Message to Stakeholders

During the past year, the Financial Crimes Enforcement Network marked its 15th birthday. In those 15 years, we have been charged with growing responsibility for protecting the nation's financial system from the threats of terrorism and financial crime. Our accomplishments during the past year convince me that we are increasingly realizing our tremendous potential for contributing to the financial and national security of our country and of financial systems around the globe.

In our role as Administrator of the Bank Secrecy Act, we took decisive steps toward ensuring more effective and uniform application of this important statute. We developed information-sharing agreements with Federal and state banking agencies that give us more comprehensive data than ever before on Bank Secrecy Act compliance. We also cooperated with regulatory agencies in ways that were not even conceived of a few years ago to promote more uniform examination procedures for compliance with the Bank Secrecy Act, faster and more consistent compliance activities, and joint action in cases of egregious violations of the law.

To improve the management of data filed under the Bank Secrecy Act, we developed BSA Direct—a major initiative that will eventually collect, process, store, and disseminate all Bank Secrecy Act data. As the fiscal year ended, we were close to completing the initial phase of the system, which will provide authorized law enforcement and regulatory agencies with easier access to the Bank Secrecy Act data and enhanced ability to query and analyze that data.

We also saw that our strategy of increasing the number of authorized law enforcement agencies with controlled access to the Bank Secrecy Act data is paying off in greater and more creative use of the data. Increasing customer access to the data has allowed us to begin moving away from serving as a "library" for Bank Secrecy Act data and to focus more of our analytical resources on producing complex, actionable intelligence related to financial crimes. In addition, we produced an outstanding manual on funds transfers that demonstrates our expertise in the complex mechanisms that can be misused in financial crime.

We also strengthened partnerships with key allies in the fight against money laundering, terrorist financing and other financial crimes. Internationally, we hosted the 13th Plenary of the Egmont Group of financial intelligence units and continued to support and provide leadership for this group. At home, we stepped up cooperative efforts with our sister agencies within the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence. Through

our joint efforts, the Treasury Department was able to identify several foreign banks of special money laundering concern and to impose special measures against these institutions.

We are proud of these accomplishments. We are equally proud of the swift and well-reasoned actions that we took to meet the unexpected challenges of Fiscal Year 2005. For example:

- Realizing that some banks were suspending or refusing to provide services to money services businesses such as check cashers and money transmitters because of fears of violating Bank Secrecy Act regulations, we worked with the banking regulators to provide uniform guidance for taking a risk-based approach to providing bank services for this important sector.
- Faced with a dramatic increase in the number of Suspicious Activity Reports filed under the Bank Secrecy Act, we analyzed patterns of filings to determine whether unnecessary reports were being filed to avoid possible penalties. We found some indications of unnecessary filings and have been working closely with the financial industry and banking regulators to guard against such filing through education and by ensuring the consistent application of Suspicious Activity Report regulations.
- Following discovery of a vulnerability on our QuikNews e-mail list server, we immediately assessed the damage, reported the incident to appropriate Federal law enforcement authorities, notified those whose information was compromised, and took steps to prevent a reoccurrence.
- In the aftermath of Hurricane Katrina, we issued a joint statement with the bank regulators encouraging depository institutions to be "reasonable" in their approach to verifying the identity of individuals temporarily displaced by the storm and unable to provide standard identification documents.

I feel very privileged to have recently completed my second year at the helm of an organization that is having a profound impact on financial systems and practices around the world. I am also very proud of, and grateful to, the dedicated men and women of the Financial Crimes Enforcement Network who have so diligently served the nation and the world during the past year.

Message to Stakeholders

We recognize that there is much more to do in our quest to safeguard the financial system from the abuses of financial crime. In February 2005, we launched a new strategic plan that sets our course for the near future.

We need to continue to strengthen the Bank Secrecy Act regulatory regime, deploy and expand BSA Direct, step up the production of policy-level analysis of financial crimes patterns and threats, and better leverage our knowledge of global financial activity to promote greater international collaboration against financial crime. We must also continue to build the internal infrastructure, employee and management skills, and processes required of a world-class financial intelligence unit. We look forward to continuing to work with our law enforcement, regulatory, and government partners as we pursue these priorities in the coming year.

William J. Fox, Director
Financial Crimes Enforcement Network
January 2006

Table of Contents

About the Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network, a bureau within the U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, is America's financial intelligence unit. Financial intelligence units are national centers set up to collect information on suspicious or unusual financial activity from the financial industry, to analyze that data, and to make the data available to appropriate authorities for use in combating financial crime.

- Our mission is to safeguard the financial system from the abuses of terrorist financing, money laundering and other financial crime. We fulfill this mission through our role as administrator of the Bank Secrecy Act, as amended. Among a broad range of interrelated activities, we:
- Issue, interpret, and enforce compliance with regulations implementing the Bank Secrecy Act, which includes key provisions of Title III of the USA PATRIOT Act;
- Support and oversee compliance examination functions delegated to other federal regulators;
- Manage the collection, processing, storage, and dissemination of Bank Secrecy Act data;
- Maintain a government-wide access service to the Bank Secrecy Act data, and network users with overlapping interests; and
- Conduct analysis in support of policy makers; law enforcement, regulatory, and intelligence agencies; and the financial industry.

Because illicit financial activity is not confined to our borders, we also work to build global cooperation, strengthen other countries' efforts to deter and detect financial crime, and promote international information sharing about financial crime. To meet these aims, we coordinate with and collaborate on anti-terrorism and anti-money laundering initiatives with our financial intelligence unit counterparts around the world.

To learn more about the Financial Crimes Enforcement Network, visit our website at www.fincen.gov.

History

The Department of the Treasury established the Financial Crimes Enforcement Network in 1990. Our initial charge was to establish a government-wide multi-source financial intelligence and analysis network. Our operations were expanded in 1994 to include regulatory responsibilities for administering the Bank Secrecy Act, one of the nation's most potent weapons for preventing abuse of the U.S. financial system by financial criminals and terrorist financiers.

The Bank Secrecy Act, enacted in 1970, authorizes the Secretary of the Treasury to issue regulations requiring that financial institutions keep records and file reports on certain financial transactions determined to have a high degree of usefulness in criminal, tax, regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters. The authority of the Secretary to administer Title II of the Bank Secrecy Act (codified at 31 U.S.C. 5311-5330 with implementing regulations at 31 C.F.R. Part 103) has been delegated to the Director of the Financial Crimes Enforcement Network.

Hundreds of thousands of financial institutions are subject to Bank Secrecy Act anti-money laundering program, record keeping and reporting requirements. These include, but are not limited to: depository institutions (*e.g.*, banks, credit unions, and thrifts); brokers or dealers in securities; money services businesses (*e.g.*, money transmitters; issuers, redeemers, and sellers of money orders, travelers' checks, and stored value; currency dealers and exchangers; and check cashers); and casinos and card clubs. In Fiscal Year 2005, dealers in precious metals, stones, or jewels also became subject to Bank Secrecy Act requirements.

The USA PATRIOT Act of 2001 broadened the scope of the Bank Secrecy Act to focus on terrorist financing as well as money laundering. The Act also gave the Financial Crimes Enforcement Network additional responsibilities and authorities in both important areas, and established the organization as a bureau within the Department of the Treasury.

In 2004, the Financial Crimes Enforcement Network became part of the Treasury Department's new Office of Terrorism and Financial Intelligence. This is the lead office within the Department for fighting the financial war on terror, combating financial crime, and enforcing economic sanctions against rogue nations.

The Bank Secrecy Act is the nation's first and most comprehensive federal anti-money laundering statute. Since it was enacted in 1970, the Act has been amended several times, most recently by the USA PATRIOT Act. The Bank Secrecy Act authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including filing reports that have been determined to have a high degree of usefulness in criminal, tax, regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters.

The Bank Secrecy Act's anti-money laundering program requirement helps financial institutions to protect themselves, and thus the U.S. financial system, from abuse by financial criminals, and helps those institutions identify and mitigate the risks inherent in their operations. The Bank Secrecy Act's record keeping and reporting requirements provide transparency in the financial system and help to create a financial trail that law enforcement and intelligence agencies can use to track criminals, their activities, and their assets. For an overview of the relationship between Bank Secrecy Act records and money laundering, terrorist financing, and other financial crimes, see Appendix A.

Twelve types of reports are required under the Bank Secrecy Act. The reports that are filed most often are:

- Currency Transaction Reports, which are filed in connection with deposits, withdrawals, exchanges of currency, or other payments or transfers by, through, or to a financial institution exceeding $10,000. Currency transaction reporting requirements are a key impediment to criminal attempts to legitimize the proceeds of crime.
- Suspicious Activity Reports, which describe financial transactions of any amount and type that financial institutions suspect may be related to illicit activity. These reports are especially valuable to law enforcement and intelligence agencies because they reflect activity considered problematic or unusual by financial institutions, casinos, money services businesses, and the securities industry. Suspicious Activity Reports contain sensitive information and, consequently, may be disclosed and disseminated only under strict guidelines. Unauthorized disclosure of Suspicious Activity Reports is a violation of criminal law.

Bank Secrecy Act Reports

- Currency Transaction Report (CTR)
- Currency Transaction Report by a Casino (CTR-C)
- Currency Transaction Report by a Nevada Casino
- Designation of Exempt Person
- Report of Foreign Bank and Financial Accounts (FBAR)
- Report of International Transportation of Currency or Monetary Instruments (CMIR - Collected by U.S. Customs and Border Protection)
- Report of Cash Payments over $10,000 Received in a Trade or Business (8300)
- Suspicious Activity Report (SAR)
- Suspicious Activity Report by a Money Services Business (SAR-MSB)
- Suspicious Activity Report by Casinos & Card Clubs (SAR-C)
- Suspicious Activity Report by Securities & Futures Industries (SAR-SF)
- Registration of Money Services Business (RMSB)

The latest versions of these forms are available at www.fincen.gov.

The number of Bank Secrecy Act reports filed in Fiscal Year 2005 was more than 5 percent higher than the number filed the previous year, rising from nearly 15 million in Fiscal Year 2004 to approximately 15.8 million in Fiscal Year 2005. Increases in the number of Suspicious Activity Reports and Currency Transaction Reports accounted for most of the rise during this period.

- The number of Suspicious Activity Reports jumped by about 32 percent, from 663,655 to 878,021.
- The total number of Currency Transaction Reports grew by nearly 6 percent, from 13.7 million to 14.2 million.

The only type of filing that declined was registration of money services businesses. Money services businesses registrations are effective for two years before re-registration is required.

The Financial Crimes Enforcement Network encourages electronic filing of Bank Secrecy Act reports to accelerate the secure flow of information from financial institution filers to law enforcement and regulatory agencies. In Fiscal Year 2005, about 24 percent of Bank Secrecy Act reports were e-filed, more than twice the 11 percent e-filed in Fiscal Year 2004. In the last two months of the fiscal year, about 29 percent of all reports were electronically filed.

Testimony on Value of Bank Secrecy Act Data

"Financial information, lawfully acquired, significantly enhances the ability of U.S. law enforcement and intelligence community members to overcome defects in financial transparency…. BSA data is of incalculable value in this important effort. When combined with other data collected by the law enforcement and the intelligence community, investigators are better able to 'connect the dots.'

"More recently, BSA data has proven its utility relative to counterterrorism matters. For example, BSA data is used to obtain additional information about subject(s) under investigation and their methods of operation. Analysis of BSA data permits counterterrorism investigators to acquire biographical and descriptive information, to identify previously unknown subject associates and/or co-conspirators, and, in certain instances, to determine the location of subject(s) by time and place.

"The value of BSA data to counterterrorism efforts is reflected in the results of a recent review of BSA data. In this instance, the FBI, using information technology, reviewed approximately 71 million BSA documents for their relevance to counterterrorism investigative and intelligence matters. The review identified over 88,000 Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) that bore some relationship to subjects of terrorism investigations."

—Michael F.A. Morehart, Section Chief, Terrorist Financing Operations Section, Counterterrorism Division, Federal Bureau of Investigation, before the U.S. House of Representatives Committee on Financial Services, May 26, 2005

The following chart lists the different types of Bank Secrecy Act reports and the numbers filed in Fiscal Years 2004 and 2005.

Bank Secrecy Act Filings by Type, Fiscal Years 2004 and 2005

Type of Form	Filed in FY 2004	Filed in FY 2005[1]	Percent e-filed in FY 2004	Percent e-filed in FY 2005
Currency Transaction Report (all types)	13,674,114	14,210,333	11%	24%
Suspicious Activity Report (for all covered industries)	663,655	878,021	17%	42%
Report of Foreign Bank and Financial Accounts	218,667	283,895	E-filing not available	E-filing not available
Registration of Money Services Business	17,037	13,425	E-filing not available	E-filing not available
Designation of Exempt Person[2]	80,763	92,404	E-filing not available	2%
Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300)	151,998	160,449	E-filing not available	E-filing not available
Report of International Transportation of Currency or Monetary Instruments[3]	152,934	153,785	E-filing not available	E-filing not available
Total	14,959,168	15,792,312	11%	24%

[1] Fiscal Year 2005 figures are as of December 2, 2005.

[2] The "Designation of Exempt Person" Form enables depository institutions to use Currency Transaction Report exemption rules to reduce the burden of large currency transaction reporting. Banks, thrifts, and credit unions can use the rules and this form to eliminate the reporting obligation for transactions by most business customers with routine needs for currency.

[3] Reports of International Transportation of Currency or Monetary Instruments are paper reports collected and processed by U.S. Customs and Border Protection, U.S. Department of Homeland Security. These reports are not included in e-filing calculations.

In Fiscal Year 2005, we published an adjusted strategic plan that reflects our role as a regulatory agency, our responsibilities for combating terrorist financing, and our long-range vision for providing law enforcement and regulatory agencies with better access to the Bank Secrecy Act data while supporting these agencies with more complex and sophisticated analyses. The plan, which covers Fiscal Years 2006 through 2008, is available at www.fincen.gov.

The Strategic Plan outlines five goals:

- **Goal 1:** Protect the financial system through effective administration of the Bank Secrecy Act.
- **Goal 2:** Combat terrorism, money laundering, and other financial crime through analysis of Bank Secrecy Act data and other relevant information.
- **Goal 3:** Intensify international anti-money laundering collaboration through the global network of financial intelligence units.
- **Goal 4:** Facilitate regulatory compliance, data management, and information through E-government.
- **Goal 5:** Develop a more nimble and responsive management structure.

This report lists major Financial Crimes Enforcement Network accomplishments for each of these goals in Fiscal Year 2005 and priorities for Fiscal Year 2006.

Goal 1: Bank Secrecy Act Administration

Major Accomplishments in Fiscal Year 2005

Bank Secrecy Compliance Activity

This year, we made marked progress toward assuring the effectiveness and uniformity of Bank Secrecy Act compliance activity in all covered industry sectors. Specifically, we:

- Signed a memorandum of understanding with the Internal Revenue Service to routinely exchange information about Bank Secrecy Act examination activities, including the identification of financial institutions with significant Bank Secrecy Act compliance deficiencies. We now have such agreements with six Federal banking regulators.
- Negotiated 35 information exchange agreements with state and territorial (Puerto Rico) supervisory agencies that examine for compliance with the Bank Secrecy Act or similar state regulations.
- Developed and published an interagency Bank Secrecy Act/Anti-Money Laundering Examination Manual in collaboration with the five Federal banking agencies. The manual is designed to ensure the consistent application of the Bank Secrecy Act at all banking organizations, including commercial banks, savings associations, and credit unions. In conjunction with the manual rollout, we participated in eight outreach sessions, three industry conference calls, and a national video conference for examiners and industry around the country.
- Developed and delivered, through the Federal Financial Institutions Examination Council, nine training sessions for examiners from a variety of federal and state banking agencies.

Board of Governors of the Federal Reserve System

Excerpt from Joint Release

Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision
Financial Crimes Enforcement Network

For Immediate Release June 30, 2005

Agencies Release Bank Secrecy Act/Anti-Money Laundering Examination Manual

The Federal Financial Institutions Examination Council (FFIEC) today released the Bank Secrecy Act/Anti-Money Laundering Examination Manual (FFIEC BSA/AML Examination Manual). The manual's release marks an important step forward in the effort to ensure the consistent application of the BSA to all banking organizations including commercial banks, savings associations, and credit unions.

The FFIEC BSA/AML Examination Manual was developed by the Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS) (collectively referred to as the federal banking agencies) in collaboration with the Financial Crimes Enforcement Network (FinCEN), the delegated administrator of the BSA. In addition, through the Conference of State Bank Supervisors, the state banking agencies played a consultative role. The Office of Foreign Assets Control (OFAC) collaborated on the development of core overview and examination procedures addressing compliance with regulations enforced by OFAC.

The FFIEC BSA/AML Examination Manual emphasizes a banking organization's responsibility to establish and implement risk-based policies, procedures, and processes to comply with the BSA and safeguard its operations from money laundering and terrorist financing.

Praise for Interagency Manual

"This interagency [Bank Secrecy Act/Anti-Money Laundering Examination] manual is a significant step toward consistency in the area of anti-money-laundering examination. The new manual promotes understanding of the Bank Secrecy Act and anti-money laundering regulations and supervisory expectations. We look forward to ongoing dialogue with the industry on these important issues."

—Susan Schmidt Bies, Federal Reserve Board Governor, July 11, 2005

Regulatory Coverage and Guidance

We extended Bank Secrecy Act anti-money laundering program requirements to dealers in precious metals, stones, or jewels to protect this potentially vulnerable industry from abuse by terrorist financiers and perpetrators of financial crime. Further, we issued substantive guidance for industries already covered, including:

- An interpretive advisory requiring money services businesses to perform appropriate due diligence with respect to their foreign agents and counter parties.
- Guidance, an advisory, and a joint statement with Federal banking agencies about the provision of banking services to money services businesses. These steps were taken after fact-finding meetings indicated that some banks were closing or declining to open accounts for money services businesses because of perceived risks.
- Guidance, developed jointly with the federal banking agencies, for financial institutions on exercising reasonable judgment when complying with Bank Secrecy Act obligations in interactions with victims of Hurricane Katrina.

Section 311

To safeguard the financial system at home from criminal threats abroad, we proposed special measures authorized by section 311 of the USA PATRIOT Act against three financial institutions designated as being of "primary money laundering concern" by the Secretary of the Treasury. The institutions are Multibanka and VEF Banka, both located in Latvia, and Banco Delta Asia, located in the Macau Special Administrative Region of China. If made final, the rules will prohibit U.S. financial institutions from establishing, maintaining, administering, or managing any correspondent account in the United States for or on behalf of these banks.

We also conducted in-depth analyses, including interagency consultation, to produce the Administrative Records required for section 311 special measures. In all section 311 activities, we worked closely with our sister organizations within the Treasury Department's Office of Terrorism and Financial Intelligence.

Enforcement

In situations involving egregious violations of the Bank Secrecy Act, we took joint enforcement actions with appropriate regulators. Specifically, we jointly assessed civil money penalties against Arab Bank and AmSouth Bank for systematic violations of the Bank Secrecy Act, including failure to comply with the anti-money laundering program and suspicious activity reporting requirements. We also imposed a civil money penalty against Gulf Corporation for violation of Bank Secrecy Act currency transaction and suspicious activity reporting requirements. We believe that such actions not only resolve compliance issues in the institutions affected but also encourage other institutions to comply with the law.

Accomplishments/ Priorities

Organizational Development

Internally, we strengthened our capacity to assure consistent application of the Bank Secrecy Act. With funds authorized last year by Congress, we hired 18 employees for the Office of Compliance, established in Fiscal Year 2004 to assure that examinations for compliance with the Bank Secrecy Act and related requirements are uniform and effective.

We also developed a system for securely managing the data and cases resulting from the information-sharing agreements with Federal banking regulators and state supervisory agencies, and developed initial reports on financial industry compliance based on the information provided. To improve our ability to respond to industry requests for guidance and assistance in complying with regulatory requirements, we created and began staffing a regulatory resource center to centralize the function of providing responses.

Currency Transaction Report Exemptions

As the year ended, we were working with Congress on a proposal to streamline Currency Transaction Report exemptions for qualified customers. Our aim is to ease reporting burdens on financial institutions covered by the Bank Secrecy Act while continuing to assure that requirements meet the needs of law enforcement agencies.

Priorities for Fiscal Year 2006

Strengthen Regulatory Regime

We will continue to strengthen the Bank Secrecy Act regulatory regime by releasing a number of significant regulations in Fiscal Year 2006. These include:

- Regulations implementing section 312 of the USA PATRIOT Act, which requires that due diligence be performed on correspondent and private banking accounts.
- Final rules and related guidance requiring certain insurance companies to establish anti-money laundering programs and report suspicious activity.
- Regulations requiring investment advisers, commodity trading advisors, commodity pool operators, and unregistered investment companies to establish anti-money laundering programs.
- Rules requiring that mutual funds report suspicious activity.

In addition, we will develop a regulatory framework for stored-value products/ services that reflects ongoing changes in that industry and review our regulatory regime for money services businesses.

Provide Guidance to Covered Industries

To provide covered industries enhanced information about complying with Bank Secrecy Act requirements, we will establish a seminar program on regulatory matters and continue to develop and issue needed guidance. We will also continue to develop a regulatory resource center to integrate web- and telephone-based communications, ensure better consistency and accuracy of responses, improve response times, and improve overall customer service.

Promote Uniform and Effective Application of Law

Promoting consistent application of the Bank Secrecy Act is an ongoing priority. Toward this aim, we plan to develop information exchange agreements with the Securities and Exchange Commission, the Commodity Futures Trading Commission, and additional state supervisory agencies and to use the resulting information to promote uniform application of the law. In situations where financial institutions fail to comply with the Act, we will continue to work closely with the supervisory authorities to take appropriate action.

Cooperation with Industry and Law Enforcement

We will continue to work with the financial industry on ways to reduce the number of Currency Transaction Reports filed on legitimate financial transactions that are of little or no value to law enforcement. We will also seek to develop innovative ways to exchange critical and sensitive law-enforcement information with the financial industry as a means of strengthening a government-private partnership to prevent and detect terrorist financing and other financial crime.

Priorities

Bank Secrecy Act Emphasis on Risk Management

"The Bank Secrecy Act regulatory regime is all about risk management – it is about identifying and mitigating risk. Under the Bank Secrecy Act, financial institutions are required to identify and mitigate the risk that their business will be abused by criminals and terrorists. Risks can be jurisdictional, product-related, service-related, or client related. Regardless of where those risks arise, financial institutions covered by our regulations must take reasonable steps to mitigate them. Compliance is risk-based, meaning that financial institutions must devote more compliance resources to the areas of its business that pose the greatest risk. Moreover, as is true for all industries we regulate, we do not expect businesses of different sizes and circumstances to have the same types of anti-money laundering programs."

—William J. Fox, Jewelers Vigilance Committee Industry Seminar, August 1, 2005

Accomplishments

Goal 2: Analysis

Major Accomplishments in Fiscal Year 2005

Law Enforcement Support

A major thrust during Fiscal Year 2005 was to develop and begin to implement a strategy for focusing our law enforcement support activity on high impact, complex analyses rather than on straightforward database queries. In line with this strategy, we increased our production of analytic products defined as "complex" and reduced the number of basic database queries that law enforcement agencies with direct access to the Bank Secrecy Act data can more efficiently conduct themselves. We also supported major Federal law enforcement agencies by analyzing Suspicious Activity Report data to assess trends, patterns, and threats in specific states and localities.

New Analytical Paradigm

"We are changing the way we analyze information at the Financial Crimes Enforcement Network. We are moving away from the notion of FinCEN as a library, with FinCEN analysts acting as librarians assisting customers with efforts to retrieve and understand Bank Secrecy Act data. Our new analytical paradigm requires higher-level research and analysis utilizing all sources of information to understand and explain the cutting-edge problems relating to money laundering and illicit finance, including terrorist financing. Our goal is nothing short of being as good as, if not better than, any other analytic unit focused on financial issues in the world."

—William J. Fox, before the U. S. House of Representatives Committee on Financial Services, Subcommittee on Oversight and Investigations, May 26, 2005

Policy Level Analysis

We developed a number of policy-level analytical products, including:

- An analysis of the trends, patterns, and financial crime vulnerabilities for domestic shell corporations (limited liability companies and corporations).
- A national analysis of Suspicious Activity Report data in support of the Money Laundering Threat Assessment being prepared by the U.S. Department of the Treasury.

Regulatory Analysis

For the first time, we devoted staff resources to regulatory analyses, including assessments of 42 banking institutions identified by banking regulators as having possible compliance issues with the Bank Secrecy Act.

Funds Transfer Guide

As part of our Technical Reference series, we published a comprehensive, Official Use Only guide for law enforcement agencies on the mechanisms used for funds transfers. The guide provides investigative officials with information about funds transfer processes and systems, the related roles of financial institutions and centralized funds transfer systems, and the documentation generated for funds transfer transactions.

Customer Feedback on Funds Transfer Guide

"Thank you VERY much for the new Funds Transfer Guide. Excellent job. I know that this will be a very handy reference guide to our analysts and investigators. In fact, I provided one to a TFOS [Terrorist Financing Operations Section] analyst… and she was thrilled…. I've requested that it be posted… on the FBI Intranet."

—FBI Liaison to the Financial Crimes Enforcement Network

"I write to commend you and your staff on the recent publication of the Reference Series: Funds Transfers…. We believe that the Financial Crimes Enforcement Network's success in publishing this first-rate manual will lead to higher quality investigations throughout the United States Law enforcement community."

—Special Investigator, U.S. Federal Reserve

"This looks like a great source of info for the agent in the field who's working complex fraud or money laundering cases and needs to query banks for transaction information to further their investigation. This reference will be helpful to investigators who aren't totally aware of the funds flow process or the information sources and documentation available through the banking industry."

—U.S. Secret Service Analyst

Training

We strengthened our ability to perform complex analyses of all-source data by providing our analysts with more than 10,500 hours of high-level analytical skills training. The training included courses at the Central Intelligence Agency's Sherman Kent School, the Defense Intelligence Agency's Joint Military Intelligence Training Center, and the Foreign Service Institute.

Priorities

Priorities for Fiscal Year 2006

Complex Analysis for Law Enforcement

We will continue to enhance the value of our support to law enforcement agencies by increasing the amount of complex, actionable analyses targeted at high-priority money laundering and terrorist financing investigations and reducing the amount of basic Bank Secrecy Act research that the agencies could more efficiently perform themselves. We will also develop financial intelligence referrals for use by the U.S. Department of Justice U.S. Attorney's Office in identifying high-impact investigative cases.

Policy-level Analyses

We will publish in-depth analytical products covering patterns and trends in financial crimes and regulatory and/or industry vulnerabilities that will serve as the basis for policy decisions and strategic action to reduce the threat of financial crime. A project of this type already in progress is an analysis of mortgage loan fraud based on Suspicious Activity Report filings.

Collaboration

We will take full advantage of sources of and resources for financial intelligence by completing collaborative analytic efforts with other organizations. We will work on joint projects with analysts from other financial intelligence units, from at least one large Federal law enforcement agency, and from the intelligence community.

Technical Reference Guide

We will publish at least one technical reference guide for law enforcement officials describing a financial transaction system.

Goal 3: International Collaboration

Major Accomplishments in Fiscal Year 2005

Egmont Group Plenary

In Fiscal Year 2005, the Financial Crimes Enforcement Network hosted the 13th Plenary of the Egmont Group, an international network of financial intelligence units. (See page 47.)

The Plenary was a major international event that marked the Egmont Group's 10th anniversary. The meeting was attended by nearly 300 delegates from more than 90 financial intelligence units from countries and jurisdictions around the world, as well as by representatives from international organizations. At the Plenary, seven new financial intelligence units were granted membership, bringing the total to 101.

Collaboration with Other Financial Intelligence Units

We collaborated and communicated with many other financial intelligence units and governments in Fiscal Year 2005 in efforts to strengthen anti-terrorist financing and anti-money laundering programs and policies world wide. For example, we:

- Conducted personnel exchanges with the financial intelligence units in Russia, Mexico, and Liechtenstein. The exchanges were designed to improve channels for communicating operational information in support of anti-money laundering and terrorist financing investigations.
- Ended a 4-year moratorium on the exchange of financial intelligence with Paraguay, where the existence of more than one financial intelligence unit violated Egmont Group standards. To address this issue, we traveled to Paraguay with representatives from the Treasury Department's Office of Technical Assistance. Following resolution, we signed a Memorandum of Understanding with Paraguay to reinstate information sharing.
- Participated with other U.S. Department of the Treasury officials in bilateral talks with Brazil, Chile, Guatemala, Mexico, Jordan, France, and Austria to discuss efforts to counter terrorist financing and money laundering.

Accomplishments

Assessments

With other U.S. agencies, international groups, or financial intelligence units, we conducted assessments of the financial intelligence units in the Philippines, Peru, and Qatar, and of the anti-money laundering and terrorist financing regimes in Afghanistan, Nigeria, and Tanzania. We also traveled with Treasury's Office of the Comptroller of the Currency to examine bank compliance issues in Romania's banking, regulatory, and law enforcement sectors.

We used our expertise in the international financial arena to write 110 country assessments on financial crimes and money laundering for the International Narcotics Control and Strategy Report published by the U.S. Department of State.

Financial Intelligence Unit Development

To help our counterparts strengthen their capacities, we coordinated and/or secured outside funding to train analysts from 17 different financial intelligence units in South and Central America, the Caribbean, and the Caucasus. Partners in these efforts included the U.S. Departments of Justice and State, other Egmont members, the Organization of American States, and the International Monetary Fund/World Bank. We also linked nine additional financial intelligence units to the Egmont Secure Web, which allows secure global information exchanges related to financial crimes investigations in Egmont member countries.

Through our foreign visitors program, we hosted or briefed government, financial sector, or law enforcement agency representatives from 58 countries. We provided these visitors with information on new money laundering trends and patterns, the Bank Secrecy Act, details of the USA PATRIOT Act, information technology systems and databases, international information exchange processes, and the regulatory role of the Financial Crimes Enforcement Network.

Key Global Activity, Fiscal Years 2003 - 2005

	FY 2003	FY 2004	FY 2005
Number of countries to which Financial Crimes Enforcement Network provided assistance in establishing financial intelligence units	9	11	9
Number of established financial intelligence units to which Financial Crimes Enforcement Network provided regulatory and technical assistance	34	27	30
Number of financial intelligence units connected to Egmont Secure Web during fiscal year	13	20	9
Total number of financial intelligence units connected to Egmont Secure Web	64	84	93
Number of law enforcement cases supported through information-sharing with foreign jurisdictions[1]	724	844	985

[1] Includes requests for information from other financial intelligence units and information requests to financial intelligence units

Priorities for Fiscal Year 2006

Egmont Group Leadership

To strengthen the global network of financial intelligence units, we will continue to chair the Egmont Group's Egmont Committee and to provide staff support for the organization's five working groups. We will sponsor a number of financial intelligence units in the Middle East and Asia for admission to the Egmont Group and will conduct onsite acceptance assessments of at least five potential new members as part of the admission process.

Country Assessments

We will devote increased resources to the production of written reports assessing the anti-money laundering and terrorist-financing policies and programs in countries with significant financial centers or other characteristics that make them especially important in the international effort against financial crime. We expect these reports to provide important financial intelligence for other Federal agencies and for international organizations that set policy and standards for combating financial crime.

Support for the Financial Action Task Force

We will coordinate research for and publication of a Financial Action Task Force Typologies Report on "Money Laundering and Terrorist Financing Trends and Indicators." The Financial Action Task

Force is an inter-governmental body created in 1989 to develop and promote national and international policies to combat money laundering and terrorist financing.

Collaboration

Strengthening collaboration among financial intelligence units remains a priority. To this end, we plan to conduct personnel and operational exchanges with five financial intelligence units.

Egmont Secure Web

We will upgrade the Egmont Secure Web to leverage new technology, expand services to financial intelligence units, and facilitate information sharing. We will also continue to connect new financial intelligence units to the Egmont Secure Web and to collaborate with FIU.NET, a computer network that enables intelligence units from the European Union to share financial intelligence quickly and securely.

Priorities

Global Threat of Terrorist Financing and Money Laundering

"There is now near-unanimous recognition among nations that terrorist financing and money laundering pose threats that cannot be ignored and there is widespread agreement upon a shared set of standards to combat these dangers. We will not accept the protest that ideological differences or bureaucratic obstacles excuse nations from the obligation to comply with global standards. As we were all brutally reminded by the attacks in London last week, we are facing a global threat with global implications. All civilized nations must meet their basic responsibilities to prevent the financing and support of terrorism."

—Stuart Levey, Under Secretary, Office of Terrorism and Financial Intelligence, U.S. Department of the Treasury, before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, July 13, 2005

Goal 4: E-Government

Major Accomplishments in Fiscal Year 2005

BSA Direct

To improve the management of data filed under the Bank Secrecy Act, we managed the development and initial testing of BSA Direct, a major initiative that provides the architecture for long-range plans to collect, process, store, and disseminate Bank Secrecy Act data. BSA Direct establishes a data warehouse with integrated query and analysis tools that will streamline and enhance our customers' processes for accessing and analyzing data collected under the Bank Secrecy Act. BSA Direct will be deployed to authorized users of the Bank Secrecy Act data in Fiscal Year 2006.

E-Filing

We provided outreach and technical assistance to support an increase in electronic filing of Bank Secrecy Act reports from 11 percent in Fiscal Year 2004 to 24 percent in Fiscal Year 2005. During the last two months of the year, 29 percent of reports were electronically filed.

E-Filing Found Effective

"We found BSA E-Filing to be an effective mechanism for filing BSA reports. BSA E-Filing reduces processing time, provides controls to improve the accuracy, completeness, and security of BSA data, and, if used instead of paper processing, could significantly reduce the cost of processing BSA reports. Moreover, institutions using BSA E-Filing to file reports generally found the system easy to use."

—Treasury Office of Inspector General report on BSA E-Filing, March 31, 2005

Accomplishments

Support for Users of Bank Secrecy Act Data

We more effectively assisted the law enforcement and regulatory agencies that access Bank Secrecy Act through our Gateway program, which provides data access via a secure internet connection. For example, we developed and implemented an on-line training program that eliminated the need for live training classes and allowed redirection of internal resources. This system improved management of content, and provides re-certification testing to ensure that our users are updated on program changes.

We also authorized, trained, audited, and provided customer assistance to 3,344 Gateway users, almost 1,200 more than in Fiscal Year 2004. The number of users trained rose from 1,007 to 1,343, and the number of inspections more than doubled—increasing from 313 to 679.

314 Information-Sharing Program

In Fiscal Year 2005, we strengthened both policies and technology for the information-sharing program authorized by section 314 of the USA PATRIOT Act for Federal law enforcement agencies and financial institutions. This program is designed to support investigations with a significant money laundering or terrorist financing component. Specifically, we:

- Developed and deployed a secure, web-based system for transmitting information requests from Federal law enforcement agencies to financial institutions, and for transmitting the institutions' responses. Previously, information requests and responses were transmitted via a slower system of e-mail and faxes.
- Streamlined the section 314 program policy and strengthened the acceptance criteria for incoming requests. These changes have improved the quality of these requests, further ensured that investigative agencies have exhausted other means of information, and reduced the burden on financial institutions that conduct the requested searches.

Treasury Designates Mexican Money Laundering Cell; Financial Crimes Enforcement Network Provided Supporting Data

On January 12, 2005, the U.S. Department of the Treasury identified 15 companies and 24 individuals associated with a money laundering cell of the Arellano Felix Organization (AFO), a violent drug trafficking ring operating out of Mexico.

"Over a three year period, this cell laundered more than $120 million in illicit proceeds from the sale of narcotics," said Robert Werner, Director of the Treasury's Office of Foreign Assets Control (OFAC). "By freezing these individuals and companies out of the U.S. financial system, we are dealing a significant blow to the fiscal underbelly fueling the notorious drug trade of the Arellano Felix Organization."

OFAC added the names of these 39 entities to its list of persons designated pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act). AFO, which was named as a drug kingpin by President Bush on June 1, 2004, is based in Tijuana, a large city in the Mexican state of Baja California, which borders the United States.

This money laundering cell was developed by Ivonne Soto Vega, also known as "La Pantera" (the Panther), and Jose Manuel Ruelas Martinez. The cell is involved in a money laundering scheme centered on the use of casas de cambio, or currency exchange houses. These front companies launder U.S. currency illicitly earned through narcotics sales in the United States and bulk smuggled into Mexico.

The Financial Crimes Enforcement Network played several roles in the support and development of the investigation. Members of the Ruelas Martinez family, their associates, and their businesses and currency houses were the subject of a USA PATRIOT Act Section 314(a) information request that FinCEN broadcast to financial institutions in 2003 on behalf of a Federal law enforcement agency. The request resulted in the identification of numerous previously unknown bank accounts in the United States.

Members of the Ruelas Martinez organization and their associated businesses were also the subjects of a proactive targeting report prepared by FinCEN. In addition, the Ruelas Martinez investigation was the first case developed as part of a pilot program to concurrently conduct financial, law enforcement, and commercial database analysis of the subjects of Section 314(a) requests to provide the requesting law enforcement agencies with the most comprehensive analytical product available. An agent from the investigating agency said that the identification and analysis of numerous Bank Secrecy Act documents, in conjunction with accounts identified through the 314(a) request "helped expand the investigation by identifying new leads and accounts."

—Compiled from Treasury Department Press Release, January 12, 2005, and reports by Financial Crimes Enforcement Network staff

Priorities

Priorities for Fiscal Year 2006

BSA Direct

We will continue to closely manage the final development stages and rollout of BSA Direct. We will transition customers to this new system and integrate additional system components. Following full deployment, we will survey users to establish a baseline measure of user satisfaction with the system.

E-filing

We will continue to increase the percentage of Bank Secrecy Act reports that are electronically filed by providing outreach and technical assistance to the largest filers.

Suspicious Activity Report Data Quality

To improve the quality of Suspicious Activity Report data, we will identify the critical fields that are most often left blank. This analysis will serve as the foundation for developing strategies to reduce data omissions and ensure that the data reported is of maximum benefit to law enforcement agencies.

Cross-Border Wire Transfer Feasibility Study

We will conduct a feasibility study for a system to collect data on cross-border wire transfers, as mandated by the Intelligence Reform and Terrorism Prevention Act of 2004. Such a system would eliminate an important gap in the financial transactions data now available to law enforcement and intelligence agencies.

Infrastructure

We will upgrade our corporate case and document management capabilities and enhance the overall security and safety of FinCEN's network infrastructure.

Management Goal

Major Accomplishments in Fiscal Year 2005

Organizational Realignment

In Fiscal Year 2005, we completed a major organizational restructuring initiated the previous year to realign functional units with our strategic priorities. Among other actions, we:

- Filled 10 senior management positions previously held by persons serving in an acting capacity.
- Set up the Office of Public Affairs, which reports to the Deputy Director, to more effectively communicate our programs and objectives to the public and the media.
- Established the Office of Intelligence Support to provide analytic services for the intelligence community. This office works closely with Treasury's Office of Intelligence and Analysis and other agencies engaged in anti-terrorist investigations and activity.

Strategic Plan

Following the introduction of our new strategic plan in February 2005, we established systems for monitoring and communicating progress toward achieving the plan. We also developed organizational performance measures linked to the strategic plan and implemented a system for quarterly reporting of progress toward these measures.

Treasury Department Collaboration

We increased collaboration within Treasury's Office of Terrorism and Financial Intelligence through joint projects with the Office of Foreign Assets Control and the Office of Intelligence and Analysis. Cooperative activities included personnel details, sharing of information concerning terrorism-related requests for research, and joint travel to bolster anti-money laundering and counter-terrorism regimes in several countries.

Staff Hiring, Training, and Performance Management

We used our increased budget to hire 64 new employees, strengthening our total force from 253 to 291 employees. To help both new and experienced staff develop their expertise, we provided over 270 training opportunities for our employees, including technical or job skills training for 214 employees and management skills training for 100 percent of our managers.

We also implemented a bureau-wide, multi-tier performance management system for employees and drafted a comprehensive awards policy to reward excellent performance.

Financial Management

To steward the growing financial resources with which we have been entrusted, we ensured that management control systems provided reasonable assurance of compliance with the Federal Managers

Financial Integrity Act. No material weaknesses were open in Fiscal Year 2005. We also completed our first balance sheet audit and received an unqualified audit opinion from the independent auditors.

Employee Programs

We promoted diversity awareness and wellness among employees by presenting four special emphasis programs addressing gender, ethnic, and health issues in the workplace. We also presented five additional community-building and employee recognition programs, including Diversity Day; Bring Your Child to Work Day; an appreciation luncheon for employee volunteers involved in special emphasis programs; the Director's Awards Program; and a Holiday Celebration.

Security

In line with our increased responsibilities in the area of terrorist financing, we took steps to move from a "Public Trust" to a "National Security" security posture by developing a personnel security policy that sets minimum risk and sensitivity designations for positions throughout our organization.

Priorities for Fiscal Year 2006

Human Capital

Recognizing that we cannot achieve our mission without a diverse, high-performing workforce, we will take steps to expand and enrich our human assets. To align our workforce with current and future mission needs, we will develop:

- A Human Capital Strategic Plan.
- A corporate recruitment plan that will help us continue to attract diverse, highly-skilled new employees.
- A succession planning strategy that includes programs for building needed skills, mentoring, and regular in-house professional development.

We will also assess competency gaps for mission-critical occupations, streamline hiring through approved hiring flexibilities, and design a training strategy for managers in support of succession planning.

Internal Communications

We will develop and implement a strategy for enhancing communications among our Divisions and Offices as well as between managers and nonsupervisory employees. A key element of this strategy will be quarterly "town hall" meetings that focus on progress toward meeting our performance measures and goals.

Public Website

We will re-design our public website to improve content, organization, design, navigation, and ease of use.

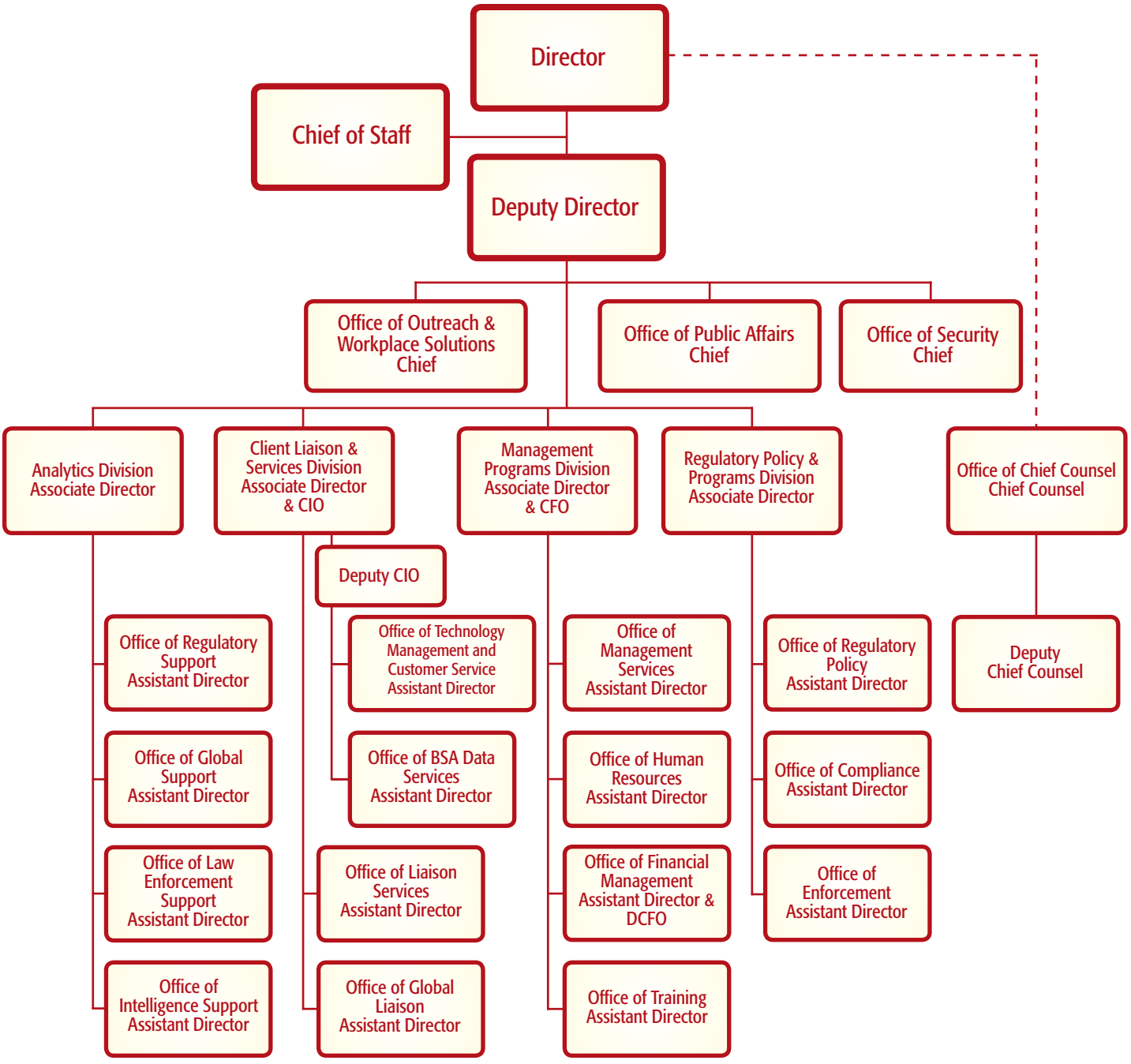
Security

In line with our expanding mission in the area of combating terrorist financing, we will continue to move from a security posture emphasizing "Public Trust" to one emphasizing "National Security." We will also continue to take all steps needed to assure the security and reliability of our data, our technology infrastructure, and our major technology initiatives.

Program Assessments and Audits

We will conduct Program Rating and Assessment Tool (PART) program evaluations for all bureau programs not yet assessed. We will also complete the first full audit of all financial statements by an independent auditor.

The Financial Crimes Enforcement Network includes the Office of the Director and four major operating divisions. In addition, the Office of Chief Counsel, which reports to the U.S. Department of the Treasury, provides legal services for the Financial Crimes Enforcement Network. Descriptions of these units and biographies of key officials follow:



Office of the Director

The Office of the Director is made up of the Financial Crimes Enforcement Network's top executives and support staff. It includes the Director, Deputy Director, Chief of Staff, Office of Security, Office of Outreach and Workplace Solutions, and Office of Public Affairs. Key officials in the Office of the Director include the following:

William J. Fox was appointed by Treasury Secretary John Snow to be the fourth Director of the Financial Crimes Enforcement Network on December 1, 2003. As Director, Mr. Fox leads our role as administrator of the Bank Secrecy Act, which authorizes the collection, analysis and dissemination of financial information important to the prevention of money laundering and terrorist financing.

Prior to his appointment as FinCEN's Director, Mr. Fox served as Treasury's Associate Deputy General Counsel and Acting Deputy General Counsel. After September 11, 2001, he also served as the principal assistant and senior advisor to Treasury's General Counsel on issues relating to terrorist financing and financial crime. Mr. Fox was recognized for his work on these issues with a Meritorious Rank Award in October 2003.

Mr. Fox came to the Department of the Treasury in December 2000 as the Acting Deputy Assistant General Counsel for Enforcement. From 1988 to December 2000, he served at the Bureau of Alcohol, Tobacco and Firearms (ATF), first as an attorney in ATF's Chicago office, then as the Senior Counsel for Alcohol and Tobacco and finally as ATF's Deputy Chief Counsel. During his time with ATF, Mr. Fox provided legal support to several large scale criminal investigations; helped oversee ATF's regulatory program; served as a legal point person for ATF's alcohol and tobacco diversion program; worked on several important legislative initiatives; and served as principal legal support for the United States Trade Representative's Office for wine trade negotiations with the EU and other wine producing countries.

Mr. Fox was born and raised in Nebraska. He received his bachelor's degree in history and a law degree from Creighton University in Omaha. In March 2005, U.S. Banker magazine named him one of the 25 most influential people in high finance. He is married and has two children.

William F. Baity was appointed Deputy Director of the Financial Crimes Enforcement Network in January 1995. In his position as Deputy Director, Mr. Baity is responsible for working

with the law enforcement, financial and regulatory communities to ensure the effective coordination of anti-money laundering initiatives.

Before his appointment, Mr. Baity served as Acting Director (February 1994 - December 1994) and Deputy Director (August 1991- December 1994) of the United States Bankruptcy Trustee Program of the Department of Justice. He also served for more than three years as the first United States Trustee for Region 5 (the Judicial Districts of Louisiana and Mississippi). From February through October 1990, Mr. Baity concurrently administered Region 15 (the Judicial Districts of Southern California, Hawaii, and Guam).

From 1980 to 1988, Mr. Baity served as an Assistant U.S. Attorney in the Eastern District of Louisiana, headquartered in New Orleans; he was chief of the Civil Division in that district during his last four years in the position. From 1976 to 1980 he was an Assistant Director Legal Officer in the U.S. Coast Guard, supervising all cases involving criminal maritime enforcement, such as narcotic, fishery and environmental violations. Before joining the government, he worked for the Exxon Company as an Economic and Business Analyst.

Mr. Baity received a bachelor's degree in mathematics from North Carolina College in 1969, a master's degree in Industrial Administration from Carnegie-Mellon University in 1971, and a J.D. from Vanderbilt University in 1976. He is admitted to the bars of Louisiana and Tennessee. Mr. Baity is married with two children.

Jeff Schwarz was named Chief of Staff for the Financial Crimes Enforcement Network in July 2004. In this capacity, he serves as the principal advisor to the Director. He oversees daily operations, coordinates policy implementation for the agency, and advises the Director on management issues impacting the organization.

Mr. Schwarz began his career with the Uniformed Division of the U.S. Secret Service at the Department of the Treasury. He then moved to the Department of State, where he served as a Special Agent with the Bureau of Diplomatic Security. Later, he went to the Department of Defense, where he became the Defense Criminal Investigative Service's representative to the Financial Crimes Enforcement Network. During his career, Mr. Schwarz has served as a Special Agent in Washington D.C., Los Angeles, Cleveland and Chicago.

Mr. Schwarz received a bachelor of arts in political science and a master of science in education administration from Fort Hays State University.

Office of Chief Counsel

The Financial Crimes Enforcement Network is dedicated to maintaining the highest legal and ethical standards of government service. The Office of Chief Counsel supports that goal by providing legal services to the bureau in the conduct of all its operations, ranging from statutory and regulatory interpretation and drafting to ethics determinations and training.

Brian L. Ferrell was appointed by Treasury's General Counsel to be the Chief Counsel of the Financial Crimes Enforcement Network in July 2005. In that role, Mr. Ferrell supervises attorneys and support staff that provide legal advice to bureau officials across the full range of their responsibilities.

Mr. Ferrell previously served as Chief Counsel of the Department of the Treasury's Bureau of the Public Debt, and as Treasury's Senior Counsel for Litigation. Before joining the Department of the Treasury in 2001, Mr. Ferrell spent nearly eight years as a Trial Attorney at the Department of Justice. Prior to entering government service, he spent several years in a litigation practice in upstate New York and two years as Assistant Dean of his Alma Mater.

Mr. Ferrell holds a bachelor's degree from Creighton University, a J.D. from Creighton University School of Law, and a master's degree in environmental law and policy from Vermont Law School. He is a member of the Nebraska and New York bars.

Office of Chief Counsel Activity, Fiscal Years 2003 – 2005

	FY 2003	FY 2004	FY 2005
Regulations and Federal Register Notices issued	47	28	6
Advisories issued	8	5	1
Memoranda of Understanding completed	11	28	84
Regulatory rulings issued	0	3	6
Enforcement actions	4	4	3

Analytics Division

The Financial Crimes Enforcement Network is the largest overt collector of financial crimes intelligence in the United States. The information we collect under the Bank Secrecy Act is highly valuable in combating terrorism and investigating money laundering and other financial crime. The Analytics Division includes approximately 80 analysts who mine the Bank Secrecy Act data and fuse it with other information to support regulatory and policy decisions and to assist law enforcement and intelligence agencies investigating terrorist financing and significant financial crimes.

David M. Vogt was named Associate Director of Analytics for the Financial Crimes Enforcement Network (FinCEN) in October 2004. In this capacity, he directs policy-level financial and threat analyses, as well as analyses in support of domestic law enforcement investigations, international law enforcement investigations, regulatory activities, and intelligence agencies.

Since joining FinCEN at its inception in 1990, Mr. Vogt has served as Acting Deputy Director and as an Assistant or Associate Director in each of the bureau's primary operational areas. Before assuming his

Analytic Products – Fiscal Years 2004 and 2005

	FY 2004	FY 2005
"Complex" analytical products[1]	42	125
Analytical products related to geographic threat assessments, money laundering/illicit financing methodologies, and/or analysis of Bank Secrecy Act compliance patterns	56	116
Number of law enforcement cases supported through information requests to or from foreign jurisdictions	844	985
"Basic" analytic products[2]	2,262	1,137[3]
Total analytic products completed by FinCEN employees and contractors	2,913	1,436[3]
Number of subjects researched by FinCEN employees and contractors	19,304	8,323[3]
Number of analytical products to support intelligence community	79	39[4]

1 "Complex" products include synthesis of data from multiple sources, interpretation of findings, link charts, recommendations for action and/or policy.

2 "Basic" products consist of database queries and reports without interpretation of findings.

3 Decrease reflects the Financial Crimes Enforcement Network's strategy of moving resources away from routine database queries to more complex analysis.

4 Decrease reflects a shift in emphasis to longer-term, more complex analysis in support of Section 311 of the USA PATRIOT Act.

current post, he served as FinCEN's Strategic Planning Advisor. Mr. Vogt's extensive experience before joining FinCEN included serving as a civilian employee in various capacities at the National Security Agency from 1975-1988.

Mr. Vogt holds bachelor's and master's degrees from the University of Missouri.

Client Liaison and Services Division

The Client Liaison and Services Division, headed by our Chief Information Officer, is responsible for managing the Bank Secrecy Act data. The Division performs a variety of roles related to collection, processing, and dissemination of the Bank Secrecy Act data. For example, the Division manages:

- The Gateway program, through which law enforcement agencies and regulators can access the Bank Secrecy Act data through a secure web connection. We authorize Gateway users, train them, and monitor their use to ensure that the data, which are considered law enforcement sensitive, are properly used, disseminated, and kept secure.
- The ***Platform*** and ***Detailee*** programs, which enable Federal law enforcement and intelligence agency representatives to utilize our databases and analytical tools on-site at our facility.

The Division also provides liaison services with domestic law enforcement agencies, with our counterpart foreign intelligence units in other countries, and with international organizations that set international standards for anti-money laundering and anti-terrorist financing programs. The Division's Special Programs Development Section prepares technical reference guides for law enforcement and other agencies on complex financial transactions.

In addition, the Division manages the technical infrastructure needed for internal operations within the Financial Crimes Enforcement Network.

Jack Cunniff was named Associate Director of Client Liaison and Services for the Financial Crimes Enforcement Network in June 2004. In this capacity, Mr. Cunniff oversees information technology and liaison initiatives in support of our partners within the law enforcement, regulatory and international communities. In addition, he serves as Chief Information Officer. Mr. Cunniff joined the bureau in December 2003 as the Gateway Program Manager.

Mr. Cunniff was previously the Deputy Assistant Inspector General for Investigations at the Federal Emergency Management Agency, Office of Inspector

General. That office became the Department of Homeland Security Office of Inspector General. He also served as a Senior Policy Advisor for the Under Secretary of Treasury (Enforcement). Mr. Cunniff began his law enforcement career as a Special Agent with the U.S. Secret Service in New York in 1975. He held senior management positions in the Intelligence and Presidential Protective Divisions, ending his career with the Secret Service in 1999 as the Special Agent in Charge of the Office of Protective Operations.

Mr. Cunniff received his bachelor's degree from Northeastern University in Boston.

Law Enforcement Support through Financial Crimes Enforcement Network Research and Provision of Access to Bank Secrecy Act Data,

Fiscal Years 2003 – 2005

	FY 2003	FY 2004	FY 2005
Number of law enforcement cases supported through research by FinCEN staff/ contractors	4,403	2,913	1,400
Platform/Detailee cases (individuals from other agencies work on-site at FinCEN)	2,058	2,640	2,519
Gateway cases (customers access Bank Secrecy Act data through secure Internet)	9,410	14,795	19,785
Total cases supported[1]	15,871	20,348	23,704
Number of subjects researched for law enforcement by FinCEN	30,429	19,304	8,323
Subjects researched by Platform participants and Detailees	8,345	9,425	9,517
Subjects researched by Gateway users	22,980	33,954	50,113
Total subjects researched	61,754	62,683	67,953

[1] Totals do not include cases or subjects in Federal law enforcement agencies with authorized downloads of Bank Secrecy Act data.

Regulatory Policy and Programs Division

The Regulatory Policy and Programs Division assists in safeguarding the financial system through balanced and consistent administration of the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001. The Division's Office of Regulatory Policy develops and implements policy through outreach, training, and the issuance of anti-money laundering program, record keeping, and reporting regulations and guidance.

The Division's Office of Compliance promotes effective and uniform application of the regulations by providing support for and oversight of Bank Secrecy Act compliance examinations conducted by other Federal agencies that have been delegated examination authority. More information about these organizations appears on page 45. The Office of Compliance also interacts and exchanges data with a variety of self-regulatory organizations and state regulatory authorities that conduct anti-money laundering examination activities for their own purposes.

The Division's Office of Enforcement addresses instances of non-compliance with the Bank Secrecy Act by penalizing egregious or systemic offenses, compelling corrective action, and promoting future compliance.

The Division also takes regulatory action authorized under section 311 of the USA PATRIOT Act of 2001 if the Secretary of the Treasury finds reasonable grounds for concluding that a financial institution, jurisdiction, class of transaction, or type of account is of primary money laundering concern. Under this authority, we are authorized to impose a range of special measures that require U.S. financial institutions to take a variety of remedial actions, up to and including a prohibition on the opening or maintenance of correspondent or payable-through accounts.

William D. Langford was named Associate Director of the Financial Crimes Enforcement Network's Regulatory Policy and Programs Division in May 2004. As Associate Director, he oversees the bureau's regulatory functions, including the development and implementation of regulatory policy, Bank Secrecy Act compliance oversight, and civil enforcement. He joined the organization in December 2003 as a principal advisor to the Director for strategic development and administration of regulations involving the Bank Secrecy Act. Since September 11, his focus has been largely on the implementation of the anti-terrorism and anti-money laundering provisions of the USA PATRIOT Act, including the drafting of the regulations implementing these provisions.

Mr. Langford previously held positions as Senior Advisor to the General Counsel as well as Senior Counsel for Financial Crimes in the Office of the Assistant General Counsel for Enforcement, both in the Department of the Treasury. Prior to joining the government, he practiced law, focusing on commercial litigation.

Mr. Langford holds a bachelor of arts in mathematics from Hastings College in Nebraska, and a J.D. from the University of Texas School of Law.

Key Regulatory Activity – Fiscal Years 2003 – 2005

	FY 2003	FY 2004	FY 2005
Number of federal, state, and territorial financial regulators with whom information-sharing agreements have been executed	0	5	41
Number of compliance matters referred to FinCEN for review and, as appropriate, consideration of possible enforcement action	49	52	233
Number of regulatory inquiries answered (Helpline, Financial Institutions Hotline, e-mail, correspondence, and publication requests)	7,119	8,893	7,612[1]
Number of rulings issued interpreting Bank Secrecy Act regulations concerning money services businesses	8	7	27
Bank Secrecy Act forms revised	8	4	4[2]
Bank Secrecy Act forms for which revisions were proposed	3	1	5[3]

1 The decrease in the total from Fiscal Year 2004 reflects a decline in and shifts in responsibility for answering technical questions about the information program authorized by section 314a of the USA PATRIOT Act. Beginning in Fiscal Year 2005, the Client Liaison and Services Division became responsible for answering these inquiries and the Regulatory Policy and Programs Division answered only regulatory inquiries about this program.

2 Currency Transaction Report; Designation of Exempt Person; Registration of Money Services Business; Suspicious Activity Report by Securities and Futures Industries

3 Currency Transaction Report by Casinos; Suspicious Activity Report by Casinos and Card Clubs; Suspicious Activity Report for Depository Institutions; Suspicious Activity Report by Insurance Companies; Suspicious Activity Report by Securities and Futures Industries

Management Programs Division

The Management Programs Division performs a crucial enabling role in achieving the mission of the Financial Crimes Enforcement Network. The Division leads efforts to attract, develop, and retain a highly skilled, diverse workforce, facilitates responsiveness to internal and external customers, and evaluates bureau performance to meet stakeholder requirements.

Headed by our Chief Financial Officer, the Management Programs Division accomplishes these goals by providing financial, planning and performance measurement, human resources, and logistics services critical to the Bureau's operations. This Division, formerly known as the Administrative and Communications Division, includes four offices: Financial Management, Management Services, Human Resources, and Training. The Division manages our financial resources; provides human capital leadership and services; ensures staff training and individual development opportunities; offers graphics and editorial support for internal and external publications; and provides contracting, logistics, records management, and other essential services.

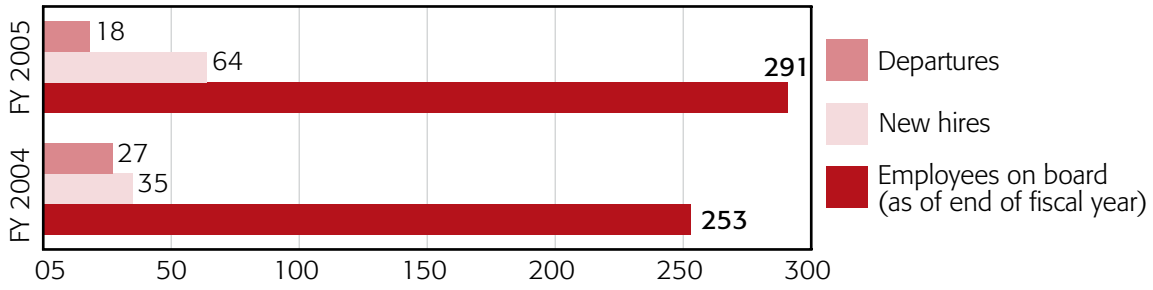
In November 2004, **Diane K. Wade** was named Associate Director of the Financial Crimes Enforcement Network's Management Programs Division, which provides human resources, financial management, administrative, and communications services for the bureau. In addition, Ms. Wade serves as Chief Financial Officer.

Before joining the bureau, Ms. Wade led a team implementing the Department of Energy's Budget and Performance Integration and Five-Year planning initiatives. She was also a civilian employee in the Department of the Army, serving most recently as Acting Deputy Division Chief, Operating Force Division, in the Army's Budget Office. In that position she was responsible for the formulation and justification of the Army's $21.0 billion operations budget. Ms. Wade also led the preparation and justification of the Army's Training and Mobilization budgets and served as Chief, Resource Management Division, of the Army's Material Command – Far East.

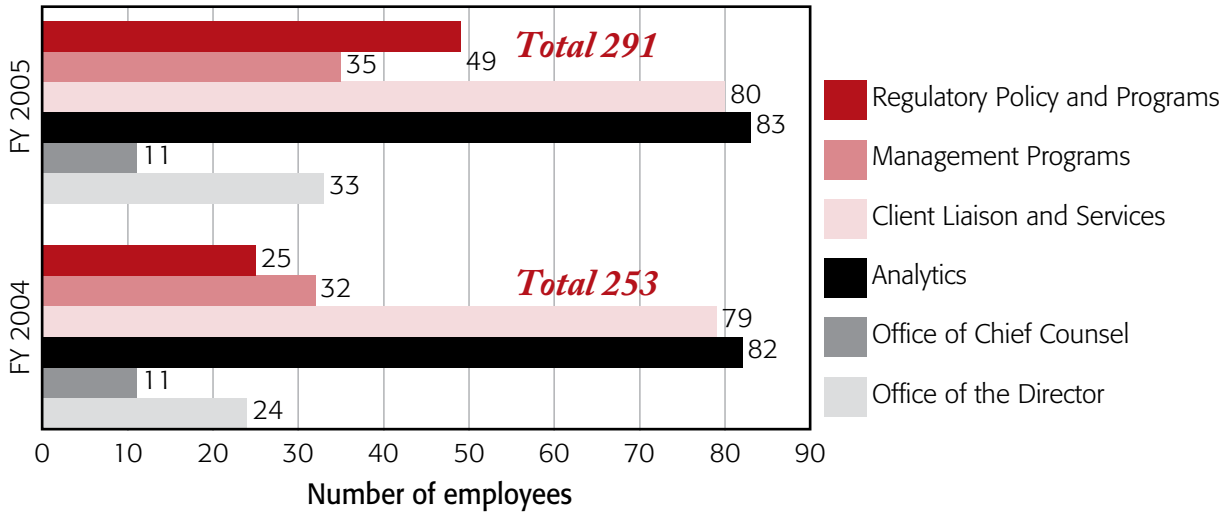
Ms. Wade holds a bachelor of science in marketing from George Mason University in Virginia.

The Financial Crimes Enforcement Network is a small, growing bureau. As of September 30, 2005, we had a staff of 291, including 27 managers.

Financial Crimes Enforcement Network Staff



Number of On-board Employees by Division



Managers and Non-supervisory Employees

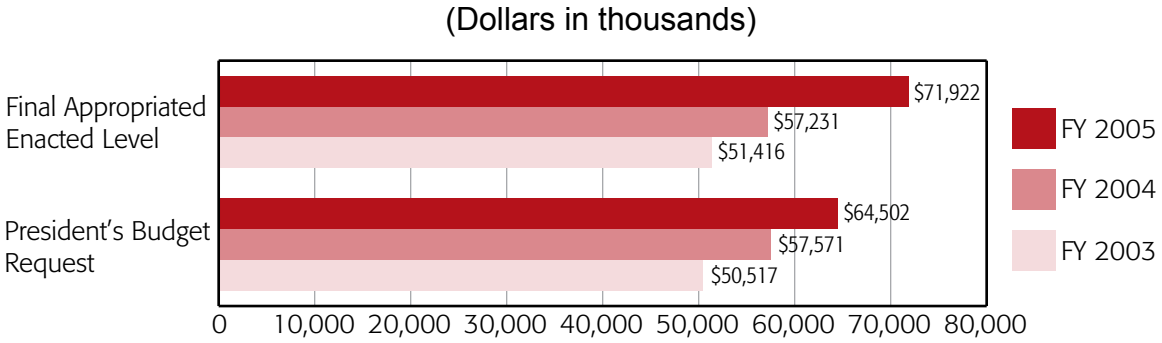
	September 30, 2004	September 30, 2005
Senior Executive Service	4	7
Other Managers	22	20
Nonsupervisory Employees	227	264

Financial Crimes Enforcement Network Diversity Profile, September 30, 2005

	Male	Female	Total
Total employees	42.19%	57.81%	100%
Hispanic/Latino	1.17%	1.95%	3.12%
White	32.81%	37.89%	70.70%
Black/African American	5.47%	14.84%	20.31%
American Indian/Alaska Native	0%	0.78%	0.78%
Asian	2.73%	2.34%	5.07 %
Employees with Disabilities	Not Available	Not Available	6.25%

In Fiscal Year 2005, the appropriated budget for the Financial Crimes Enforcement Network was nearly $72 million. A breakout of obligations appears in Appendix B.

History of President's Budget Requests and Appropriations, Fiscal Years 2003 – 2005



The following Congressional and Senate Committees and Subcommittees have authorizing and appropriations responsibilities for our operations.

U.S. House of Representatives Committees

- Committee on Financial Services, Subcommittee on Oversight and Investigations (Authorizing Committee)
- Committee on Appropriations, Subcommittee on Transportation, Treasury, Housing and Urban Development, the Judiciary, and the District of Columbia (Appropriating Committee)

U.S. Senate Committees

- Committee on Banking, Housing, and Urban Affairs (Authorizing Committee)
- Committee on Appropriations, Subcommittee on Transportation, Treasury, the Judiciary, Housing and Urban Development, and Related Agencies (Appropriating Committee)

The Financial Crimes Enforcement Network works closely with regulatory, law enforcement, private sector, and international partners. Among the entities with which we work especially closely are the Federal supervisory agencies, the Bank Secrecy Act Advisory Group, and the Egmont Group, all described below.

Federal Regulatory Agencies

Responsibility for conducting Bank Secrecy Act compliance examinations has been delegated to the following Federal agencies:

- Federal Deposit Insurance Corporation
- Board of Governors of the Federal Reserve System
- Office of the Comptroller of the Currency (U.S. Department of the Treasury)
- Internal Revenue Service, Small Business/Self-Employed Division (U.S. Department of the Treasury)
- Office of Thrift Supervision (U.S. Department of the Treasury)
- National Credit Union Administration
- Securities and Exchange Commission
- Commodity Futures Trading Commission

The Financial Crimes Enforcement Network provides assistance and support to these agencies to promote effective and uniform application of the Bank Secrecy Act regulations.

Bank Secrecy Act Advisory Group

Congress established the Bank Secrecy Act Advisory Group in 1992 to enable the financial services industry and law enforcement to advise the Secretary of the Treasury on ways to enhance the utility of Bank Secrecy Act records and reports. Since 1994, the Advisory Group has served as a forum for industry, regulators, and law enforcement to communicate about how Suspicious Activity Reports and other Bank Secrecy Act reports are used by law enforcement and how record keeping and reporting requirements can be improved. The Director of the Financial Crimes Enforcement Network chairs the Bank Secrecy Act Advisory Group.

The Bank Secrecy Act Advisory Group, which is not subject to the Federal Advisory Committee Act, meets twice each year in Washington, DC. In light of the expansion of Bank Secrecy Act requirements since the enactment of the USA PATRIOT Act of 2001, the Financial Crimes Enforcement Network has been taking steps to ensure that the Bank Secrecy Act Advisory Group continues to fully and fairly reflect the entire Bank Secrecy Act constituency. The Advisory Group now has 50 members.

The Bank Secrecy Act Advisory Group utilizes a variety of permanent and ad hoc subcommittees to identify and analyze

relevant issues. Current subcommittees focus on: Suspicious Activity Report issues; Bank Secrecy Act examination consistency; wire transfer reporting thresholds; privacy/security issues; non-bank financial institutions issues; securities/futures issues; law enforcement issues; and reducing the filing of Currency Transaction Reports with little or no value to law enforcement. The Bank Secrecy Act Advisory Group also co-chairs publication of ***The SAR Activity Review—Trends, Tips & Issues***, which provides meaningful information to the financial community about the preparation, use, and value of Suspicious Activity Reports.

Need for Government-Private Sector Partnership

"I am convinced that if we are ever going to achieve our goal of truly safeguarding the financial system from criminal abuse under the current paradigm, the government and private sector must act in true partnership. The word 'partnership' gets thrown around an awful lot these days, at least in the United States, and this tends to breed a great deal of cynicism. Partnership demands a commitment on both sides. For the private sector this means a commitment to develop and implement reasonable, risk-based programs to address the risks of financial crime posed by each private sector member's business lines and customer base. This program should result in the reporting of suspicious activity and other relevant information to the government when appropriate. The government, in turn, must educate the private sector about the risk and – most importantly – be willing to share information with the private sector so they can develop their programs to address the risks associated with their business and customers.…

"The 20th Century paradigm of governments alone protecting their citizens from outside threats is no longer valid in a post-September 11 world. This paradigm simply no longer applies when enemies can melt into society and commandeer aircraft to use as missiles of devastation, or when a group of mad men board public transportation and murder innocent souls who are simply trying to live and work in the world. Good partners talk with one another. I am convinced that if we are to make the present regime work, government and the private sector need to be in a constant dialogue on these issues."

—William J. Fox, Cambridge International Symposium on Economic Crime, September 5, 2005

The Egmont Group

The Egmont Group is a global association of 101 financial intelligence units, national centers that have been set up to collect information on suspicious or unusual financial activity from the financial industry, to analyze the data, and to make it available to appropriate national authorities and other financial intelligence units for use in combating terrorist funding and other financial crime. The Group takes its name from the palace in Brussels where 15 financial intelligence units first met in 1995 to establish an informal group for sharing information about money laundering.

The Financial Crimes Enforcement Network has played a major role in helping other countries develop their financial intelligence units, and we help those units strengthen anti-terrorist financing and money laundering policies and programs. We also sponsor new financial intelligence units for membership in the group and provide a secure web system through which Egmont members can exchange information.

Our Deputy Director chairs the Egmont Committee, which coordinates Egmont Group activities. We also provide staff support for Egmont's five working groups, which are described below:

- The Legal Working Group reviews the candidacy of potential members and handles all legal aspects and matters of principle within Egmont, including cooperation between financial intelligence units.
- The Outreach Working Group seeks to create a global network of financial intelligence units by identifying candidates for membership and working with them to ensure that they meet international standards.
- The Training Working Group identifies training opportunities for financial intelligence unit personnel. The Training Working Group has also published a collection of sanitized terrorist and money laundering cases that were

used at the typology exercises of the Financial Action Task Force, an inter-governmental body that develops and promotes national and international policies to combat money laundering and terrorist financing.

- The Operational Working Group seeks to bring financial intelligence units together on cases and strategic projects such as insurance schemes and stored value.
- The IT (Information Technology) Group examines new software applications that might facilitate analytical work and focuses on such issues as data mining, information fusion, and security.

Egmont Group Achievements

"A review of what has happened over the past decade can lead to only one conclusion . . . that the Egmont Group has achieved [its] original goals in spectacular fashion. Right now that original handful of units has expanded to 101 countries and jurisdictions each of which has made a commitment to put the resources in place to accomplish what the FATF envisioned. The fact that 101 countries and jurisdictions have established units is impressive in its own right, but what is even more important is that each FIU has made a commitment to share the information they collect with other FIUs. We all know it works. We see it in action every day."

—William J. Fox, 13th Plenary Session of Egmont Group, June 30, 2005

Publications

The following publications, all produced in Fiscal Year 2005, are available on the Financial Crimes Enforcement Network website, www.fincen.gov:

- *Financial Crimes Enforcement Network Strategic Plan, Fiscal Years 2006-2008*
- *Financial Crimes Enforcement Network Annual Report for Fiscal Year 2004*
- *SAR Activity Review—Trends, Tips and Issues – Issue 8, April 2005*
- *SAR Activity Review—By the Numbers – Issue 3, December 2004*
- *SAR Activity Review—By the Numbers – Issue 4, May 2005*

Earlier issues of the publications above are also available on our website.

The Reference Series: Funds Transfer Manual published in Fiscal Year 2005 is an Official Use Only document available to law enforcement, intelligence, and regulatory agencies. For further information about this manual, e-mail webmaster@fincen.gov, call (703) 905-3591, or write to us:

Financial Crimes Enforcement Network
Post Office Box 39
Vienna, VA 22183-0039

The Financial Crimes Enforcement Network relies on internal and external evaluations to gauge program effectiveness and make improvements as needed. Listed below are key evaluations completed and underway during Fiscal Year 2005.

Program Rating Assessment Tool (PART)

The Program Rating Assessment Tool is a systematic method of assessing the performance of program activities across the Federal Government. It is composed of a series of questions designed to assess program performance related to the Government Performance and Results Act and the goals of the President's Management Agenda. Answers to PART questions must be supported by objective data. The PART is administered by the Office of Management and Budget, which rates the program evaluated as "Effective," "Moderately Effective," "Adequate," or "Results Not Demonstrated."

In Fiscal Year 2005, the Financial Crimes Enforcement Network completed its first PART evaluation, which covered activities related to managing Bank Secrecy Act data. This program received a PART rating of "Moderately Effective."

Government Accountability Office Audits

Completed in FY 2005:

- *Additional Guidance Could Improve Implementation of Regulations Related to Customer Identification and Information Sharing Programs*

Underway in FY 2005:

- *Effectiveness of Bank Secrecy Act Examinations and Enforcement*
- *Joint Review of FinCEN's and IRS' Management of Bank Secrecy Act*
- *FinCEN's Responsibilities Under USA PATRIOT Act Sections 361 and 330*

Treasury Office of Inspector General Audits

Completed in FY 2005:

- *Heightened Management Attention Needed Over Longstanding Suspicious Activity Report (SAR) Data Quality Problems*
- *Additional Outreach and Systems Enhancements Are Needed to Encourage Greater Use of FinCEN's Bank Secrecy Act E-filing*
- *Status Report on the Establishment of the Financial Crimes Enforcement Network's Office of Compliance*
- *Major Challenges Faced by FinCEN in its Program to Register Money Services Businesses*

Underway in FY 2005:

- *Analysis and Dissemination of Bank Secrecy Act and Criminal Data*
- *Treasury's Administration of the Bank Secrecy Act*

Treasury Financial Management Assessment

Using criteria from the Office of Management and Budget, the Treasury Department sets standards for Green, Yellow, and Red performance in financial management and regularly monitors key performance indicators. The table below shows our Fiscal Year 2005 record in meeting the standards for Green performance.

Fiscal Year 2005 Financial Performance

Financial Area	Treasury Standard for "Green"	FinCEN FY 2005 Average	FinCEN Score
% of cash reconciled to total	>99.99%	100%	Green
% of uncleared suspense transactions over 60 days	<10%	0%	Green
% of Accounts Receivable from public delinquent over180 days	<10%	0%	Green
% of electronic vendor payments	96%	100%	Green
% non-credit card invoices paid on time	>98%	99%[1]	Green
% of centrally billed travel cards with balances over 61 days past due	0%	0%	Green
% of individually billed travel cards with balances over 61 days past due	<2%	3%	Yellow
% of purchase cards with balances over 61 days past due	0%	0%	Green

[1]Excludes months affected by the transition from Customs cross servicing to Administrative Resource Center (ARC) cross servicing

Internal Assessments

Completed in FY 2005:

- Self-assessment of our equal employment opportunity policies and practices.
- Legal review of contracting and procurement matters.

Bank Secrecy Act requirements serve to deter financial crimes, to detect them when they occur, and to support attempts to bring the perpetrators to justice. This section provides an overview of major financial crimes and describes ways that Bank Secrecy Act recordkeeping and reporting requirements are helping to detect these activities and the individuals behind them.

Money Laundering

Money laundering is the disguising of funds derived from illicit activity so that they may be used without detection of the illegal activity that produced them. Money laundering may be attempted by individuals, small and large businesses, corrupt officials, and individuals involved in organized crime, such as drug dealers or Mafia members.

Money laundering poses international and national security threats. It can fuel organized crime, corrupt financial systems, undermine free enterprise by crowding out the private sector, and threaten financial stability.

Money laundering involves three stages: placement, layering, and integration.

- ***Placement*** involves physically placing illegally obtained money into the financial system or the retail economy. "Dirty" money is most vulnerable to detection and seizure during placement.
- ***Layering*** means separating the illegally obtained money from its source through a series of financial transactions that make it difficult to trace the origin of the funds.
- ***Integration*** means converting the illicit funds into a seemingly legitimate form. Integration may include the purchase of businesses, automobiles, real estate, and other assets.

Some money laundering placement methods specifically attempt to evade Bank Secrecy Act requirements. These include:

- Structuring – An individual makes two or more cash transactions below the dollar thresholds for Bank Secrecy Act reporting and record keeping thresholds in order to avoid detection.
- Smurfing – Two or more individuals deposit cash or buy bank drafts in amounts under Bank Secrecy Act reporting requirements.

During the layering phase of money laundering, criminals often take advantage of legitimate financial mechanisms in attempts to hide the source of their funds. A few of the many mechanisms that may be misused during layering are currency exchanges, wire transmitting services, prepaid cards that offer global access to cash via automated teller machines and goods at point of sale, internet-based e-value systems, casino services, and

domestic shell corporations lacking real assets and business activity that are set up to hold and move illicit funds.

Money launderers may also attempt to mix "dirty" funds with clean. For example, criminals may take over or invest in businesses that generate large cash proceeds and mix illicit funds with those of the legitimate business. In addition, money launderers may take part in criminal activity specifically designed to hide the proceeds of other criminal acts. For instance, they may set up fraudulent invoicing schemes that over- or undervalue goods being traded.

Suspicious Activity Report Leads to Investigation, Sentencing of Marijuana Grower

A defendant was sentenced to prison, followed by several years' probation, after pleading guilty to narcotics trafficking charges and structuring financial transactions to evade Bank Secrecy Act currency reporting requirements in connection with a marijuana growing operation. The defendant incorporated a business falsely described in corporate documents as a real property development company. The defendant used the business to purchase acreage, set up the marijuana growing operation, and hired people to run it.

According to the plea agreement, the defendant admitted to making over 100 cash deposits to the corporate account over several years. The cash deposits totaled more than $1 million, but each deposit was less than $10,000. This investigation was initiated based on the filing of a Suspicious Activity Report. (Source: Internal Revenue Service-Criminal Investigation)

The SAR Activity Review – Trends, Tips & Issues
Issue 8, April 2005

Terrorist Financing

Terrorists require funds to support their deadly activities and must move those funds to individuals or cells in particular target areas. The amount needed for a particular attack may be relatively small, but larger amounts are needed to recruit, transport, train, house, pay, and equip terrorist agents.

Some terrorist funding comes from illicit activity, including traditional crimes such as kidnapping for ransom, narcotics trafficking, extortion, credit card fraud, counterfeiting, and smuggling. Other funds come from the following sources:

- Supporters – A significant portion of terrorists' funding comes from supporters. Willing donors include wealthy individuals and their families, supportive social and religious organizations, and rogue nations.
- Corruption of charities – Terrorist groups have created charitable fronts and have sought out corrupt or vulnerable non-profits to raise and move money, to transport operatives and materiel, to recruit and indoctrinate new members, and to support family members of operatives or deceased suicide bombers.

Terrorist financiers may use money laundering methods to hide the source, purpose, and movement of their assets. For example, they may use commodities, false invoicing, and other trade manipulation to move funds. Criminal organizations and terrorists sometimes employ the services of the same professionals, including personal services providers such as accountants and lawyers, to help disguise their funds.

Terrorist operatives may attempt to smuggle cash – or precious metals, stones, or jewels – across borders or may use couriers to attempt to transport these items. Likewise, terrorists may rely on currency exchangers to transfer funds, especially in countries where cash is typically used to settle accounts.

Terrorists have used informal value transfer systems, such as those known as "hawala" or "hundi." These systems use trusted networks of people who move funds and settle accounts with little or no documentation. Such systems are prevalent throughout Asia and the Middle East as well as within expatriate communities in other regions. In the United States, money transmitters involved in informal value transfer systems are required, under the Bank Secrecy Act, to register as money services businesses, develop anti-money laundering programs, and report suspicious activity.

Terrorists also use traditional financial institutions and mechanisms to move their funds. The 9/11 Commission found that Al Qaeda funded the hijackers in the United States through wire transfers from overseas,

by physically moving cash and traveler's checks into the country, and by accessing funds held in foreign accounts through debit or credit cards. Suspicious Activity Reports filed under the Bank Secrecy Act are a valuable source of information about potential terrorist financing activity.

Suspicious Activity Report Initiates Material Support of Terrorism Investigation

The Federal Bureau of Investigation initiated a Material Support of Terrorism investigation based on a Suspicious Activity Report filed by a bank detailing a series of overseas financial transactions totaling millions of dollars. Two of the participants in these transactions were a United States-based company and a money services business based in the Middle East. The bank was concerned by the unorthodox manner in which the transactions were executed and the disparate business operations of the participants. All of the money passed through an account held at the United States branch of a foreign bank headquartered in the Middle East.

During a seven-month period, millions of dollars passed through the money services business's bank account, immediately dispersing funds to scores of businesses and individuals around the world. Although the purpose of these payments is still under investigation, some of the recipients are known for, or suspected of, involvement in terrorist activities. (Source: Federal Bureau of Investigation)

The SAR Activity Review – Trends, Tips & Issues
Issue 8, April 2005

Other Financial Crimes

In addition to money laundering and terrorist financing, Bank Secrecy Act reports provide valuable leads and information for law enforcement and intelligence agencies investigating a wide variety of financial crimes. Examples are tax evasion, many types of fraud, embezzlement, counterfeiting, bribery, insider trading, and identity theft. The Financial Crimes Enforcement Network provides authorized law enforcement agencies controlled access to reported Bank Secrecy Act data so that investigators of these crimes can "follow the money." We also identify and refer to appropriate authorities potential evidence of financial crimes, provide analytical support for cases with a significant financial component, and assist in managing cases with a large number of subjects and/or large numbers of relevant Bank Secrecy Act reports.

Business Owner Sentenced for Tax Evasion

A business owner was sentenced to several years in prison followed by three years supervised release and ordered to pay a fine of nearly $1 million. The defendant was convicted of three counts of tax evasion and one count of structuring a financial transaction to avoid federal currency transaction reporting requirements. According to trial evidence, the defendant reported no taxable income and paid no federal income tax during three years, although the two businesses the defendant owned and operated were profitable and the defendant was earning a substantial taxable income from their operations.

The defendant, an accountant by training, engaged in a complicated tax evasion scheme which involved diverting hundreds of thousands of dollars from the businesses into personal investment accounts held in the name of the defendant's spouse. The defendant created a phony shareholder loan account to make it appear that the corporations that owned the businesses owed the defendant money and then took false "bad debt" deductions on the defendant's own tax returns to offset the income earned personal investment accounts belonging to the defendant and the defendant's spouse. This investigation was initiated based on the filing of a Suspicious Activity Report. (Source: Internal Revenue Service-Criminal Investigation)

The SAR Activity Review – Trends, Tips & Issues
Issue 8, April 2005

Financial Crimes Enforcement Network – Direct Obligations

Fiscal Years 2004 and 2005, by Object Classification

(Dollars in thousands)

Object Classification	FY 2004 Actual	FY 2005 Actual
Personnel compensation:		
Permanent positions	20,539	22,793
Positions other than permanent	284	475
Other personnel compensation	526	391
Special personal services payments	—	—
Total personnel compensation	21,349	23,659
Civilian personnel benefits	4,947	6,116
Benefits to former personnel	—	—
Travel and transportation of persons	796	891
Rents, communications and utilities:		
Rental payments to GSA	2,076	1,475
Other rents, communications and utilities	811	944
Printing and reproduction	200	258
Other services	23,891	30,359
Supplies and materials	335	481
Equipment	1,475	11,064
Total obligations	55,880	75,247
Change in unobligated balance from prior year	1,351	(3,325)
Total enacted appropriations and budget estimate	57,231	71,922