As a result, these customer response data were of little use in evaluating complex analysis (*proactive* cases).

Although FinCEN has taken the initiative to improve analytical tools and methods to allow for increased proactive work, progress in achieving this goal has been slow. FinCEN's proactive cases increased from 6 percent of total cases in fiscal year 2003 to 10 percent in 2005.<sup>7</sup> Despite the modest increase, however, several of FinCEN's proactive cases referred potentially important information to enforcement agencies.

---

<sup>6</sup> FinCEN's Director provided this information regarding the BSA Direct project in a March 15, 2006 letter to the Chairman of the U.S. Senate Committee on Banking, Housing and Urban Affairs.

<sup>7</sup> We cannot attest to the validity of these data because we found that the data source, the FinCEN Database, is unreliable. See finding 2.

---

FinCEN's effort to increase its proactive case work was slowed when the bureau, upon realizing that contractors were handling increasingly sensitive information, increased contractor employee security level requirements from Secret to Top Secret. FinCEN imposed an October 2004 deadline on contractors to get their employees upgraded, but contractors were unable to meet the deadline. As a result, by October 2004 FinCEN released all contractor employees. These employees had been conducting over one-third of FinCEN's reactive case work, and their release resulted in a reactive case backlog. To enable its own analysts to continue working on higher-priority proactive cases, FinCEN informed law enforcement agencies in February 2005 that existing and future domestic, non-terrorism and non-complex requests would be re-evaluated and processed as the analysts could work the cases.

### **FinCEN's Strategic Plan Focuses on Adding Value to the Analytical Program**

FinCEN's Strategic Plan for fiscal years 2006-8, which discusses FinCEN's approach to achieving its mission during this period, includes a specific goal to combat terrorism, money laundering, and other financial crime through analysis of BSA data and other relevant information. Under this goal are several strategic objectives:

- expanding the production of analytic products that incorporate analysis of relevant classified information
- producing policy-level assessments of terrorist financing and money laundering threats that combine BSA data with other information sources
- adjusting FinCEN's support of law enforcement investigations to better reflect FinCEN's increased capabilities to perform complex data mining and analysis
- applying analytical resources to support regulatory activity concerning the BSA

Within these objectives are numerous strategies that provide a framework for how FinCEN intends to accomplish its objectives. For example, FinCEN plans to increase the number of analysts with

---

full access to classified data, provide analysts the knowledge and skills necessary to expertly analyze information, reduce the time spent by analysts on routine data retrieval, and increase the number of analytic products supporting law enforcement investigations.

To lay the groundwork for meeting the plan's objectives, FinCEN established four performance measures for its Analytics Division for fiscal year 2005. Treasury's OPB approved one of these measures for inclusion in the fiscal year 2005 PAR: the percentage of customers finding FinCEN's analytic support valuable.<sup>8</sup> In November 2005, Treasury reported that 73 percent of the customers found FinCEN's support valuable. The other measures, used for internal purposes, included the following:

- percentage of complex analytic work completed by FinCEN analysts (10 percent goal and 10 percent actual)
- median time from date of receipt of terrorist financing SAR or Financial Institution Hotline Tip SAR to referral of a written analytical report to law enforcement or the intelligence community (80 days goal and 77 days actual)
- average time expended to perform financial institution review dealing with compliance issues in response to memoranda of understanding with regulatory agencies (65 days goal and 62 days actual)

Because fiscal year 2005 PAR data supporting the above measures was not complete at the time of our fieldwork, we reviewed data for fiscal years 2003-4 and the first quarter of fiscal year 2005. We found that we could not verify case summary completion or timeliness data produced by FinCEN's case management system. This is discussed in detail in finding 2 of this report. In reviewing customer feedback data, we found the data of limited value because FinCEN had a low customer response rate, lacked a formal

---

<sup>8</sup> OPB encourages the bureaus to administer their programs in a manner that ensures that programs achieve desired results. According to OPB, "If the answer [about whether a program is meeting its desired outcomes] is 'no' or 'we don't know,' they [management] must do something about it, such as clearly define the desired outcomes, determine the causes of unsatisfactory performance, construct plans to remedy any problems, develop aggressive timeframes for taking action, and ensure that actions are implemented."

---

system to accumulate and monitor the results, and had little information available concerning the value of FinCEN's proactive analysis to law enforcement. This is discussed in more detail below.

### **Customer Response Data Are Not Formally Documented and Provide Little Useful Information to Assess Complex Analysis**

The FinCEN strategic plan cites the use of customer ratings as a means of measuring the quality of its analytic products. However, the response rate to FinCEN customer survey forms included with each of its case reports has also been low. FinCEN also does not have a formal reporting system to accumulate and monitor the results derived from customer response forms provided with each of its case reports. To compensate for the low response rate, FinCEN requested information through email and telephone surveys. FinCEN's Office of Regulatory Support, which performs institutional trend analysis, has an informal process to record responses to surveys provided to institutions.

FinCEN includes customer response forms with each of its completed case reports. We found two versions of a customer response form for reactive cases and one form for proactive cases. FinCEN forms asked customers if (1) the bureau adequately responded to their requests, (2) more analytical support would have been useful, (3) the information was timely, (4) the information was shared with other agencies, and (5) they were satisfied overall with the services provided by FinCEN. One of the two versions of the form for reactive cases also asked customers to identify the ways in which information provided by FinCEN assisted investigations. The brief proactive form asked whether the information FinCEN provided was used to open a case or assign a preliminary investigation or was retained for future use. FinCEN also asked if the information assisted the agency.

In addition to the lack of a formal reporting system for responses to FinCEN customer response forms, the number of completed forms returned to FinCEN, particularly involving proactive cases, has been low. For fiscal year 2004, for example, FinCEN received information on 582 cases out of 6,270, or 9 percent, and the vast majority of the 582 cases, 493, involved routine reactive case

---

work.<sup>9</sup> We found 51 responses related to proactive cases, which we believe were so few in number that they may have been of limited value to FinCEN in enhancing complex analyses.

Although the number of forms that FinCEN received was low, feedback has been positive. Based on our review of customer response forms returned for 2004 cases, we found that by and large FinCEN's customers were satisfied. We found only isolated instances of customer concerns. In 6 of the 493 reactive cases, customers reported that FinCEN's product was either untimely or did not satisfy the request. However, in 6 of the 51 proactive cases, customers reported that the product did not assist the agency.

Agency and FinCEN officials offered explanations for the low response rate. A law enforcement agency official who serves as a liaison to FinCEN commented that customers can be so focused on the information FinCEN provides they overlook the customer response form. A FinCEN Associate Director said that the feedback process may request a response before an investigator has fully assessed the importance of the information. However, FinCEN's Assistant Director of Client and Liaison Services Division told us that FinCEN has also not been successful in obtaining responses using follow-up letters.

### **FinCEN Has Taken Initiatives to Enhance Data Analysis**

FinCEN has taken steps to increase its use of analytic tools and methods for identifying trends and patterns in BSA data.<sup>10</sup> For example, FinCEN made software such as VisuaLinks, Suspicious Activity Report Query System (SQS), Analytical System for Investigative Support (ASIS), MapInfo, and Analyst's Notebook available to its analysts to develop their cases. These tools allow analysts to link related data, including links among people, transactions, and locations, and to identify trends. (See appendix 3

---

<sup>9</sup> FinCEN included in this information 38 completed customer response forms for HIFCA, Platform, Office of Global Support, and Office of Regulatory Support cases. These cases were neither reactive nor proactive.

<sup>10</sup> FinCEN is hampered in this effort, however, by the fact that FinCEN cannot add any data query tools to the current Gateway system because the BSA data are housed in an Internal Revenue Service computer system. According to FinCEN, this will change when FinCEN transitions from Gateway to BSA Direct.



---

for further description of the software.) Also, in 2004, FinCEN created a Counter-Terrorism SAR Review Program. FinCEN maintains three analysts and a team leader to search SARs for terrorist-related activity. They monitor and review SARs filed on activity indicative of terrorism and proactively develop cases for referral to law enforcement and intelligence.<sup>11</sup>

In addition, FinCEN's Technology Working Group, established in January 2005, is developing an in-house system to allow more uniform analysis of BSA data. The group is currently working to convert large downloads of text file BSA data from the Internal Revenue System Detroit Computing Center (IRS DCC) into meaningful reports and summaries.

Moving forward, FinCEN wants to eliminate information requests that can be performed by the customers and to focus on performing data analysis. Toward this end, FinCEN intends to transition more customers to FinCEN's Gateway system for simple data requests and has sought to provide additional information to law enforcement users about other users' information requests involving the same subjects. FinCEN refers to the process by which it notifies agencies that the same individuals or businesses have been the subject of previous research requests as Networking. Ultimately, FinCEN wants to move customers to BSA Direct so they can more easily conduct their own research. FinCEN is working with both the MITRE Corporation and EDS, the BSA Direct contractor, to explore new text mining software that will simplify and enhance user access to BSA data.

### **Proactive Cases Remain a Small Percentage of Total Cases**

While FinCEN categorizes its analytical cases in several different ways, FinCEN's analytical workload consists mainly of either reactive cases--responses to requests for information--or proactive cases--complex analyses to target potential money laundering and terrorist financing activities. A reactive case generally involves particular people or entities and is based on a law enforcement request that can be satisfied with simple queries of FinCEN's

---

<sup>11</sup> Because FinCEN did not have a unique category in the FinCEN Database for cases handled by the Counter-Terrorism SAR Review Program, we were unable to determine the number of cases handled by this team of analysts.

---

financial, law enforcement, and commercial databases. Work on certain types of reactive cases is done by FinCEN's in-house analysts and work on others is done by contractors.<sup>12</sup>

A proactive case generally involves developing new information about possible terrorist financing, money laundering, or other criminal activity through the analysis of BSA, law enforcement, and commercial data. FinCEN has been attempting to increase its proactive case work. Despite its efforts, proactive cases made up a small percentage of FinCEN cases in fiscal years 2003-5. In fiscal year 2003, proactive cases represented 6 percent of case work. In 2004, this percentage rose to 8 percent. In 2005, FinCEN reported that proactive cases increased to 10 percent of total cases.

FinCEN established a goal of 10 percent for 2005.<sup>13</sup> FinCEN believed this goal would help allow the bureau to assess its efforts to increase complex analysis. FinCEN's goal is 25 percent for 2006 and 50 percent for 2007.

### **Proactive Cases Have Evolved Over Time**

Since September 11, 2001, FinCEN has adjusted the focus of its proactive case work to account for the threat associated with terrorist financing. FinCEN's analytical efforts were re-focused on identifying terrorist funding activities. Analysts searched SARs using key words and geographic areas associated with terrorism.

In 2004, FinCEN's Counter-Terrorism SAR Review Program assigned analysts to review SARs indicative of terrorism and to refer possible terrorism-related SARs to the original requestors or recipients of information on those subjects. However, according to a FinCEN Assistant Director, agency feedback on these types of cases was so minimal that FinCEN was unable to determine if its efforts were producing useful information for the agencies. Therefore, instead of sending reports to agencies that may not be

---

<sup>12</sup> FinCEN also has levels of research associated with these cases. These are referred to as Tier 1, Tier 2, and Tier 3. Tier 1 addresses a basic request for a specific subject, and Tier 2 is more complex and involves additional related subjects. Tier 3 research involves additional subjects beyond Tier 2 and cases identified from FinCEN's research and analysis.

<sup>13</sup> Fiscal year 2005 was the first year FinCEN established a goal for the percentage of complex analysis cases.

---

interested in receiving the information, FinCEN has been working with federal agency representatives to solicit their input on more meaningful areas for developing leads. FinCEN believes this will increase the likelihood that an agency will follow the lead and open its own case.

FinCEN is also commissioning an analytic team to begin the “SAR Mapping Project” to tag SAR clusters by type of activity, geographic scope, HIFCA links, number of subjects, number of accounts, foreign involvement, and other factors to be developed by the team. FinCEN hopes this will allow the bureau to better focus analyst efforts. FinCEN had not produced results from this effort at the time of our audit.

### **Though Limited, FinCEN’s Evolving Proactive Case Work Has Referred Potentially Important Cases to Law Enforcement**

In our case review, we found evidence that FinCEN’s proactive case referrals could benefit law enforcement. The eventual results, however, would depend on what law enforcement was able to accomplish once the analyses were received. We identified the following case referrals from cases FinCEN provided to law enforcement agencies:

- Analysts identified suspicious check and wire transfer activity involving a pharmaceutical company and its owners. Several checks from the subjects’ accounts were deposited in high-risk countries. FinCEN forwarded the information to liaisons at the FBI and ICE.
- Using the search criterion “money remitter,” an analyst conducted an analysis of SAR narratives filed in fiscal years 2003 and 2004 to pinpoint money service businesses that might be engaging in suspicious activity.<sup>14</sup> The results were forwarded to IRS.
- In a case performed pursuant to FinCEN’s Counter-Terrorism SAR Review Program, an analyst found 19 additional SARs that were filed on the subject. The information from these

---

<sup>14</sup> FinCEN defines money services businesses as including the following five types of financial services providers, as well as the U.S. Postal Service: (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler’s checks, money orders, or stored value; (4) sellers or redeemers of traveler’s checks, money orders, or stored value; and (5) money transmitters.

---

additional SARs was forwarded in a memorandum to the requester.

- A FinCEN analyst took three original subjects from a prior 314(a) case<sup>15</sup> request of ICE and searched financial, commercial, and law enforcement databases for additional information. The analyst's search for these three subjects yielded four additional SARs in which they were named, and these four SARs identified six additional subjects. This information was referred to ICE.

### **FinCEN Has Experienced a Backlog of Reactive Cases**

Over the past decade, FinCEN has filled information requests from law enforcement agencies and the regulatory and financial communities. FinCEN accomplished this work with help from contractors. As FinCEN has moved more of its analysts to proactive work, contractors have become important in meeting requestor needs. However, in fiscal year 2004, FinCEN reorganized and increased BSA data security requirements, which included elevating the contractor security clearance level from Secret to Top Secret.

When FinCEN's contractors (who brought 63 employees on board from 1992 through 2004) were unable to furnish FinCEN with Top Secret clearances for their employees by October 2004, the employees were released. Consequently, FinCEN no longer had contractors available to handle reactive cases, and a backlog of cases developed. In February 2005, FinCEN's data showed 526 cases awaiting completion, including 344 waiting to be started.<sup>16</sup>

---

<sup>15</sup> Law enforcement can send what are known as 314 (a) requests to FinCEN to forward to financial institutions to locate accounts and transactions of subjects who may be involved in terrorism or money laundering. The financial institutions query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. The financial institution notifies FinCEN if a match is found for the named subject and provides point-of-contact information. The financial institutions have 2 weeks from the transmission date of FinCEN's request to respond.

<sup>16</sup> This information is from a FinCEN Database report of bi-monthly inventory counts of cases categorized as started, not started, opened, and closed. The reliability of this information may be questionable because we found handwritten numbers on these reports that were not reflected in the case numbers generated from the system. Also, cases were omitted from the report because the dates were "misaligned" in the system, meaning that the start and close dates were out of sequence. Considering these anomalies, we cannot attest to the accuracy of the case numbers reported.

---

To compensate, in February 2005 FinCEN placed a moratorium on non-terrorist related reactive case work. The moratorium required agencies to do research on domestic non-terrorism cases, using their own access to the data, freeing FinCEN analysts to perform more proactive analytical work. FinCEN officials envisioned that requests for non-terrorism research would decrease following the moratorium.

Although FinCEN made some progress in reducing this workload, the backlog was not entirely eliminated. As of July 2005, FinCEN reported 170 unassigned domestic non-terrorism requests dating back to December 2004.

At the time of our audit, FinCEN was in the process of transitioning agencies with low-priority case support work to researching their own cases via the Gateway system. From March through July 2005, FinCEN also hired 10 contractor staff with updated security clearances to assist with these requests. Although the number of incoming domestic requests declined, FinCEN was not able to eliminate the backlog.

### **Task Force Recommended Change**

In November 2004, FinCEN's Case Management Task Force, established to review analytical processes and services, recommended short-term priorities and long-term strategies to maximize client benefit and increase the value and impact of future FinCEN products. For the short-term, the Task Force recommended prioritizing work, empowering law enforcement users to handle their own requests, developing policies for the future, and streamlining the processing of requests. For the long-term, the Task Force recommended developing strategies to increase responsiveness to customers and developing FinCEN's Intelligence Research Specialists through training and experience. At the time of our review, we could not assess how well FinCEN had addressed these recommendations.

### **Conclusions**

FinCEN has found it difficult to increase the number of proactive analytic products supporting law enforcement investigations that

---

incorporate complex analysis. Nonetheless, FinCEN's analysts appear to have referred potentially important information to law enforcement. Because of continuing requests from law enforcement for case support, coupled with the release of contractors who had been working reactive cases, FinCEN needs to find ways to ensure that its analysts can continue to work proactive cases. In this regard, FinCEN should continue to direct law enforcement to Gateway and, when available, the BSA Direct system.

### **Recommendations**

We recommend that the Director of FinCEN do the following:

1. Develop a strategy to implement FinCEN's goal of performing more complex analysis.

Management Response The Director of FinCEN stated that in fiscal years 2004-2005, the bureau's Analytics Division developed a strategy to enhance the quality of its analytic products. This included reducing the number of domestic routine cases, and transitioning its customers requiring simple BSA data extracts to FinCEN programs that allow direct access to BSA data. According to the Director, FinCEN has engaged its customers to identify opportunities for complex case support, and begun providing bulk data downloads of the BSA data to its primary law enforcement customers allowing them to integrate this data with their own data warehouses. The Director also said FinCEN has participated in monthly Law Enforcement Round Table meetings to identify how it can better support law enforcement and provide more insightful and higher quality analytic products. For example, FinCEN worked with the Department and other agencies in the efforts to develop a National Money Laundering Threat Assessment and identify jurisdictions and institutions as primary money laundering concerns under the USA PATRIOT Act. Internally, the Director said FinCEN has increased the skills of its analysts with participation in training sessions with organizations such as the Central Intelligence Agency's Sherman Kent School. Going forward, he indicated FinCEN will continue its collaboration with law enforcement and the intelligence communities to allow the bureau to continue to provide more insightful and higher quality analytic products.

---

Overall, the Director said the improvement in FinCEN's analytic products is a continuous process.

OIG Comment Although FinCEN has identified the action as completed, we believe in future years FinCEN will need to continually reassess the strategy and make adjustments as needed.

2. Develop a mechanism to periodically assess FinCEN's progress in achieving its strategic goals and objectives, and make corrections if goals and objectives are not met.

Management Response The Director of FinCEN stated that the bureau began tracking its strategic goals through a Quarterly Performance Report that included targets for each performance measure and milestone. The results are reported each quarter to track progress. FinCEN has two performance measures for its analytic products. The first is the percentage of complex analytic work completed by FinCEN analysts. The percentage reported for fiscal year 2005 was 10 percent and the target for fiscal year 2006 is 25 percent. The second measure is the percentage of customers finding FinCEN's analytic support valuable. FinCEN reported 73 percent in fiscal year 2005, and has a target of 75 percent in fiscal year 2006. The Director said FinCEN will re-evaluate the workload and the assessment method to identify additional steps required to improve the quality and value of its analytic products.

OIG Comment In assessing the value of its complex analytic work, we believe FinCEN will need to find ways to improve the rate of customer response and the quality of information received.

## Finding 2

### **The FinCEN Database Cannot Be Relied On for Accurate and Complete Data**

Section 361 of the USA PATRIOT Act requires FinCEN to analyze and disseminate available data to identify possible criminal activity to appropriate federal, state, local, and foreign law enforcement agencies, and determine emerging trends and methods in money laundering and other financial crimes. FinCEN is to document the results of this analytical effort in its case management system known as the FinCEN Database. The act also requires FinCEN to

---

establish and maintain operating procedures with respect to the use of its databases. FinCEN established standard operating procedures to instruct analysts on the system's data requirements and their role in entering data into the system.

We reviewed the data maintained in the system and found that FinCEN does not have reliable management information that can accurately and consistently represent the status, completeness, and timeliness of its research, analytical, and informational services. We found that the FinCEN Database produced different case number totals for the same date, contained data that did not agree with case file documentation, and lacked information on resources used to develop the cases or track timeliness. Data errors resulted from system weaknesses that made it difficult to develop accurate summary data and from recording errors made by analysts. Recording errors occurred when analysts did not record data consistently or in accordance with standard operating procedures. In addition, FinCEN did not have adequate controls to prevent unauthorized deletion of cases.

Without reliable management information, FinCEN is unable to determine whether it is efficiently and effectively using its analytical resources. FinCEN is also unable to attest to the reliability of information included in its annual report or the Department of the Treasury PAR.

### **Case Data to be Entered in the FinCEN Database**

FinCEN uses the FinCEN Database to manage its analytical cases. The database includes specific case information, which is entered by analysts. In the FinCEN Database standard operating procedures, FinCEN instructs analysts to enter: (1) the number of hours worked on a case, (2) the number and transaction amounts of related BSA reports, (3) the number of subjects, (4) new subjects, (5) networking status, (6) information including what the requester is asking for and any significant findings, and (7) conversations with the requester or progress on the case.

### **Requests for Case Status Produced Different Results**

Despite the existence of standard operating procedures, we found several problems with the case data housed in the FinCEN



---

Database. These problems limited use of the system for analytical purposes.

First, for a single query, the system can generate different results for each day the query is run. For example, the system produced conflicting information regarding the total number of cases processed. Tables 1 and 2 below illustrate that FinCEN was unable to provide us with compatible numbers for cases closed in fiscal years 2003 and 2004. The data that were initially provided to us on November 18, 2004, differed from the data subsequently provided on December 2, 2004, for these same fiscal years. We asked for this data in December because we could not reconcile the fiscal year 2003 data provided by FinCEN in November. We found the same problems with the data provided to us in December. For example, the FY 2003 data that FinCEN provided in December included a figure of 4,403 total cases, though the subtotals by type of case totaled 4,228. In addition, in January 2005, FinCEN provided a total for fiscal year 2004 reactive cases of 114, though the totals provided in November and December 2004 were 797 and 811, respectively.

**Table 1: Differences in Fiscal Year 2003 FinCEN Case Total Data**

<b>Type of Case</b>	<b>12-02-04</b>	<b>11-18-04</b>	<b>Difference</b>
Contractor	2,033	2,035	-2
Reactive	868	856	12
HIFCA	541	541	0
Support	537	528	9
Proactive	249	247	2
<b>Total FinCEN Cases</b>	<b>4,228</b>	<b>4,207</b>	<b>21</b>

Note a

Source: OIG presentation of FinCEN data.

Note a: FinCEN actually provided us with data that showed a total of 4,403 cases as of December 2, 2004. However, we found that the supporting numbers totaled only 4,228. The difference represented a mathematical error.

---

**Table 2: Differences in Fiscal Year 2004 Case Total Data**

Type of Case	12-02-04	11-18-04	Difference
Contractor	1,305	1,298	7
Reactive	811	797	14
HIFCA	200	200	0
Support	252	245	7
Proactive	266	260	6
<b>Total FinCEN Cases</b>	<b>2,834</b>	<b>2,800</b>	<b>34</b>

Source: OIG presentation of FinCEN data.

A FinCEN official explained that differences exist in the numbers from one month to another because reports generated from the FinCEN Database are accurate only for a particular point in time. The dynamic nature of the system allows cases to be reopened after being closed, which changes the totals. The system cannot generate reports that are consistent and comparable from one period to another.

Second, we found that we could not reconcile closed cases. For example, FinCEN provided a file showing that of 6,270 cases FinCEN worked on in fiscal year 2004, 5,735 cases were closed "normally."<sup>17</sup> FinCEN refers to these as "C" cases. However, out of the 5,735 cases, 215 cases did not show an end date in the system. In addition, we found 90 other cases recorded as "C" cases that did not have a start date. FinCEN explained that analysts enter data from the start of a case to its completion, but the FinCEN Database was defaulting to the "C" code for these cases even though they were still open. These cases would remain as "C" cases in the system unless FinCEN analysts corrected the status manually.

Third, FinCEN relabeled cases during fiscal years 2003-5, making it difficult to review data for trends. Excluding Platform cases, fiscal year 2003 had six types of cases, 2004 had 19, and the first quarter of 2005 showed 12. For example, the Analytical ("ANL")

---

<sup>17</sup> The FinCEN Database has three codes for closed cases: "A" is for cases that are administratively closed; "C" is for cases that are closed out following the normal process; and "N" is for cases worked with negative results.

---

cases were found only in 2003. Support (“SUPP”) cases were found in fiscal years 2003 and 2004, but not in the first quarter of 2005. While we understand that some of the case types were changed to better represent the organizational needs existing at the time, FinCEN did not have a method to consistently compare data from year to year.

### **Case File Documentation Did Not Always Match Data in the FinCEN Database**

When compared with case file documentation, we determined that the FinCEN Database contained incorrect labeling, missing information, and cases denoted as closed but actually unassigned. In fiscal year 2004 through the first quarter of 2005 cases, we found 13 cases out of a sample of 66 we selected in which the information recorded in the FinCEN Database did not match the information in the case files or was misrepresented in the system.

To illustrate, in one case, the Case Assignment section of the *General Query Case Report* designated a case as a contractor case, whereas the case file listed the case as one being performed by FinCEN analysts. In another case, the “end date” field was found to be blank, indicating the case was still open. However, the backup documentation in the case file included an e-mail that explained that this case was closed in the FinCEN Database on February 10, 2005. Moreover, case file documentation showed it actually should have been closed on July 6, 2004.

Other examples include the following:

- Two cases showed a “C” in the “closed” field when they were both actually unassigned.
- A classified case was erroneously tagged as “N” or normal under the “sensitivity” field.
- A case was designated as proactive but was reactive.
- A case failed to include start and end dates and showed as not being networked when file documentation showed that it had.

Data can be also be misrepresented, and case searches affected, because FinCEN only allows cases to be labeled with and retrieved

---

by one type of violation, even though they may involve more than one type. For example, if a case involves both money laundering and narcotics and is labeled as a money laundering case, it will not show up under a search for narcotics cases.

Another obstacle to obtaining accurate and reliable information from the FinCEN Database is that some case information is in hardcopy files and other information is stored electronically, which makes it difficult and time-consuming for FinCEN to retrieve case records. Because records for individual cases are not located in a single, centralized file, it is also cumbersome for FinCEN to re-create case files, which increases the risk of omitting case documentation from a file.

### **System Controls Are Inadequate to Prevent Unauthorized Deletion of Cases**

FinCEN is responsible for ensuring that BSA and other data are adequately protected in the FinCEN Database. The Office of Management and Budget states that internal controls should be designed to provide reasonable assurance regarding prevention or prompt detection of unauthorized acquisition, use, or disposition of assets.<sup>18</sup> Moreover, the Government Accountability Office, in providing guidance regarding system software controls, states that access to resources and records should be limited to authorized individuals, accountability for their custody and use should be assigned and maintained, and periodic comparison of resources with the recorded accountability should be made to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.<sup>19</sup>

In reviewing the FinCEN Database, we found unexplained missing and deleted case numbers that raised questions about whether anyone was inappropriately deleting files. Deletions could have occurred because FinCEN did not have controls to prevent FinCEN personnel from making unauthorized deletions of data in the FinCEN Database. FinCEN did not have policies and procedures for analysts to follow when they wanted to delete case numbers from

---

<sup>18</sup> OMB Circular No. A-123, Management's Responsibility for Internal Control (Effective beginning with Fiscal Year 2006) (Revised 12/21/2004)

<sup>19</sup> GAO/AIMD-0021.3.1, Internal Control: Standards for Internal Control in the Federal Government, November 1999

---

the system. Further, when deletions were made, the system did not provide for an audit trail to trace who was responsible.

Questions about deleted case numbers came to light with our review of fiscal year 2004 cases entered into the FinCEN Database. We compared the first case number to the last case number for 2004 and calculated a total of 6,493 case numbers. The FinCEN file provided to us showed a 2004 total of 6,270 cases. The result was a difference of 223 cases. When we asked for a listing of the fiscal year 2004 cases deleted from the FinCEN Database, we were given a listing of 128 deleted case numbers. This left 95 unaccounted for case numbers.

A FinCEN Senior Intelligence Research Specialist provided possible explanations for the deleted cases. One explanation was that the case numbers were deleted because an analyst may have queried the system and created a case number in error. Also, if an analyst working on a case hit the "update" key instead of the "close" key, this would create a duplicate case in the Database. Another explanation is that an employee may have opened a second case number for an already established case and entered information in the wrong case. This would create two cases in the system when there should be only one, and the analyst would need to request that one of the duplicate case numbers be deleted. However, because FinCEN was unable to account for all case numbers, and analysts were not required to provide justification for requesting the deletion of a case number, the potential exists for the FinCEN Database to have been subject to unauthorized deletions. The potential also exists for analysts to have queried subjects for personal reasons and then deleted the case number without any justification.

Moreover, the system itself can also delete case numbers. FinCEN's Supervisory Information Technology Specialist explained that if two users log onto the FinCEN Database at the same time, the system may initially assign identical case numbers to both users. When that occurs, the system deletes the number from both users and assign two new case numbers. There is no lasting evidence of the original case number. Furthermore, a system error can sometimes occur in which an assigned case number is lost in transit between the system and the user. Those numbers do not appear anywhere in the system. Therefore, according to the

---

Supervisory Information Technology Specialist, some numbers in the FinCEN Database will never be used for a case. This creates a gap in the list of case numbers.

To compound our concern about deleted case numbers, we noted instances of multiple unaccounted for case numbers occurring in sequential order. For example, case numbers missing from the master file of all cases entered in fiscal year 2004 included the following: 89006, 89007, 89008, 89009, and 89010. None of the five cases numbers between 89006 and 89010 appear on the list of deleted FinCEN Database cases provided to us by FinCEN. FinCEN did not have an explanation for these missing numbers.

We reviewed FinCEN's process for deleting cases. The only users authorized to delete cases, and to make special edits to the FinCEN Database were the 16 FinCEN employees designated "Super Users." Ten of these individuals were in the Analytics Division and six were in the Client Liaison and Services Division.

We met with one such individual to discuss the deletion of case numbers. This Super User provided us with samples of e-mails requesting the deletion of case numbers from the database. The e-mails used to support the deletion of case numbers varied in content. While some e-mails gave great detail as to the reasons why a case number should be deleted, others gave no explanation. Before our meeting, this Super User had been reviewing the FinCEN Database and deleting duplicate cases without written justification so that the statistics pulled from the system would be more reflective of the workload. While the Super User's intent was reasonable, we do not believe that deleting case numbers from the FinCEN Database without valid justification was.

### **Neither Resources Devoted to Cases nor Timeliness of FinCEN Products Can be Determined**

According to FinCEN's Standard Operating Procedures, analysts are instructed to enter the number of hours spent working on a case and the dates when cases are started and completed into the FinCEN Database. However, we found that because analysts did not consistently enter the number of hours spent working on cases, FinCEN was unable to use these statistics from the FinCEN Database to measure the resources used to complete its products

---

or the timeliness of FinCEN products. A FinCEN Senior Intelligence Research Analyst explained that data on resources used to complete cases cannot be relied upon from the FinCEN Database because of incomplete and inconsistent data input.

To determine the time and resources it took to complete a case, FinCEN must review case data and make manual calculations using those data. Even if the start and completion dates were entered by the analysts, the FinCEN Database cannot calculate the number of days between the dates. The system also cannot calculate the hours worked on a case. In addition, data must be downloaded to a program, such as Microsoft Excel, for reporting purposes.

### **FinCEN Database Is Used for Performance Reporting**

FinCEN uses the FinCEN Database for external performance reporting purposes. For example, information in the FinCEN Annual Report for Fiscal Year 2004, and data used for FinCEN's performance measures cited in the Department of the Treasury's Fiscal Year 2004 PAR were derived from this system.

In its fiscal year 2004 annual report, FinCEN reported major accomplishments such as supporting more than 2900 investigative efforts through research and analysis of BSA and other data and researching more than 19,300 subjects being investigated by law enforcement. In Treasury's fiscal year 2004 PAR, FinCEN used case data to measure the number of subjects in completed investigative analytical reports (19,158 in fiscal year 2004 and 31,000 proposed for fiscal year 2005), and the number of strategic analytic products (56 in fiscal year 2004 and 90 proposed for fiscal year 2005).

FinCEN cannot verify the accuracy of the information provided in these reports. As we discussed earlier, running identical data requests through the FinCEN Database at different times can yield different outcomes.

In summary, we noted several weaknesses in the FinCEN Database that made it difficult for FinCEN to produce accurate summary information. The system would at times default to identifying a case as being closed, even if the case was open, if the analyst did not change the code manually. The database format also made it

---

difficult to summarize data and required a download of data to other programs, such as Microsoft Excel, to allow FinCEN to summarize results.

In addition, FinCEN managers did not review cases to ensure that the analysts were following their standard operating procedures. As also reported above, we found that analysts sometimes left data fields blank or that there were inconsistencies in how they filled out the fields.

### **Future System Is Expected to Improve Internal Data Management**

FinCEN awarded a contract to EDS, a global information technology services company, to design, develop, and implement a new information storage and delivery system called BSA Direct and to provide Web-hosting and support services for the new system. FinCEN believes BSA Direct, which FinCEN expects to be operational in January 2006, will enhance how data collected under the BSA are stored, accessed, and utilized. FinCEN indicated to us that the bureau will control the data and data query tools, especially text mining, once BSA Direct is up and running. FinCEN plans to upgrade its current case management system by linking it with BSA Direct.

### **Conclusion**

FinCEN's case management system, the FinCEN Database, is of limited value in its present form. The data it produces are unreliable and inaccurate. To better manage analytical cases and products, FinCEN needs a system that can provide management with useful and reliable information. FinCEN also needs to ensure that analysts accurately, completely, and consistently record data to a management information system. FinCEN will have to determine whether enhancements can be made to the current system or a new system is needed.

### **Recommendations**

We recommend that the Director of FinCEN do the following:

1. Enhance the current FinCEN Database system or acquire a new system. An improved system should provide for complete and



---

accurate information on the case type, status, and resources and time expended in performing the analysis. This system should also have the proper security controls to maintain integrity of the data.

Management Response The Director of FinCEN stated that the bureau previously concluded that enhancement to the FinCEN Database is not a viable option, and that replacement of the system is required. The system was designed in 1990 as a repository for case information and as a tool for analysts to track case work; however, it has not evolved as a case management tool along with FinCEN's work. Funding for a new system was not approved in either the fiscal year 2006 or 2007 budgets. FinCEN will again request funding to acquire a new system to track and report on all of its analytic efforts in the fiscal year 2008 departmental budget request, and will complete this in June 2006. If funding is approved, FinCEN expects to implement the new system by 2010.

OIG Comment We believe FinCEN's planned corrective action to request funding to acquire a new case system meets the intent of our recommendation. However, in light of the years it will take to develop and implement a new system, we believe FinCEN should take other interim measures that will allow the bureau to have more valid and reliable case data available to management. Additionally, FinCEN should not consider the recommendation to have a final action until a new case system is implemented.

2. Ensure that analysts follow standard operating procedures when recording case data.

Management Response According to the Director, FinCEN will update its Standard Operating Procedures that are currently in place and include a methodology for periodically extracting a sample of cases to review for compliance with these procedures. The target date for updating the Standard Operating Procedures is October 2006.

OIG Comment We believe FinCEN's planned corrective action to revise its Standard Operating Procedures and require sampling of cases to determine compliance with these procedures meets the intent of our recommendation.

---

## Finding 3

### **Improved Internal Controls Are Needed to Protect BSA and Other Data**

FinCEN is responsible for ensuring that BSA and other data are adequately protected. However, we found that certain internal controls over data security were weak. While we could not test for inappropriate use of FinCEN systems, no incidents came to our attention during the audit. Specifically, we found the following:

- In July 2005, 28 of FinCEN's required fiscal year 2005 on-site inspections had not yet been scheduled.
- FinCEN does not have a policy to address inappropriate browsing nor a methodology to monitor for this activity.
- After FinCEN increased the security level needed for contract employees, those who did not have the appropriate clearances were allowed to continue to access sensitive but unclassified BSA and law enforcement data.

#### **Gateway Inspections Not Completed in Accordance with FinCEN's Policy**

As a periodic check on usage, FinCEN employees and Law Enforcement Liaison Specialists perform on-site inspections in accordance with FinCEN's Gateway Inspection Policy and Procedure. Inspections at Gateway user sites are performed primarily to determine whether the system is being used to query BSA data in a secure environment.

According to FinCEN policy, on-site inspections are to be performed at each user site every 2 years. When FinCEN inspectors are on-site, they verify that the user has the latest version of FinCEN's Gateway Security Plan and review compliance in such areas as security controls over system passwords, physical security of the computers, and background investigation procedures for employees. FinCEN's policy also requires its inspectors to review (1) system queries for which there are no user or requestor case numbers, (2) compliance with FinCEN policy to retain case files for 6 years, and (3) compliance with FinCEN policy that requires BSA data not be shared with unauthorized users.

---

At the time of our review, we found that FinCEN has not been conducting all required on-site inspections. We reviewed data for 66 state agencies that FinCEN officials told us represent the bureau's highest inspection priority and found that the bureau was falling behind on inspections. For example, we found 28 agencies due to be inspected in fiscal year 2005 had not been scheduled as of July 2005. This included 7 agencies for which there was no record of a prior inspection being conducted, dating back to fiscal year 2002. In January 2006, following our exit conference, FinCEN provided us with data that showed the bureau had completed the majority of these inspections. Data showed that 27 agencies had been inspected following completion of our audit work. Twenty-three were completed in fiscal year 2005 and 4 in fiscal year 2006. We did not verify the source documentation for this data.

At the time of our audit, FinCEN officials said that the bureau did not have adequate resources to perform on-site inspections. FinCEN planned to form a dedicated inspection team. At the time, the inspectors were also the Gateway trainers, and outreach representatives. FinCEN planned to develop and transition the inspection team by fiscal year 2007.

### **FinCEN Does Not Have a Policy to Address Browsing**

FinCEN does not have a policy to address inappropriate browsing by its analysts of the FinCEN Database and the financial, law enforcement, and commercial databases. The Internal Revenue Service (IRS) identified browsing as a potential concern when it found that certain employees were obtaining electronic access to taxpayer data for unauthorized purposes. IRS established controls to prevent browsing, which included an information system log to monitor and detect this inappropriate activity. IRS also established a penalty process to discipline employees who engaged in browsing.

Our concern in this area is based on FinCEN's lack of a policy to address the possibility of inappropriate browsing by its analysts. The FinCEN Database contains sensitive financial and law enforcement data. We believe that these data need as much protection as taxpayer data. Although we did not identify any inappropriate use, we believe that internal users represent an

---

inherent risk and that to prevent browsing a policy would be beneficial.

Establishing a policy of protecting against analyst browsing is only a first step in the process. FinCEN also needs to establish a system, similar to what IRS established, to monitor system activity and detect any inappropriate use. We recognize that distinguishing between browsing and legitimate work activity will not always be easy. However, establishment and use of a monitoring and detection process can better provide assurance that employee queries are related to a specific analytical case or purpose. In this regard, FinCEN's monitoring and detection system will need to be able to review internal queries to ensure they either relate to proactive research or an established case.

### **Contractor Employees Who Did Not Meet the Contract's Upgraded Security Requirements Were Allowed To Access BSA and Law Enforcement Data**

Over the years, FinCEN has employed contractors to help its own analysts with data queries and retrieval. These contractors had to meet certain security clearance requirements. During 2003 and 2004, a number of contractor employees who did not meet the upgraded security requirements were allowed to access sensitive though unclassified BSA and law enforcement data.

This situation arose when FinCEN elevated security level requirements. In April 2003, FinCEN increased the security level requirement for contractor employees who access BSA and law enforcement data to a favorably adjudicated background investigation and Secret clearance. Previously, under Public Trust Designations, a lesser National Agency Check with Local Record Check clearance was acceptable.<sup>20</sup> At the time of the security upgrade, 21 of the 63 contractor personnel did not have a Secret clearance. Over the upcoming year, 11 of the employees continued working without increasing their security levels.

---

<sup>20</sup> Public Trust Designations are positions in which the individual's actions or inactions could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. Individuals are entrusted with control over information which the Government has legal or contractual obligations not to divulge.

---

In July 2004, in an effort to better protect BSA and law enforcement databases, FinCEN again increased security clearance requirements, this time to Top Secret. From July to October 2004, FinCEN's records showed that only 8 of the 63 contractor employees had been upgraded to Top Secret, though access to the data by contractor employees without upgrades was not denied. In October 2004, FinCEN released its on-board contractor workers because they failed to meet the increased security requirements.

### **Recommendations**

We recommend that the Director of FinCEN do the following:

1. Continue to monitor for the timely scheduling and completion of on-site inspections in accordance with the bureau's policy.

Management Response The Director of FinCEN stated the bureau currently maintains a database of organizations requiring on-site inspections. The last inspection date and the next inspection date are calculated in the database in accordance with FinCEN's revised policy to conduct on-site inspections every 3 years. He said a report with upcoming inspections is reviewed each month to ensure the inspections are scheduled and completed within the required time frames.

OIG Comment We believe management has taken corrective action that satisfies the intent of our recommendation.

2. Establish a policy to address inappropriate browsing of the FinCEN Database and the financial, law enforcement, and commercial databases, and establish and implement a methodology to monitor system activity.

Management Response The Director of FinCEN stated he strongly supports continuous improvement of internal controls. According to the Director, FinCEN will establish policy that prohibits browsing of all databases. FinCEN will also develop a methodology for monitoring system activity of the FinCEN Database and the financial databases containing BSA data. This is targeted for completion in September 2006. This methodology will complement the current warning displayed by all users reminding them that the system is for authorized use only. The Director said the law

---

enforcement database providers conduct their own audit investigation and call upon FinCEN to explain perceived anomalies, and to date FinCEN is unaware of questionable findings. Regarding the commercial databases, FinCEN blocks compilation of audit trails by the vendors to ensure that the sensitive, grand jury, and classified investigations supported by FinCEN are not compromised.

OIG Comment We believe FinCEN's planned corrective action to establish a policy to prohibit browsing of all databases and develop methodologies to monitor usage of its systems meets the intent of our recommendation.

3. Conduct a risk assessment of contractor employees' use of FinCEN systems from July to October 2004 to ensure employees' use involved only appropriate research or support for case work.

Management Response The Director of FinCEN stated that the bureau will conduct a risk assessment of contractor employees' use of the FinCEN Database from July to October 2004 with a target completion date of July 2006. He said that the FinCEN Database is the only FinCEN owned system that contractors used during the timeframe in question. According to the Director, the Database application does not contain classified information and the contractors had at a minimum received a public trust certification that included a national agency check for name and fingerprint records.

OIG Comment We believe FinCEN's planned corrective action to conduct a risk assessment of contract employees' use of the FinCEN Database meets the intent of our recommendation.

---

\* \* \* \* \*

We would like to extend our appreciation to FinCEN for its cooperation and courtesies extended to our audit staff during the audit. If you have any questions, please contact me at (617) 223-8640. Major contributors are listed in appendix 5.

/s/  
Donald P. Benson  
Director

The USA PATRIOT Act of 2001 elevated FinCEN to bureau status and required FinCEN to furnish research, analytical, and informational services to financial institutions and appropriate law enforcement authorities to fight terrorism, organized crime, and money laundering. We conducted our audit to determine if FinCEN complied with these USA PATRIOT Act provisions, focusing on FinCEN's efforts to provide analytical services to law enforcement. More specifically, we evaluated FinCEN's efforts to perform complex (i.e., proactive) analyses of BSA data that would provide law enforcement with new information regarding individuals, entities, and organizations engaging in terrorist acts or money laundering. In so doing, we identified issues with FinCEN's case management information system, known as the FinCEN Database, that we believe need to be addressed.

In this audit we also reviewed FinCEN's internal controls to secure data and prevent unauthorized disclosures of BSA data and other financial crimes information. During our review we identified data security concerns regarding the FinCEN Database and Gateway system.

We reviewed (1) applicable laws and regulations related to FinCEN's duties and responsibilities identified in the USA PATRIOT Act of 2001, Pub. L. No. 107-56, Section 361; (2) FinCEN's strategic plan and its annual report and PAR; (3) Congressional testimony; (4) FinCEN standard operating procedures; and (5) FinCEN's studies related to its case processing and data analysis functions.

We identified FinCEN's divisions, staff, and systems currently involved in analyzing data and sharing BSA data and other financial crime information. We conducted interviews with FinCEN officials at its Headquarters in Vienna, Va., and with the Regulatory Policy and Program Division in Washington, D.C. Fieldwork was performed in Vienna, Va., and Washington, D.C.

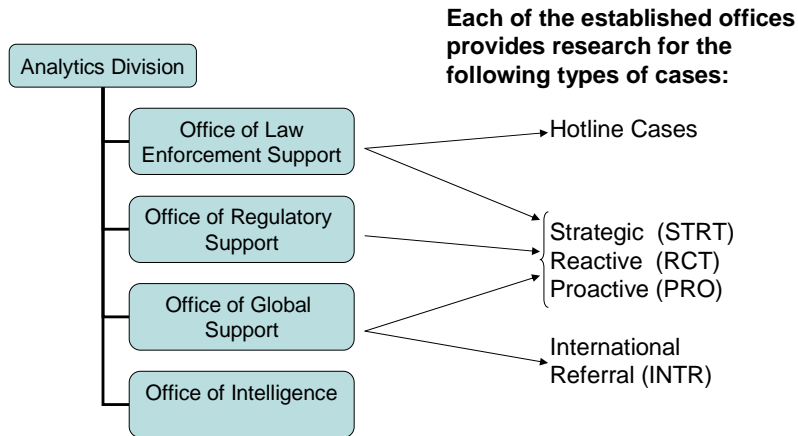
We selected a random sample of FinCEN Database cases from an electronic data file for fiscal years 2003, 2004, and the first quarter of 2005, and reviewed corresponding documentation to



assess the status, completeness, and timeliness of FinCEN's research, analytical, and informational services. We examined the analytical nature of FinCEN's products and the methods, tools, and techniques FinCEN used to identify trends and patterns in BSA data and other financial crime information reported to law enforcement agencies. The sample cases were representative of each type of case found in the FinCEN Database.

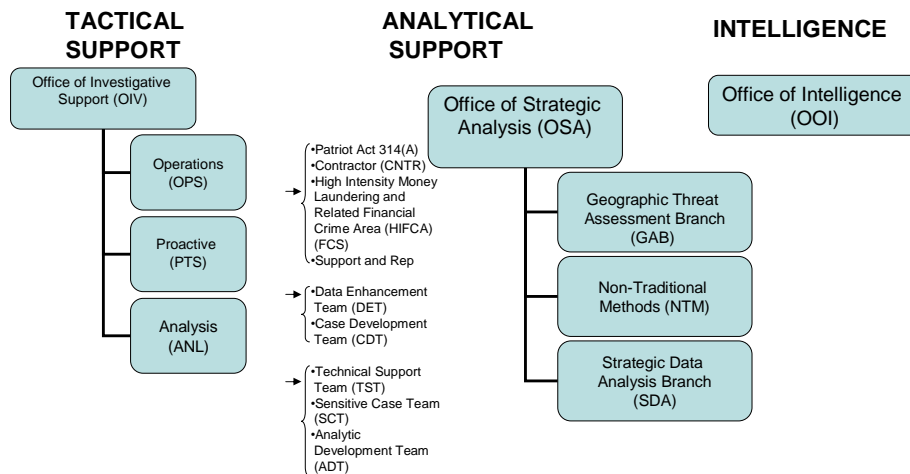
We conducted our audit from September 2004 to November 2005 in accordance with generally accepted government auditing standards.

## Current Organization of FinCEN Analytics Division



The Analytics Division is organized by the customers it supports.

## Organization of FinCEN Analytics Division Before July 2004



These offices were organized by the types of products produced.

Source: OIG Presentation of FinCEN data.

## **FinCEN Analytics Division**

### Office of Law Enforcement Support

The Office of Law Enforcement Support provides direct case support to law enforcement agencies. It provides case reports each year involving thousands of individual subjects to federal, state, local, and international agencies. Through the use of analytical tools and information extracted from numerous data sources, intelligence research analysts seek to add additional information to what is already known by investigators.

### Office of Regulatory Support

The Office of Regulatory Support (with analysts from the former Office of Investigative Support and Office of Strategic Analysis), work on identifying trends and patterns that emerge as a result of SARs. Its major project is the SAR Activity Review--Trends, Tips & Issues, a report published under the auspices of the Bank Secrecy Advisory Group. It is the product of collaboration among the financial institutions, law enforcement officials, and regulatory agencies to provide information about the preparation, use, and value of SARs filed by financial institutions. Topics presented include analyses of emerging and traditional money laundering schemes and possible terrorist financing methods.

### Office of Global Support

The Office of Global Support acts as the intermediary between law enforcement agencies, including ICE, the FBI, the Drug Enforcement Administration, and the Egmont group which is an international network of Financial Intelligence Units (FIU) around the world.<sup>21</sup> This office processes requests for information from FIUs, congressional officials, and law enforcement.

---

<sup>21</sup> An FIU is a national center established in a country to collect data from the financial industry on suspicious or unusual financial activity, analyze the data, and make those data available to appropriate national authorities and other FIUs for use in combating money laundering, terrorist financing, and other financial crime. FinCEN is the FIU for the United States.

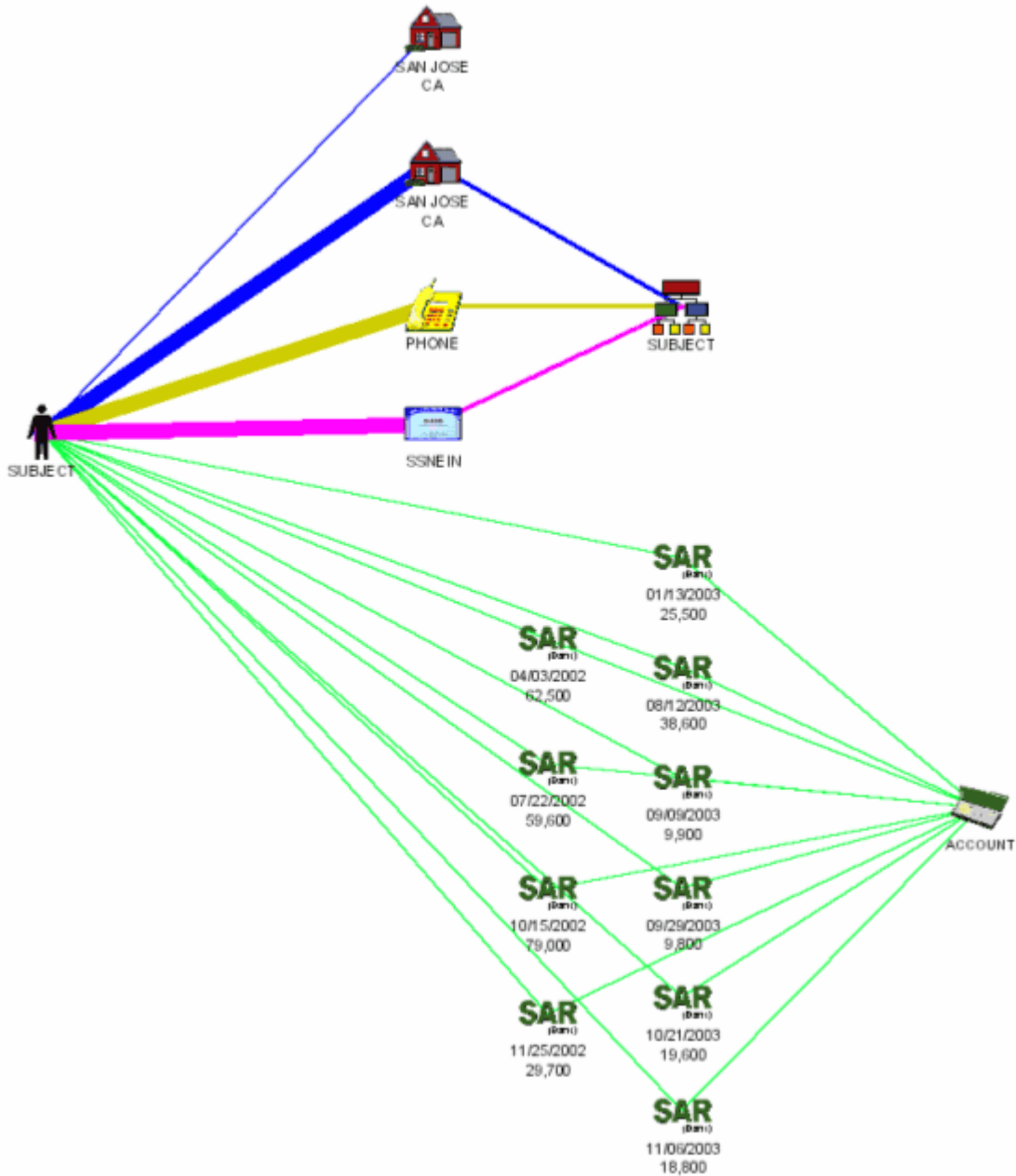
### SQS

The Suspicious Activity Report Query System (SQS) is a search engine that was developed by FinCEN analysts and technicians. It allows analysts to extract data in SARs, and perform searches for specific information contained in the SARS to identify potential money laundering or terrorist financing schemes. FinCEN downloads SARs into SQS on a daily basis from IRS-DCC.

### VisuaLinks

VisuaLinks is a commercial analytical tool developed by Visual Analytics, Inc. FinCEN analysts use this software to discover patterns, trends, and associations between persons and entities named in BSA reports filed with IRS-DCC. For instance, it allows users to identify the number of SARs with missing narratives. It also allows the user to filter the data by adding a condition which will generate useful information for potential investigation. In addition, it has a name matcher capability that searches for name spelling variations. The results of user queries are represented graphically using symbols to display links among the data. Figure 1 below illustrates a VisuaLinks diagram.

Figure 1. Example of a VisualLinks Diagram



Source: VisualLinks News, December 2004

### ASIS, MapInfo, and Analyst's Notebook

Analytical System for Investigative Support (ASIS) is a Microsoft Access database developed by FinCEN to collect money laundering and other financial crime data from financial, law enforcement, and commercial databases. It is used to assist federal agencies in their investigations by establishing one source for analyzing cases and performing searches.

MapInfo, developed by MapInfo Corp., is a mapping application that enables visualization of relationships between money laundering, other financial crime activities under investigation, and geographic locations. This information is used to assist law enforcement in their ongoing investigations.

Analyst's Notebook, developed by i2 Ltd., is an analytical tool used by FinCEN analysts to perform timeline, transaction, and link analyses with information obtained from financial, law enforcement, and commercial databases. Timeline analysis graphically represents events in chronological order. Transaction analysis links data, such as bank transfers and telephone calls, in chronological order. The link analysis feature is able to diagram connections between people, accounts, organizations and any other elements in an investigation.

Appendix 4  
Management Response



DEPARTMENT OF THE TREASURY  
FINANCIAL CRIMES ENFORCEMENT NETWORK

April 25, 2006

**MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FREEDMAN**

**FROM:** Robert W. Werner *Robert W. Werner*  
*4/25/2006*

**SUBJECT:** *Management Response to the Draft Audit Report – FinCEN Has Taken Steps to Better Analyze Bank Secrecy Act (BSA) Data But Challenges Remain*

We appreciate your efforts in reviewing the analysis of BSA data that we provide to our law enforcement customers. Providing law enforcement organizations with data and analysis to combat terrorist financing, money laundering, and other financial crimes is a key goal in fulfilling our mission to safeguard the nation's financial system.

This goal is twofold – it requires us to provide data and analysis. We have made significant progress over the past two years to improve our performance in both of these areas. In terms of data, we are transitioning customers requiring simple BSA data extracts to FinCEN programs that allow direct access to BSA data. Accordingly, we initiated a new on-line training program that speeds up the timeframe in which customers can begin searching the BSA data after signing the memorandum of understanding. In addition, we have begun providing bulk data downloads of the BSA data to our primary law enforcement customers, which allows them to integrate the BSA data with their own information data warehouses.

To support the analysis component of our strategic goal, we have implemented efforts to enhance the complexity and quality of our analytic products. First, we have increased the skills of our analysts through several training sessions with organizations such as the Central Intelligence Agency's Sherman Kent School, and the Federal Law Enforcement Training Center. Second, we have reached out to the law enforcement community through participation in monthly Law Enforcement Round Table meetings and other avenues to identify how we can better support law enforcement's large complex cases. The outcome of these efforts has resulted in more in-depth analysis of the data and increased collaboration with our law enforcement customers. For example, we worked with the Department and other agencies to identify jurisdictions and institutions as primary money laundering concerns under Section 311 of the USA PATRIOT Act, and supported the Department's efforts to develop a National Money Laundering Threat Assessment. Going forward, we plan to further leverage our unique knowledge and expertise in a manner that allows us to provide more insightful and higher quality analytic products that the law enforcement and intelligence community can not otherwise obtain.

[www.fincen.gov](http://www.fincen.gov)



Appendix 4  
Management Response

**MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FREEDMAN**

April 25, 2006

Page 2

Another future effort will be to replace the FinCEN database, our legacy case tracking system. The system was designed in 1990 as a central repository for case information and a tool for analysts to track the status of their casework. However, this case management tool has not evolved along with our case work. Hence, we agree with your recommendation to replace the FinCEN database. Although past funding requests have been denied in light of other priorities, we will request future funding to procure a new system that both tracks and reports on all of our analytic efforts.

Lastly, continuous improvement of internal controls is an area I strongly support. Establishing a methodology to monitor use of the FinCEN database will complement the current warning displayed to all users reminding them that the system is for authorized use only.

The recommendations identified by your audit team will help us to ensure any adjustments we make to our overall strategy continue to support our goal to provide law enforcement organizations with data and analysis to combat terrorist financing, money laundering, and other financial crimes. If you have any questions or concerns with our attached response to the individual recommendations in the draft report, please feel free to contact me on 703-905-3592.

Attachment

Appendix 4  
Management Response

Attachment 1 - FinCEN Response to OIG Draft Report on BSA Data Analysis

**1. Develop a strategy to implement FinCEN's goal of performing more complex analysis.**

Response: Concur. FinCEN's Analytics Division developed a strategy in FY 2004-2005 to enhance the quality of our analytic products that included: reducing the number of domestic routine cases, engaging FinCEN's customers to identify opportunities for complex case support, and increasing the skills of FinCEN analysts. Going forward, we will continue to reduce the number of domestic routine cases by transitioning more customers to direct access programs. Additionally, we will continue to collaborate with the law enforcement and intelligence communities to further leverage our unique knowledge and expertise in a manner that allows us to provide more insightful and higher-quality analytic products. Overall, the improvement of our analytic products is a continuous process.

Status: Completed.

**2. Develop a mechanism to periodically assess FinCEN's progress in achieving its strategic goals and objectives, and make corrections if goals and objectives are not met.**

Response: Concur. In FY 2005, FinCEN began tracking strategic goals through a Quarterly Performance Report. For each strategic goal, the report includes performance measures and milestones. Targets are established for each performance measure and milestone, and results are reported each quarter to track progress in meeting those targets. We have two performance measures for our analytic products: the percent of complex analytic work completed by FinCEN analysts; and the percent of customers finding FinCEN's analytic support valuable. For complex analytic work, the percent reported in FY 2005 was 10%, and the target for FY 2006 is 25%. For the value of analytic products, the percent reported in FY 2005 was 73%, and the target for FY 2006 is 75%. As needed, FinCEN will re-evaluate the workload and the assessment method to identify additional steps required to improve the quality and value of our analytic products.

Status: Completed.

**3. Enhance the current FinCEN database system or acquire a new system. An improved system should provide for complete and accurate information on the case type, status, and resources and time expended in performing the analysis. This system should also have the proper security controls to maintain the integrity of the data.**

Response: Concur. FinCEN previously concluded that enhancement of the FinCEN database is not a viable option; replacement is required. Although funding was not approved in the FY 2006 or FY 2007 budgets, FinCEN will again request funding to acquire a new system to replace the FinCEN database in the FY 2008 departmental budget request. If funding is approved, we expect to implement a system by 2010.

Status: Target completion June 2006.

Appendix 4  
Management Response

Attachment 1 - FinCEN Response to OIG Draft Report on BSA Data Analysis

**4. Ensure the analysts follow standard operating procedures when recording case data.**

Response: Concur. FinCEN will update the SOPs currently in place. A sample of cases will be extracted periodically and the case data will be reviewed to determine compliance with the SOPs; this methodology will be incorporated into the SOP.

Status: Target completion October 2006.

**5. Continue to monitor for the timely scheduling and completion of on-site inspections in accordance with the bureau's policy.**

Response: Concur. FinCEN currently maintains a database with a list of organizations requiring on-site inspections. The database contains the last inspection date and the next inspection date, which is calculated in accordance with the revised policy that requires on-site inspections to be conducted once every three years (off-site inspections are conducted quarterly). A report listing upcoming inspections is reviewed each month to ensure on-site inspections are scheduled and completed in accordance with the bureau's policy.

Status: Completed.

**6. Establish a policy to address inappropriate browsing of the FinCEN database and the financial, law enforcement, and commercial databases, and establish and implement a methodology to monitor system activity.**

Response: Concur with comment. FinCEN will establish a policy that prohibits inappropriate browsing of all databases. We will develop a methodology to monitor system activity for the FinCEN database and the financial databases containing BSA information; target completion is September 2006. The law enforcement database providers already conduct their own audit investigation and call upon FinCEN to explain any perceived anomalies; to date we are not aware of any questionable finding. Finally, given that the information contained in the commercial databases is open source information, FinCEN blocks any compilation of audit trails by the vendors to ensure that the sensitive, grand-jury and classified investigations supported by FinCEN are not compromised.

Status: Target completion September 2006.

Appendix 4  
Management Response

Attachment 1 - FinCEN Response to OIG Draft Report on BSA Data Analysis

- 7. Conduct a risk assessment of contractor employees' use of FinCEN systems from July to October 2004 to ensure employees' use involved only appropriate research or support for case work.**

Response: Concur. The FinCEN database is the only FinCEN-owned system that contractor's used during the timeframe in question. Therefore, we will conduct a risk assessment of contract employees' use of the FinCEN database during that timeframe (July to October 2004). However, it is important to note that the FinCEN Database application does not contain classified information and that the contractor employees had at a minimum received public trust certification, which includes a national agency check (NAC). A NAC includes a check of name and fingerprint records.

Status: Target completion July 2006.

Appendix 5  
Major Contributors to This Report

---

Sharon Torosian, Audit Manager  
Maryann Costello, Auditor-In-Charge  
Audrey Philbrick, Auditor  
Valerie Freeman, Referencer

**Department of the Treasury**

Under Secretary, Office of Terrorism and Financial Intelligence  
Assistant Secretary, Terrorist Financing  
Assistant Secretary, Intelligence and Analysis  
Office of Strategic Planning and Performance Management  
Office of Accounting and Internal Controls

**Financial Crimes Enforcement Network**

Director  
Assistant Director, Financial Management

**Office of Management and Budget**

OIG Budget Examiner