FINANCIAL CRIMES ENFORCEMENT NETWORK

Strategic Plan
FY 2006-2008

Safeguarding the
Financial System from the Abuse
of Financial Crime

Message From the Director

> **"Approaches that addressed the needs of the past must give way to policies, processes, and analytical techniques that meet present and future realities."**

As Director of the Financial Crimes Enforcement Network, this nation's financial intelligence unit, I am proud that our skilled professionals are at the forefront of this country's efforts to protect our financial system from abuse by criminals and terrorist financiers. Under authorities granted to us by the Bank Secrecy Act and the USA PATRIOT Act, our role is to prevent and detect terrorist financing, money laundering, and other financial crime.

These are times of rapid change in the financial arena. Internet-based financial activity, changing methodologies for money laundering and terrorist financing, and the sheer number and variety of worldwide financial transactions make tracking illicit financial activity increasingly challenging. In the face of these developments, the Financial Crimes Enforcement Network needs to become more sophisticated, agile, and creative in assessing and responding to financial system risks. Approaches that addressed the needs of the past must give way to policies, processes, and analytical techniques that meet present and future realities.

This Strategic Plan describes how our organization will achieve its mission in the next three years, consistent with the new terrorism and financial intelligence focus of the Department of the Treasury. Our goals are ambitious, and achieving them will take the combined talents of all Financial Crimes Enforcement Network employees—regulatory personnel, analysts, customer liaison staff, managers, administrative support personnel, and technology experts. I look forward to working with the dedicated men and women of the Financial Crimes Enforcement Network as we use this plan to guide our actions and decisions in the years ahead.

William J. Fox, Director
Financial Crimes Enforcement Network
February 2005

Contents

Introduction

The Financial Crimes Enforcement Network is a bureau within the U.S. Department of the Treasury. We serve as this nation's financial intelligence unit and are responsible for managing, analyzing, safeguarding, and appropriately sharing financial transaction information collected under the Bank Secrecy Act and other authorities.

Operational Charter

The Financial Crimes Enforcement Network was created by order of the Secretary of the Treasury on April 25, 1990. Section 361 of the USA PATRIOT Act, October 25, 2001, established the organization as a bureau within the Department of the Treasury and clarified the duties and powers of the Director.

Our responsibilities are keyed to and flow from 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;

- Conduct analysis in support of policy makers; law enforcement, regulatory, and intelligence agencies; and the financial industry;

- Coordinate with and collaborate on anti-terrorism and anti-money laundering initiatives with domestic law enforcement and intelligence agencies, and with our foreign financial intelligence unit counterparts.

Mission Statement

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity.

We achieve this mission by:

- *Administering* the Bank Secrecy Act;
- *Supporting* law enforcement, intelligence, and regulatory agencies through sharing and analysis of financial intelligence;
- *Building* global cooperation with our counterpart financial intelligence units;
- *Networking* people, ideas, and information.

Organizational Vision

We respond with agility and creativity to the challenges posed to the domestic and global financial systems by terrorist financiers and operatives, money launderers, and other perpetrators of financial crime.

Commitment to Excellence

The Financial Crimes Enforcement Network is committed to maintaining the highest standards of excellence, integrity, and mutual respect. We accept the public trust that underlies our role in strengthening national security, and we constantly strive to provide outstanding public service. We are committed to developing and maintaining a diverse, innovative, and expert work force to serve the public and achieve our mission.

For more information about the Financial Crimes Enforcement Network, please visit our website at www.fincen.gov.

Strategic Goal 1:

Protect the financial system through effective administration of the Bank Secrecy Act.

Criminal access to financial services and products, whether to fund terrorist operations or to hide the proceeds of drug trafficking or other crimes, poses a direct threat to both the national security of the United States and the U.S. financial system. The Bank Secrecy Act is one of the nation's most potent weapons for preventing corruption of the financial system. As administrator of the Act, the Financial Crimes Enforcement Network will apply a unique set of authorities, requirements, and tools to assist the regulated industry, regulators, law enforcement, and the intelligence community to meet this challenge. Our aim is to reduce the vulnerability of U.S. depository institutions, money services businesses, broker/dealers in securities, casinos, and other industries to abuse by terrorists and other criminals.

Strategic Objective 1.1: Develop and implement appropriate anti-money laundering regulatory policy and regulations under the Bank Secrecy Act and related authorities.

Strategies:

1.1.1   Protect additional segments of the financial industry through the application of anti-money laundering programs, suspicious activity reporting, and other record keeping requirements as may be appropriate.

1.1.2   Revise data collection forms, regulations, and practices as needed to ensure that we collect the information required to accomplish our mission while minimizing reporting burdens on the financial industry.

1.1.3   Apply regulatory and legal resources in support of Treasury responsibilities under Section 311 of the USA PATRIOT Act.

Strategic Objective 1.2: Provide guidance to support financial institutions in establishing risk-based programs that comply with the Bank Secrecy Act.

Strategies:

1.2.1   Enhance our outreach program to educate regulated industries, especially small money services businesses and others considered most vulnerable to the movement of terrorist funds, about terrorist financing methodologies.

1.2.2 Increase the production of written guidance for the regulated industries concerning Bank Secrecy Act compliance, including staff commentaries and frequently asked questions.

1.2.3 Expand the availability of industry-friendly compliance support processes, including hot lines and web-based information services.

1.2.4 Implement a call center to consolidate and coordinate responses to industry requests for guidance and assistance on compliance with regulatory requirements.

1.2.5 Play a recognized, formal leadership role in international organizations and initiatives designed to combat money laundering and terrorist financing.

Strategic Objective 1.3: Promote uniform and effective application of, examination for, and enforcement of the Bank Secrecy Act.

Strategies:

1.3.1 Enhance support for and oversight of regulators who have been delegated compliance examination responsibilities for both the depository and nondepository financial industries.

1.3.2 Develop information exchange agreements that will increase our ability to identify compliance problems at an earlier stage and reduce the time needed for appropriate remedial action.

1.3.3 Provide additional guidance to regulated industries, regulators, examiners, and law enforcement to improve consistency in the administration and enforcement of the Bank Secrecy Act.

1.3.4 Assist Federal regulators in the development of Bank Secrecy Act examination procedures and best practices.

1.3.5 Where necessary, impose appropriate civil enforcement remedies to ensure compliance.

1.3.6 Develop and operate a system and processes needed to track the level of compliance of examined institutions with the Bank Secrecy Act.

Strategic Objective 1.4: Use regulatory means to support law enforcement in the investigation and prosecution of financial crimes.

Strategies:

1.4.1   Provide law enforcement agencies data on large currency transactions and suspicious financial activity that they judge to be valuable in preventing, detecting, and prosecuting financial crime.

1.4.2   Reduce the number of Currency Transaction Reports filed on legitimate financial transactions that are of little or no value to law enforcement.

1.4.3   Find innovative ways to exchange critical information with the financial industry.

How We Will Measure Success:

Success will be measured by tracking the industries covered by anti-money laundering regulations, the level of stakeholder satisfaction with FinCEN's regulatory guidance, time taken to process compliance matters–including the time taken to conclude enforcement actions–and ability to monitor the level of compliance of examined institutions with the Bank Secrecy Act.

Strategic Goal 2:

Combat terrorism, money laundering, and other financial crime through analysis of Bank Secrecy Act data and other relevant information.

The Financial Crimes Enforcement Network is the largest overt collector of financial intelligence in the United States. The information we collect is highly valuable in combating terrorism and investigating money laundering and other financial crime. We mine data collected under the Bank Secrecy Act as well as law enforcement, commercial, and other intelligence to follow the money trails of terrorists and other criminals and to identify networks of people and accounts engaged in unlawful activity. To enhance the value of our efforts to combat terrorism and money laundering, we seek to broaden the types of data available to our analysts. To make better use of our resources, we also aim to focus the analytic resources of the Financial Crimes Enforcement Network on complex investigative case support and assessments of terrorist financing and money laundering threats.

Strategic Objective 2.1: Expand the production of analytic products that incorporate analysis of relevant classified information.

Strategies:

2.1.1   Build the secure physical, personnel, and information technology infrastructure needed to allow analysts full access to classified data.

2.1.2   Increase the number of our analysts with full access to classified data.

2.1.3   Provide our analysts the knowledge and skills necessary to expertly analyze all-source information.

Strategic Objective 2.2: Produce policy-level assessments of terrorist financing and money laundering threats that fuse Bank Secrecy Act data with all appropriate information sources.

Strategies:

2.2.1   Increase the amount of analytic resources devoted to assessments of terrorist financing and money laundering threats by geographic area, industry, type of criminal activity, and methodology.

2.2.2 Increase the number of analytical exchange programs and collaborative analyses with our foreign counterparts in the Egmont Group of financial intelligence units.

Strategic Objective 2.3: Adjust our support of law enforcement investigations to better reflect our increased capabilities to perform complex data mining and analysis.

Strategies:

2.3.1 Increase the number of analytic products supporting law enforcement investigations that incorporate complex analysis; graphic displays of data relationships; and analytic findings, comments, and recommendations.

2.3.2 Reduce the time spent by our analysts in routine data retrieval and manipulation tasks by enhancing our customers' ability to access Bank Secrecy Act data directly.

2.3.3 Develop better methods and data for assessing complexity of analytical products supporting law enforcement.

2.3.4 Continue to produce reference materials that provide law enforcement and intelligence agencies with a better understanding of financial transactions and mechanisms, such as wire transfer services.

2.3.5 Consistent with the operating procedures of other financial intelligence units, increase the number of reports provided to law enforcement that incorporate information obtained through cooperation with our Egmont partners.

Strategic Objective 2.4: Apply analytical resources to support regulatory activity concerning the Bank Secrecy Act.

Strategies:

2.4.1 Increase the amount of analytical expertise devoted to industry assessments that support effective rule making and other regulatory actions.

2.4.2 Analyze Bank Secrecy Act data to flag compliance problems, including possible willful violations of regulatory requirements and to identify opportunities to strengthen data collection forms or processes.

2.4.3 Analyze Bank Secrecy Act data to identify areas where filers need assistance or education to improve the quality of Bank Secrecy Act reporting.

2.4.4 Increase interactions with and feedback to the financial industry regarding analysis of Bank Secrecy Act data and financial crimes risk factors.

How We Will Measure Success:

Progress will be measured by monitoring types and complexity of analytic products, customer ratings of analytic products, and information sources used to develop analytic products.

Strategic Goal 3:

Intensify international anti-money laundering collaboration through the global network of financial intelligence units.

The Financial Crimes Enforcement Network is the financial intelligence unit of the United States. As such, we are a member of the Egmont Group of financial intelligence units, an international network of nearly 100 national centers set up specifically 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. We will continue to play a leadership role in the Egmont process, using it as a springboard for intensifying international cooperation, collaboration, and information sharing. Our aim is to reduce global vulnerability of both the formal and informal financial sectors to abuse by terrorists and other criminals.

Strategic Objective 3.1: Strengthen anti-terrorist financing and anti-money laundering policies and programs worldwide.

Strategies:

3.1.1   Assist in the development of new financial intelligence units in regions especially critical in the fight against terrorist financing and money laundering, such as the Middle East and Central Asia.

3.1.2   Work on an interagency basis to expand the capacity of key partner to combat money laundering and terrorist financing through cooperative efforts, such as conducting financial sector assessments, and through targeted training and technical assistance programs.

3.1.3   Focus on expanding and enhancing information sharing within the Egmont Group by exploring new technologies to expand members' accessibility to the Egmont secure web and other established secure web systems.

3.1.4   Partner with other financial intelligence units, international organizations and financial institutions to coordinate and fashion efforts to reduce the threat of money laundering and terrorist financing and build the institutional capabilities of other nations to address that threat.

Strategic Objective 3.2: Enhance international standard-setting and cooperation in the areas of money laundering, terrorist financing and other financial crimes.

Strategies:

3.2.1 Exercise leadership within the Egmont Group to promote policies and initiatives that reinforce channels for communicating operational intelligence on behalf of law enforcement and policy makers.

3.2.2 Expand support activities for the Department of the Treasury and other policy-making bodies that set and refine international standards for combating terrorist financing and money laundering.

3.2.3 Play a significant role in international organizations and initiatives designed to combat terrorist financing and money laundering.

3.2.4 Utilize our relationships with other financial intelligence units to improve law enforcement's ability to track terrorism and financial crimes globally.

How We Will Measure Success:

Success will be measured by tracking the amount of assistance and support provided to financial intelligence units, and to countries establishing financial intelligence units.

Strategic Goal 4:

Facilitate regulatory compliance, data management, and information sharing through E-government.

With the continuing threat of terrorist activity world wide, it has become imperative to gather and disseminate accurate financial intelligence as quickly as technology allows. We are moving on several fronts to improve Bank Secrecy Act data collection, management, and sharing. Our aim is to ensure that data collected under the Bank Secrecy Act and related authorities are of high quality, and are made available in database systems and formats appropriate for law enforcement, regulators, and the financial industry as accurately and quickly as possible. We are expanding the use of technology to meet this aim. These electronic methods are expected to improve the quality of the Bank Secrecy Act data by preventing the omission of critical information, by validating the information collected, and by assuring feedback on the use and utility of the data.

Strategic Objective 4.1: Accelerate the secure flow of financial information from the industries subject to Bank Secrecy Act requirements to the law enforcement agencies that use it to prevent, detect, and prosecute financial crime, including terrorist financing; and to the regulators who must assess the adequacy of that information as well as oversee Bank Secrecy Act compliance.

Strategies:

4.1.1   Move aggressively to implement and enhance BSA Direct, a major initiative that will provide secure, user-friendly, web-based tools for accessing, analyzing, and filing Bank Secrecy Act data.

4.1.2   Provide the technology, education, and support needed to accommodate e-filing of 90% of Bank Secrecy Act reports by FY 2009.

4.1.3   Increase the number of law enforcement agencies and regulators accessing Bank Secrecy Act data through our web-based technology.

4.1.4   Maintain strict controls, appropriate training, enhanced outreach and guidance, and a robust audit program to ensure that Bank Secrecy Act data are accessed, disseminated, and used in accordance with applicable legal requirements.

4.1.5   Enhance processes for networking law enforcement and intelligence agencies investigating the same subjects and for getting feedback on the usefulness of networking activity.

Strategic Objective 4.2: Enhance communications between the government and the financial industry to ensure expeditious notification to law enforcement of possible terrorist or other illegal activity.

Strategies:

4.2.1   Improve the information-sharing established between law enforcement and the financial industry under Section 314 (a) of the USA PATRIOT Act.

4.2.2   Seek innovative, faster, and more efficient technical channels for dialog between government and the financial industry.

How We Will Measure Success:

Success will be measured by the increase in users accessing Bank Secrecy Act data though our web-based technology, an increase in the number of BSA forms filed through electronic means, and evaluation of government-industry information exchange programs.

Management Goal:

Develop a more nimble and responsive management structure.

Because of our national and global roles in protecting financial systems from criminal abuse, the Financial Crimes Enforcement Network needs to be ready to respond nimbly to changing national and international conditions related to financial crimes. We also need to meet the changing needs and requirements of the financial industry, and our regulatory, law enforcement, and international partners. At the same time, we must fulfill our legal obligations as a Federal bureau within the Treasury Department. Meeting all these requirements requires a careful blend of innovation, prudence, flexibility, and consistency. Our aim is to ensure that the Financial Crimes Enforcement Network has the human, technology, and data resources needed to respond effectively to legislative and regulatory mandates, as well as to methodological and other changes relating to terrorist financing, money laundering, and other illicit financial activity.

Management Objective 1.1: Attract, develop, and retain a high-performing, diverse workforce.

Strategies:

1.1.1   Offer structures and incentives, including defined paths for career progression, to enhance employee recruitment and retention.

1.1.2   Provide employees with cross training that prepares them to respond flexibly to changing needs.

1.1.3   Establish stronger lateral communications across organizational functions and programs.

1.1.4   Establish a performance management system that fairly and objectively measures employee performance and rewards excellent performance.

Management Objective 1.2: Satisfy internal and external customers, and meet stakeholder requirements for excellent government performance.

Strategies:

1.2.1   Keep abreast of customer needs through close liaison and by soliciting and acting on feedback.

1.2.2   Streamline organizational structures and processes.

1.2.3   Enhance our systems for managing tasks and projects.

1.2.4   Promptly address and attempt to eliminate any shortcomings identified via internal or external evaluations or audits.

1.2.5   Develop enhanced methods and data for evaluating success of our programs.

Management Objective 1.3: Strengthen our organizational infrastructure.

Strategies:

1.3.1   Continue to move from a "Public Trust" to a "National Security" security posture by upgrading background investigation and clearance requirements for employees.

1.3.2   Increase the reliability, performance, and security of our technology infrastructure.

How We Will Measure Success:

Success will be measured by employee and customer satisfaction ratings and monitoring of internal performance.

APPENDIX A:

How the Financial Crimes Enforcement Network Supports
the Department of the Treasury*

TREASURY STRATEGIC GOAL: F3: Preserve Integrity of Financial Systems
TREASURY STRATEGIC OBJECTIVE: Disrupt and dismantle financial infrastructure of terrorists, drug traffickers, and other criminals and isolate their support networks
OFFICE OF TERRORISM AND FINANCIAL INTELLIGENCE MISSION: Safeguard the U.S. and international financial systems from abuse by terrorist financing, money laundering, and other financial crime, and to sever the lines of financial support to international terrorists

FINANCIAL CRIMES ENFORCEMENT NETWORK

STRATEGIC GOALS:

1. Protect the financial system through effective administration of the Bank Secrecy Act

2. Combat terrorism, money laundering, and other financial crime through analysis of Bank Secrecy Act data and other relevant information

3. Improve international anti-money laundering collaboration through the global network of financial intelligence units

4. Facilitate regulatory compliance, data management, and information sharing through E-government

MANAGEMENT GOAL:

Develop a more nimble and responsive management structure

*Treasury Strategic Goals and Objectives appear in the Treasury Strategic Plan at http://www.treas.gov/offices/management/budget/planningdocs/treasury-strategic-plan.pdf

APPENDIX B:

STRATEGIC CHALLENGES

Following are external or internal challenges to each of our strategic goals. In managing its programs, the Financial Crimes Enforcement Network considers ways to offset and alleviate these challenges.

Challenges to Strategic Goal 1: Protect the financial system through effective administration of the Bank Secrecy Act

The central role of the Financial Crimes Enforcement Network is to administer the Bank Secrecy Act. That Act is unique in that its implementation involves multiple government agencies and, perhaps more than any other regulatory regime, requires a vibrant partnership with the regulated industry.

For example, the Financial Crimes Enforcement Network is accountable for ensuring compliance with the Bank Secrecy Act, but does not itself directly examine financial institutions for compliance with that law. Instead, we have delegated examination responsibility to eight different federal regulators that are responsible for examining specific industry sectors. Moreover, although they have no delegated authority, a variety of self-regulatory organizations and state regulatory authorities also conduct extensive Bank Secrecy Act examination activities. Although this unusual structure has the benefit of building on the expertise and resources of the regulators that know their industries best, it is a major challenge because of the inherent risk of fragmentation, lack of uniformity, and potential lack of accountability. These challenges have required us to reevaluate our role and lay the framework for strengthening our support of the examination process. This will require extensive coordination, leadership, tact, and resources.

Challenges to Strategic Goal 2: Combat terrorism, money laundering and other financial crime through analysis of Bank Secrecy Act data and other relevant information

Like the rest of America, the Financial Crimes Enforcement Network is still adapting to changes triggered by the events of 9/11. These changes include incorporating the responsibilities assigned to us in the USA PATRIOT Act and supporting the Department of the Treasury's new focus on detecting and preventing terrorist financing.

These shifts challenge us to make the best use of our analytical resources in the context of today's war on global terrorism while continuing to meet our traditional efforts to detect and halt money laundering and other financial crimes. Money laundering is the effort to take cash derived from an illicit activity, often in large sums, and "clean" it through a series of financial transactions that disguise its origins and make it appear to be a legitimate part of the financial system. Illicit financing, including funding of terrorist activity, often involves the movement of "clean" money to support criminal purposes.

These two types of financial crime require different analytical approaches. With money laundering, analysts must look through a telescope to identify the movement of large amounts of cash. With terrorist financing, analysts often need a microscope to identify the movement of small amounts of cash destined for evil purposes. While the Financial Crimes Enforcement Network has historically developed the information, analytical processes, and tools required to detect money laundering, we need to develop additional tools– and to gain access to additional data, including classified data–in order to better detect terrorist financing.

Related challenges are assuring that our analysts have the knowledge, skills, resources, direction, and support needed for sophisticated, all-source analysis; assuring that we have in place the secure physical and technological environment and the strong internal processes required to protect sensitive and classified data; and effectively recruiting, hiring, training, retaining, and rewarding analytical staff.

A strategic challenge is to make the transition away from relatively simple query services that we have historically provided to law enforcement agencies, so that we can redirect our efforts toward more complex analysis and investigative support. To assure that the needs of our law enforcement customers continue to be met, we are committed to providing them with easy, well-monitored access to the Bank Secrecy Act data and effective analytical tools so that they can more efficiently perform straightforward queries and enhance their internal capabilities for analysis. As a result, additional analytical resources at the Financial Crimes Enforcement Network will be available to provide more comprehensive and sophisticated support for law enforcement customers confronting major and complex cases.

Challenges to Strategic Goal 3: Improve international anti-money laundering collaboration through the global network of Financial Intelligence Units

These are times of rapid change in the global financial arena. Internet-based financial activity, changing methodologies for money laundering and terrorist financing, and the number and variety of worldwide financial transactions make tracking illicit financial activity increasingly challenging. Fortunately, our counterparts in the Egmont Group of financial intelligence units are working cooperatively to address these issues. Our challenge is to effectively use our resources to support and encourage this collaboration.

Challenges to Strategic Goal 4: Facilitate regulatory compliance, data management, and information sharing through E-government

The Financial Crimes Enforcement Network is responsible for managing the Bank Secrecy Act data filed by the regulated industries. Yet, we do not directly collect, process, store, or disseminate filed data. The Internal Revenue Service performs these functions for us under a longstanding partnership arrangement. A consequence of this activity is that we lack oversight authority over the policies and resources devoted to Bank Secrecy Act activity.

Working within these existing parameters, as well as changing those that can and should be altered, is a major, ongoing challenge. Our aim is to increase both our management of and our operational role in collecting, processing, storing, and disseminating the data. Our BSA Direct initiative is the first step toward this vision, which will challenge us to perfect a new array of skills, to upgrade our informational technology management capabilities, and to acquire and steward a significant increase in resources.

The rapid and unrelenting pace of technological change further challenges us to stay abreast of technological developments, and to have access to personnel skilled in advanced technologies, in order to effectively reach our E-government goals.

Challenges to Management Goal: Develop a more nimble and responsive management structure

Like all public service organizations within the Executive branch of the Federal government, the Financial Crimes Enforcement Network faces the common challenge of the unknown: economic changes, political shifts, new developments in the war on terror, new legislative or Executive mandates, and other unforeseen events can affect our activity. We also need to meet the changing needs and requirements of the financial industry, and of our regulatory, law enforcement, and international partners.

To prepare for these challenges, the Financial Crimes Enforcement Network aims to develop a future-oriented management structure and cross-trained professional workforce ready to respond quickly to changing national and international conditions related to financial crimes. We also need to be prepared to meet the operational challenges inherent in our mission. For example, we must safeguard the confidentiality of the financial data that we collect while maintaining the level of transparency appropriate for sound government.

In Fiscal Year 2004, the Financial Crimes Enforcement Network began a major organizational realignment to accommodate the conditions described above. This strategic plan reflects those shifts. As a result, we are now challenged to meet the demands of internal as well as external change.

We foresee ongoing efforts to enhance communication throughout the organization; to assure that employee reactions to and concerns about organizational changes are addressed fairly; and to pay close attention to performance results so that we can quickly correct missteps or unintended adverse consequences. In facing all these challenges, we are also committed to meeting legal and stakeholder requirements for excellent government performance.

APPENDIX C:

PROGRAM EVALUATIONS

The Financial Crimes Enforcement Network maintains a robust evaluation program consisting of both internal and external reviews. Its components include:

- Internal work process reviews that are used as a basis for improving programs and processes.

- Internal control reviews used to evaluate and, if needed, to strengthen management controls over resources.

- Internal reviews of technology, case management and other issues that are used as a basis for making strategic decisions.

- Customer satisfaction surveys, which are used to identify strengths and opportunities to improve services to external clients, including law enforcement agencies, regulators, and the financial industry.

- Employee satisfaction surveys, which are used as a basis for making decisions related to human resources activity, employee communications, and other management areas.

- External evaluations of major program activities, which are contracted for as needed and used in strategic planning.

In addition, the Financial Crimes Enforcement Network will conduct a Performance Assessment Rating Tool (PART) evaluation in conjunction with its FY 2007 budget activity.

APPENDIX D:

ABOUT THIS STRATEGIC PLAN

This plan is an interim adjustment to the plan developed as part of the Department of the Treasury's FY 2003 formal strategic planning process under the Government Performance and Results Act. This adjustment reflects the need for the Financial Crimes Enforcement Network to more clearly articulate its role as a regulatory agency and to set goals for better using its analytical resources for more complex financial and classified data analysis. These needs arose, in part, from the Fiscal Year 2004 assignment of the Financial Crimes Enforcement Network to the Department of the Treasury's new Office of Terrorist Financing and Intelligence, and the realignment of the Financial Crimes Enforcement Network organizational structure.

The plan was developed through a series of senior management meetings, senior management reviews, and employee reviews. It has been reviewed for policy and conformance with requirements set by the Office of Management and Budget by officials at the Department of the Treasury.

Please send any comments or questions concerning the plan to:

Strategic Planning Office
Office of the Director
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, Virginia 22183

Comments may also be e-mailed to webmaster@fincen.gov.

For more information about the Financial Crimes Enforcement Network, please visit our website at www.fincen.gov.