

May 2006

INTERNATIONAL FINANCIAL CRIME

Treasury's Roles and Responsibilities Relating to Selected Provisions of the USA PATRIOT Act



GAO
Accountability · Integrity · Reliability

Highlights

Highlights of [GAO-06-483](#), a report to the Chairman, Committee on the Judiciary, House of Representatives

Why GAO Did This Study

Money laundering and terrorist financing can severely affect the nation's economy and also result in loss of lives. To combat these transnational crimes, the Treasury Department (Treasury) and its component bureau, the Financial Crimes Enforcement Network (FinCEN), have key roles. Section 330 of the USA PATRIOT Act encourages the federal government to engage foreign jurisdictions in negotiations to ensure that foreign banks and financial institutions maintain adequate records to combat international financial crime. Treasury plays a lead role in facilitating such efforts. In accordance with its various responsibilities codified by section 361, FinCEN is to coordinate with its foreign counterparts—financial intelligence units (FIU). This report describes (1) Treasury's approach for negotiating with foreign jurisdictions, (2) how FinCEN has contributed to establishing FIUs in foreign countries and enhancing the capabilities of these units, and (3) what actions FinCEN is taking to maximize its performance as a global partner.

What GAO Recommends

GAO recommends that the Director of FinCEN take appropriate steps to ensure that future customer satisfaction surveys include more comprehensive coverage of and higher response rates from FIUs. Treasury agreed.

www.gao.gov/cgi-bin/getrpt?GAO-06-483.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Rich Stana at (202) 512-8777 or stanar@gao.gov.

INTERNATIONAL FINANCIAL CRIME

Treasury's Roles and Responsibilities Relating to Selected Provisions of the USA PATRIOT Act

What GAO Found

With Treasury's leadership, the U.S. interagency community has been acting to accomplish the goals articulated in section 330 of the USA PATRIOT Act. In particular, according to Treasury, negotiations with foreign jurisdictions are being accomplished through U.S. interactions with the Financial Action Task Force on Money Laundering (FATF), an intergovernmental entity that has developed international standards for combating money laundering and terrorist financing. Treasury emphasized that enactment of section 330 provided a welcomed congressional endorsement of long-standing U.S. policy to combat international financial crime by negotiating with foreign jurisdictions through multilateral organizations, such as FATF.

Since its formation in 1995, FinCEN has helped foreign jurisdictions establish new FIUs and improve the capabilities of existing units. The number of FIUs has jumped from 14 in 1995 to 101 currently, partly because of training and technical support provided by FinCEN and Treasury's Office of Technical Assistance and funding provided by the Department of State. Given the growth in the number of FIUs, future efforts likely will involve giving more attention to improving the capabilities of existing units, especially in reference to combating terrorist financing—an operational task now included in the formal definition of an FIU.

To maximize performance as a global partner, FinCEN is taking various actions, such as assigning an analyst to the Federal Bureau of Investigation's Terrorist Financing Operations Section. Also, FinCEN is modernizing the Egmont Secure Web, which is used by FIUs worldwide to exchange sensitive case information. To enhance its responsiveness to FIUs that request case assistance, FinCEN is allocating additional staff to its Office of Global Support and also is developing a new case management system. However, in the most recent customer satisfaction survey, FinCEN invited less than one-half of FIUs to participate and received only two responses. Future surveys would need to be more inclusive and incorporate better survey development and administration practices, such as follow-up efforts to achieve higher response rates, if the surveys are to serve as a useful management information tool for monitoring and enhancing performance.

Meeting of FIU Representatives in Washington, D.C. (June 30 to July 1, 2005)



Source: Financial Crimes Enforcement Network (FinCEN).

Contents

Letter		1
	Results in Brief	3
	Background	5
	Treasury Department Has a Key Role in Promoting International Cooperation to Combat Money Laundering and Terrorist Financing	7
	Enhancing the Capabilities of Financial Intelligence Units Is a Continuing Challenge	12
	FinCEN Is Taking Various Actions to Maximize Its Performance as a Global Partner, but More Comprehensive Feedback from Financial Intelligence Units Would Be Useful	23
	Conclusions	33
	Recommendation for Executive Action	34
	Agency Comments and Our Evaluation	34
Appendix I	Objectives, Scope, and Methodology	36
	Objectives	36
	Scope and Methodology	37
	Data Reliability	41
Appendix II	Financial Action Task Force and Related Regional Bodies	42
	The Financial Action Task Force and Related Regional Bodies Encompass Member Jurisdictions around the Globe	42
	FATF Recommendations Provide a Set of Countermeasures against Money Laundering and Terrorist Financing	44
	A Widely Adopted Methodology Is Used for Monitoring Compliance with Financial Action Task Force Recommendations	51
Appendix III	The Egmont Group of Financial Intelligence Units	53
	The Egmont Group of Financial Intelligence Units Has Grown Significantly since 1995	53
	The Egmont Group Provides a Network for Exchanging Information	54

Tables

Table 1: Main Weaknesses Identified in Assessments of Compliance with FATF Recommendations for Combating Money Laundering and Terrorist Financing	19
Table 2: Financial Intelligence Units Connected to Egmont Secure Web and Number of User Accounts per Country (as of February 2006)	27
Table 3: Case-Management Statistics—Foreign FIU and FinCEN Requests for Assistance	29
Table 4: Number and Names of Foreign Customer Entities That Requested Assistance from FinCEN in Fiscal Year 2005 (as of July 25, 2005)	31
Table 5: Establishment Dates and Membership of FATF and FATF-style Regional Bodies	43
Table 6: FATF Recommendations on Money Laundering and Terrorist Financing	45
Table 3: Essential Criteria Used in the Methodology for Monitoring Implementation of FATF Recommendation 26	52
Table 8: Egmont Group Membership by Year and Jurisdiction	54

Figure

Figure 1: Annual Growth in the Number of Financial Intelligence Units	13
---	----

Abbreviations

BSA	Bank Secrecy Act
FATF	Financial Action Task Force on Money Laundering
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FIU	financial intelligence unit
IDW	Investigative Data Warehouse
IMF	International Monetary Fund
SAR	suspicious activity report
USA PATRIOT (Act)	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Act)

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

May 12, 2006

The Honorable Jim Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

Money laundering and terrorist financing are transnational crimes that can have devastating effects, involving severe economic consequences as well as loss of lives. The combating of these crimes demands not only effective U.S. interagency efforts but also concerted international cooperation. Key roles are played by the Department of the Treasury (Treasury) and one of its components, the Financial Crimes Enforcement Network (FinCEN).¹ Section 330 of the USA PATRIOT Act² expresses the sense of the Congress that the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury to enter into negotiations with foreign jurisdictions to ensure that foreign banks and other financial institutions maintain records of transactions and account information relating to terrorist organizations or their members and to ensure that such records are made available to U.S. law enforcement and domestic financial institutions when appropriate. State Department, Justice Department, and Federal Reserve Board officials told us that the Treasury Department plays a lead role in addressing the efforts encouraged by section 330. According to Treasury Department officials, the U.S. interagency community has been acting to accomplish the goals articulated in section 330 through ongoing efforts to combat international financial crime. Section 361 of the USA PATRIOT Act³ established FinCEN as a statutory bureau in the Treasury Department and listed its various duties and powers, which include coordinating with its foreign

¹Among other functions, FinCEN is responsible for administering the Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1115 (1970) (codified as amended at 12 U.S.C. §§ 1951 *et seq.*), which is a record-keeping and reporting law designed to prevent financial institutions from being used as intermediaries for the transfer or deposit of money derived from criminal activity. See also 31 U.S.C. § 5301 *et seq.*

²Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 330, 115 Stat. 272, 320.

³Codified as amended at 31 U.S.C. § 310.

counterparts—that is, financial intelligence units (FIUs) in other countries. These units are specialized governmental agencies created to combat money laundering, terrorist financing, and other financial crimes. Each FIU is the respective nation’s central agency responsible for obtaining information (e.g., suspicious transaction reports) from financial institutions, processing or analyzing the information, and then disseminating it to appropriate authorities.

This report addresses the following questions regarding efforts under sections 330 and 361 of the USA PATRIOT Act to combat money laundering and terrorist financing:

- Under section 330, how has the Department of the Treasury interacted or negotiated with foreign jurisdictions to promote cooperative efforts to combat money laundering and terrorist financing?
- Under section 361, how has FinCEN contributed to establishing FIUs in foreign countries and enhancing the capabilities of these units to combat money laundering and terrorist financing?
- What actions is FinCEN taking to maximize its performance as a global partner in combating money laundering and terrorist financing?

To address these questions, we interviewed responsible officials at and analyzed relevant documentation obtained from the Departments of Justice, State, and the Treasury and applicable components. Also, in further reference to promoting international cooperation, we focused on obtaining information about Treasury’s role and activities regarding multilateral organizations—particularly the Financial Action Task Force on Money Laundering (FATF), an intergovernmental entity that has developed international standards for combating money laundering and terrorist financing, and the various FATF-style regional bodies that implement the standards.⁴ We obtained information about FinCEN’s participation in the Egmont Group, the association of FIUs worldwide, whose purpose is to facilitate transnational cooperation and information sharing to combat money laundering and terrorist financing. Regarding statistical information that we obtained from FinCEN—such as the number of requests for assistance submitted by foreign FIUs to FinCEN—

⁴FATF-style regional bodies represent nations in seven geographic areas, respectively, Asia/Pacific, Caribbean, Europe, Eurasia, South America, Eastern and Southern Africa, and Middle East and North Africa.

we discussed the sources of the data with FinCEN officials and worked with them to resolve any discrepancies. We determined that these data were sufficiently reliable for the purposes of this review. We conducted our work from May 2005 through March 2006 in accordance with generally accepted government auditing standards. Appendix I presents more details about our objectives, scope, and methodology.

Results in Brief

According to Treasury Department officials, the U.S. interagency community has been seeking to accomplish the goals articulated in section 330 through ongoing efforts to combat international financial crime by actively engaging and negotiating with foreign jurisdictions through the medium of FATF, the related FATF-style regional bodies, the International Monetary Fund, and the World Bank. Treasury officials also commented that enactment of section 330 represents a welcomed congressional endorsement of long-standing U.S. government policy to work with these entities to develop a global system to ensure that all countries adopt and are assessed against international standards for protecting financial systems and jurisdictions from money laundering and terrorist financing. Further, as an incentive or pressure mechanism that can be used in conjunction with foreign negotiations, Treasury considers section 311 of the USA PATRIOT Act to be particularly relevant.⁵ For example, section 311 authorizes the Secretary of the Treasury (following appropriate interagency consultation and consideration of multiple factors) to designate a foreign jurisdiction or an institution as being of “primary money laundering concern”—which, in turn, could result in the Secretary of the Treasury taking one or more special measures, such as prohibiting or imposing conditions upon the opening of correspondent accounts with the designated entity. Since the USA PATRIOT Act was signed into law in October 2001, three foreign jurisdictions (Burma, Nauru, and Ukraine) and certain financial institutions in Belarus, Latvia, the Macau Special Administrative Region (China), Syria, and the “Turkish Republic of Northern Cyprus”⁶ have been designated primary money laundering concerns. Special measures have not been imposed in most of these cases, but the prospect of imposing them has led to some corrective actions.

⁵Codified as amended at 31 U.S.C. § 5318A.

⁶The quotes indicate that the U.S. government has not officially recognized the “Turkish Republic of Northern Cyprus.”

As a member of the Egmont Group since 1995, FinCEN has focused its global efforts particularly on assisting jurisdictions to establish new FIUs and improving the capabilities of existing units. Over the past decade, the number of FIUs recognized by the Egmont Group has increased more than sevenfold, from 14 in 1995 to 101 as of July 2005, partly because of federal interagency efforts, including training and technical support provided by FinCEN and Treasury's Office of Technical Assistance as well as funding provided by the Department of State.⁷ According to FinCEN, given the dynamic growth in the number of FIUs, future efforts will involve giving more attention to improving the capabilities of existing units, especially in reference to combating terrorist financing—an operational task now included in the Egmont Group's definition of an FIU. During our review, State Department officials noted one area where they would like to augment U.S. assistance to nascent FIUs; that is, ensuring the nascent FIUs have appropriate information technology (hardware and software) because such technology is essential to appropriately functioning FIUs. The State Department and FinCEN are engaged in ongoing discussions on how to augment such assistance.

To maximize its performance as a global partner in combating money laundering and terrorist financing, FinCEN is undertaking various actions. Following passage of the USA PATRIOT Act, FinCEN's most important operational priority has been to provide counterterrorism support to the law enforcement and intelligence community. In this regard, FinCEN in January 2006 assigned an analyst to the Federal Bureau of Investigation's (FBI) Terrorist Financing Operations Section. Also, FinCEN currently is modernizing the Egmont Secure Web—an Internet-based system used primarily for its encrypted e-mail capability to exchange sensitive case information. Most (96) of the Egmont Group's 101 members are connected to the Egmont Secure Web, which is operated and maintained by FinCEN, and the system is considered to be of paramount importance to the operations of FIUs. By operating and improving the Egmont Secure Web, FinCEN plays a key role in fostering the exchange of information among FIUs. Further, to enhance its own responsiveness to information requests submitted by foreign FIUs, FinCEN is allocating additional staff resources to its Office of Global Support, which is responsible for processing requests from foreign FIUs, and FinCEN is developing a new case

⁷The most recent Egmont Group plenary meeting was held June 30 to July 1, 2005, in Washington, D.C. At the plenary meeting, the Egmont Group recognized 7 new members to its global network of FIUs, bringing the total membership to 101.

management system, which is targeted for completion in fiscal year 2008. FinCEN periodically surveys its customers to help assess its responsiveness to domestic and international requests for assistance. However, FinCEN's most recent customer satisfaction survey of external clients had limited coverage of FIUs; less than half of all Egmont Group members were invited to participate, and only two provided responses. This report recommends that the Director of FinCEN take appropriate steps to help ensure that future surveys of FIUs are sufficiently inclusive and responsive to achieve the intended purpose of providing performance-based information as a basis for evaluating services, including the identification of areas warranting improvement. The Department of the Treasury agreed with our recommendation.

Background

In an international context, the Treasury Department is the United States' counterpart to other nations' ministries of finance. The department's responsibilities, among other things, include safeguarding the U.S. financial system from abuse by money launderers, terrorists, and other criminals. Over the years, in carrying out this responsibility, the department has established relationships with finance ministries, central banks, and other financial institutions in nations around the world as well as with multilateral organizations such as FATF, the FATF-style regional bodies, the International Monetary Fund (IMF), and the World Bank.

FATF is an intergovernmental entity whose purpose is to establish international standards and to develop and promote policies for combating money laundering and terrorist financing. At its formation in 1989 by the United States and other industrialized nations, FATF's original focus was to establish anti-money-laundering standards and monitor the progress of nations in meeting the standards. In 1990, FATF issued its "Forty Recommendations on Money Laundering" to promote the adoption and implementation of anti-money-laundering measures. For instance, the recommendations encouraged nations to enact legislation criminalizing money laundering and requiring financial institutions to report suspicious transactions. Following the events of September 11, 2001, FATF expanded its role to combat terrorist financing. Specifically, in October 2001, FATF adopted "Eight Special Recommendations on Terrorist Financing." Among other actions, these recommendations committed members to criminalize the financing of terrorism and to freeze and confiscate terrorist assets. In October 2004, FATF published a ninth special recommendation on terrorist financing to target cross-border movements of currency and monetary instruments ("cash couriers").

Collectively, FATF's "40 plus 9" recommendations are widely recognized as the international standards for combating money laundering and terrorist financing (see app. II). In monitoring nations' progress in implementing the recommendations, FATF collaborates with other multilateral organizations, particularly the FATF-style regional bodies that represent nations in seven geographic areas. These regional groups are to help nations in the region to implement the international standards developed by FATF. Also, these standards have been recognized and endorsed by the World Bank and IMF for use in conducting evaluations and assessments of nations' progress in implementing measures to counter money laundering and terrorist financing. To be compliant with FATF recommendations, a nation must, among other measures, establish an effective FIU.

The United States' FIU is FinCEN, which was administratively established in 1990 as a Treasury Department component. FinCEN was 1 of the 14 charter members of the Egmont Group, which was formed in 1995 to enhance information sharing among FIUs (see app. III). In 2001, section 361 of the USA PATRIOT Act established FinCEN as a statutory bureau in the Treasury Department. Organizationally, FinCEN is part of Treasury's Office of Terrorism and Financial Intelligence, which is the department's policy and enforcement entity regarding terrorist financing, money laundering, financial crime, and sanctions issues. Treasury's budget request for fiscal year 2007 included \$91.3 million (and 352 full-time-equivalent personnel) to support FinCEN's mission of safeguarding the financial system from abuses of money laundering, terrorist financing, and other financial crime. FinCEN carries out this broad mission by, among other means, administering the Bank Secrecy Act (BSA)⁸ and networking with domestic regulatory, law enforcement, and intelligence agencies as well as with foreign counterparts.

⁸Pub. L. 91-508, 84 Stat. 1115 (1970).

Treasury Department Has a Key Role in Promoting International Cooperation to Combat Money Laundering and Terrorist Financing

Section 330 of the USA PATRIOT Act expresses the sense of the Congress that the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury to enter into negotiations with foreign jurisdictions to facilitate cooperative efforts to combat money laundering and terrorist financing. State Department, Justice Department, and Federal Reserve Board officials told us that the Treasury Department plays a lead role in addressing these efforts. According to Treasury Department officials, the U.S. interagency community has been acting to accomplish the goals articulated in section 330 through its interactions with FATF and the FATF-style regional bodies to ensure global compliance with international standards for combating money laundering and terrorist financing. Treasury officials also told us that enactment of section 330 provided a welcomed congressional endorsement of long-standing U.S. government policy to actively engage and negotiate with foreign jurisdictions through the medium of FATF and the related FATF-style regional bodies. Further, in conjunction with foreign negotiations, Treasury considers another provision of the USA PATRIOT Act—section 311—to be a useful mechanism for helping to promote compliance with standards.

The Congress Has Encouraged International Cooperative Efforts

Through section 330 of the USA PATRIOT Act, Congress has encouraged the United States to engage in international cooperative efforts to combat money laundering and terrorism. Specifically, section 330 specifies, “It is the sense of the Congress that the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury, as appropriate, and in consultation with the Board of Governors of the Federal Reserve, to seek to enter into negotiations with the appropriate financial supervisory agencies and other officials of any foreign country the financial institutions of which do business with United States financial institutions or which may be utilized by any foreign terrorist organization (as designated under section 219 of the Immigration and Nationality Act), any person who is a member or representative of any such organization, or any person engaged in money laundering or financial or other crimes.” In carrying out such negotiations, section 330 further specifies the sense of the Congress that

“the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury, as appropriate, to seek to enter into and further cooperative efforts, voluntary exchanges, the use of letters rogatory,⁹ mutual legal assistance treaties, and international agreements to (1) ensure that foreign banks and other financial institutions maintain adequate records of transaction and account information relating to any foreign terrorist organization (as designated under section 219 of the Immigration and Nationality Act), any person who is a member or representative of any such organization, or any person engaged in money laundering or financial or other crimes; and (2) establish a mechanism whereby such records may be made available to United States law enforcement officials and domestic financial institution supervisors, when appropriate.”

Section 330 does not constitute an express mandate—that is, section 330 does not impose an affirmative obligation on any agency or official to enter into negotiations. Nonetheless, the language of section 330 does suggest that efforts should be undertaken to engage in appropriate negotiations.

Treasury and the Interagency Community Engage in Multilateral Efforts to Promote International Cooperation

State Department, Justice Department, and Federal Reserve Board officials told us that the lead role regarding the efforts encouraged by section 330 of the USA PATRIOT Act is held by the Treasury Department. According to the Treasury Department, the U.S. interagency community is fulfilling section 330 by actively engaging and negotiating with foreign jurisdictions through the medium of FATF and the related FATF-style regional bodies. The U.S. delegation to FATF, which is headed by the Deputy Assistant Secretary of the Treasury’s Office of Terrorist Finance and Financial Crime, includes representatives of the Departments of Homeland Security, Justice, and State; the federal financial regulators; and the National Security Council.

Regarding efforts encouraged by section 330, Treasury’s Office of Terrorist Finance and Financial Crime said that the United States—working through FATF, the FATF-style regional bodies, the International Monetary Fund, and the World Bank—has led efforts to develop a global system to ensure that all countries adopt and are assessed against international standards for protecting financial systems and jurisdictions from money laundering and terrorist financing. As mentioned previously, these international

⁹In this context, a letter rogatory is a method of obtaining assistance from abroad in the absence of a treaty or executive agreement. Essentially, this device is a formal request from a court in one country to a court in another country to seek international judicial assistance in obtaining testimony or other evidence.

standards consist of the FATF “Forty Recommendations on Money Laundering” and “Nine Special Recommendations on Terrorist Financing” (see app. II).

Treasury testimony at a congressional hearing in July 2005 before the Senate Committee on Banking, Housing, and Urban Affairs also cited the benefits of international standard-setting bodies. Regarding U.S. efforts and participation in these bodies, the Treasury Under Secretary’s prepared statement included the following points:¹⁰

- “The Financial Action Task Force (FATF) sets the global standards for anti-money laundering and counter terrorist financing, and it is also through this venue that we promote results. Treasury, along with our counterparts at State, Justice, and Homeland Security, has taken an active role in this 33-member body which articulates international standards in the form of recommendations, guidelines, and best practices to aid countries in developing their own specific anti-money laundering and counter-terrorist financing laws and regulations. ... The success and force of FATF lie not only in the mutual evaluation process to which it holds its own members, but also in the emergence of FATF-style regional bodies ... that agree to adopt FATF standards and model themselves accordingly on a regional level.”
- “Hawala, a relationship-based system of money remittances, plays a prominent role in the financial systems of the Middle East. ... Internationally, Treasury leadership in the FATF has brought the issue of hawala to the forefront, resulting in implementation of FATF Special Recommendation VI, which requires all FATF countries to ensure that individuals and entities providing money transmission services must be licensed and registered, and subjected to the international standards set out by FATF.”
- “As governments apply stricter oversight and controls to banks, wire transmitters, and other traditional methods of moving money, we are witnessing terrorists and criminals resorting to bulk cash smuggling. FATF Special Recommendation IX was issued in late 2004 to address this problem and it calls upon countries to monitor cross-border transportation of currency and to make sanctions available against

¹⁰Testimony of Stuart Levey, Under Secretary, Office of Terrorism and Financial Intelligence, Department of the Treasury, at a hearing (“Money Laundering and Terror Financing Issues in the Middle East”), before the Senate Committee on Banking, Housing, and Urban Affairs, July 13, 2005.

those who make false declarations or disclosures in this regard. This recommendation has already prompted changes in legislation abroad.”

Further, on July 29, 2005, the United Nations Security Council unanimously adopted a U.S.-sponsored resolution (Resolution 1617) that, among other matters, “strongly urges” all member states to “implement the comprehensive, international standards” embodied in the FATF 40 plus 9 recommendations.¹¹ Subsequently, at its most recent plenary meeting (October 12 to 14, 2005), FATF noted that “formal endorsement of the FATF standards by the U.N. Security Council is a major step toward effective implementation of the Recommendations throughout the world.”

Regarding the U.S. government’s continuing efforts to actively engage and negotiate with foreign jurisdictions as encouraged by section 330, Treasury’s Office of Terrorist Finance and Financial Crime said that outreach to the international community to enhance global best practices to combat money laundering and terrorist financing involves various challenges. These challenges include ensuring that the international standards are current in reference to emerging trends and technology and are balanced and flexible enough to be relevant and applicable to all countries and situations, as well as ensuring that evaluations or assessments of countries are conducted on a consistent basis and manner.

Treasury Views Section 330 as a Congressional Endorsement of Long-standing U.S. Government Policy and a Stimulus for Continued Efforts

According to Treasury’s Office of Terrorist Finance and Financial Crime, interagency efforts to work through FATF and the FATF-style regional bodies to help ensure global compliance with international standards for combating money laundering and terrorist financing is a long-standing policy of the U.S. government—a policy that has had strong support from the White House. In further elaboration, Treasury officials said that because working through FATF and the FATF-style regional bodies is a long-standing policy, no specific guidance was needed from the President or the White House to implement section 330. That is, Treasury was already seeking to accomplish the goals articulated in section 330. The officials commented that passage of section 330 did not cause Treasury or the interagency community to alter the objectives of ongoing or planned negotiations. In sum, the Treasury officials stressed that enactment of section 330 provided a welcomed congressional endorsement of long-

¹¹A primary purpose of Security Council Resolution 1617 was to reaffirm and strengthen international sanctions on Al-Qaida, the Taliban, and their associates.

standing U.S. government policy and also provided a stimulus for continued efforts in negotiating with foreign jurisdictions.

Treasury Considers Section 311 as Particularly Relevant for Negotiating with Foreign Jurisdictions

As an incentive or pressure mechanism that can be used in conjunction with foreign negotiations, Treasury considers section 311 of the USA PATRIOT Act to be particularly relevant for helping to ensure global compliance with international standards for combating money laundering and terrorist financing.¹² Section 311 authorizes the Secretary of the Treasury—in consultation with the Secretary of State and the Attorney General and with consideration of multiple factors—to find that reasonable grounds exist for concluding that a foreign jurisdiction, a financial institution, a class of transactions, or a type of account is of “primary money laundering concern.” Such a designation is a precursor or condition precedent for taking one or more special measures. For instance, following a designation and with additional consultation and consideration of specific factors, the Secretary of the Treasury may require U.S. financial institutions to take certain “special measures” with respect to applicable jurisdictions, institutions, accounts, or transactions. The special measures can range from enhanced recordkeeping or reporting obligations to a requirement to terminate and not open correspondent accounts involving the primary money laundering concern.

Since the USA PATRIOT Act was signed into law in October 2001, section 311 designations have been announced for three foreign jurisdictions (Ukraine, Nauru, and Burma). Treasury’s first use of section 311 authority was in December 2002, with the designation of Ukraine and Nauru as being of primary money laundering concern. A third jurisdiction, Burma, was designated in November 2003.

In addition to foreign jurisdiction designations, Treasury has also used section 311 authority to designate certain foreign financial institutions as being of primary money laundering concern. Examples include Myanmar Mayflower Bank and Asia Wealth Bank (November 2003), Commercial Bank of Syria (May 2004), First Merchant Bank of the “Turkish Republic of Northern Cyprus” and Infobank of Belarus (August 2004), and Multibanka and VEF Banka of Latvia (April 2005). More recently, in September 2005, Treasury designated Banco Delta Asia SARL, which is located in the Macau Special Administrative Region, China.

¹²Codified as amended at 31 U.S.C. § 5318A.

In discussing section 311 with us, Treasury's Office of Terrorist Finance and Financial Crime officials characterized designations—even without subsequent special measures being taken—as a very useful tool for bringing pressure on countries and institutions to meet international standards. For example, after being designated by Treasury in December 2002, Ukraine subsequently took steps to address deficiencies by amending its anti-money-laundering law, its banking and financial services laws, and its criminal code. Accordingly, Treasury revoked its designation in April 2003.

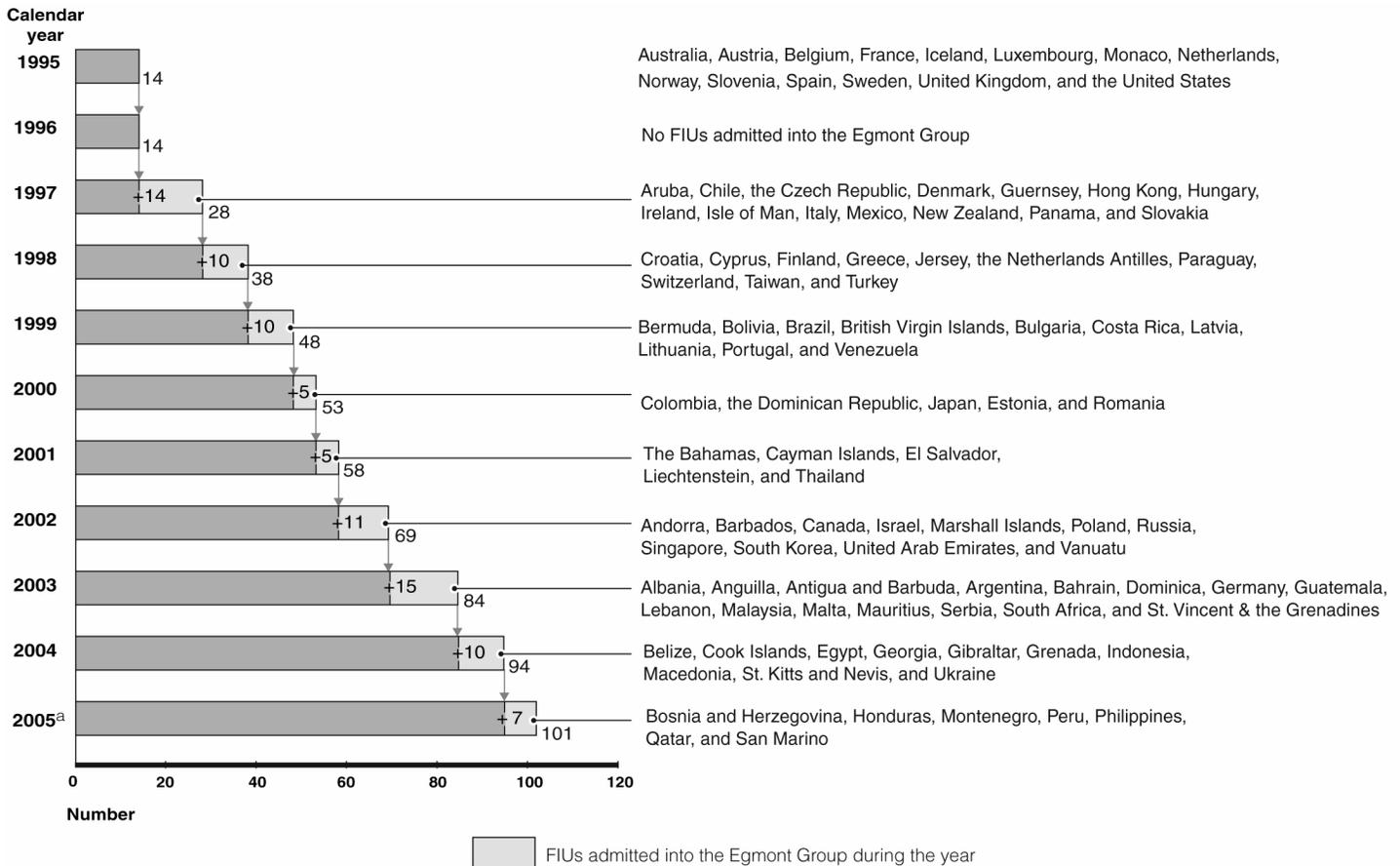
Enhancing the Capabilities of Financial Intelligence Units Is a Continuing Challenge

Since 1995, the number of FIUs recognized by the Egmont Group has increased more than sevenfold. Attributable reasons include FATF-related efforts, as well as those of the federal interagency community. A particular focus of FinCEN—working with federal interagency partners—has been to provide training and technical assistance to help create and enhance the capabilities of FIUs. Given the significant growth in the number of FIUs recognized by the Egmont Group, which now totals 101, more attention is being focused on improving the capabilities of existing units, especially in reference to combating terrorist financing—an operational task now included in the Egmont Group's definition of an FIU. Generally, FIUs are evaluated as part of an overall methodology designed to assess a country's compliance with the international standards contained in the FATF 40 plus 9 recommendations for combating money laundering and terrorist financing. According to FinCEN, its efforts to improve the capabilities of foreign FIUs must be achieved through cooperation, collaboration, and consensus—given that the Egmont Group is responsible for dealing with its members' shortcomings or noncompliance with standards.

The Number of Financial Intelligence Units Has Increased Significantly Since 1995

Over the past decade, the number of FIUs recognized by the Egmont Group increased more than sevenfold, from 14 in 1995 to 101 as of July 2005 (see fig. 1).

Figure 1: Annual Growth in the Number of Financial Intelligence Units



Source: FinCEN.

^aAs of July 2005.

A goal of the Egmont Group is to provide a forum for FIUs to improve support to their respective national programs for combating money laundering and terrorist financing. Egmont Group membership is not automatic for new or nascent FIUs. Rather, the Egmont Group has a Legal Working Group responsible for assessing each FIU-candidate to ensure that the prospective member meets admission criteria. For instance, the assessment criteria are used to determine whether the FIU-candidate meets the Egmont definition of an FIU, has reached full operational status, and is legally capable and willing to cooperate on the basis of Egmont principles (see app. III). Also, among other responsibilities, an Egmont Group member that sponsors or mentors the FIU-candidate is expected to

have first-hand experience (including an on-site visit) to confirm the operational status of the candidate FIU.

Growth in the Number of Financial Intelligence Units Is Attributable to Various Reasons

The significant growth in the number of FIUs is attributable to various reasons, including FATF-related efforts to establish international standards and promote policies for combating money laundering and terrorist financing. For example, FATF recommendation number 26 (see app. II) specifies that countries should establish an FIU that serves as a national center for receiving (and, as permitted, requesting), analyzing, and disseminating suspicious transaction reports and other information regarding potential money laundering or terrorist financing. Moreover, a contributing role has been played by the Egmont Group, which has an Outreach Working Group to identify candidate countries for membership and help them meet international standards.

Further, the growth in the number of FIUs is attributable partly to federal interagency efforts, including training and technical support provided by FinCEN and Treasury's Office of Technical Assistance, as well as funding provided by the State Department. As a member of the Egmont Group since 1995, FinCEN in particular has focused its global efforts on assisting jurisdictions establish new FIUs and improving existing units. For instance, in helping to establish new FIUs, FinCEN's assistance has included a variety of activities, such as performing country assessments, advising or commenting on draft FIU legislation, providing seminars on the combating of money laundering, conducting training courses for FIU personnel, and furnishing technical advice on computer systems. According to FinCEN, much of its work now involves strengthening existing FIUs. In this regard, FinCEN's activities include conducting personnel exchanges (from foreign FIU to FinCEN and vice versa) and participating in operational workshops and other training initiatives. Also, FinCEN noted that much of its assistance involves regional or multilateral efforts, such as working closely with the Egmont Group of FIUs, the United Nations, and multilateral development banks.

As an example of a recent FIU-related activity, FinCEN reported that it sent a four-person team to Saudi Arabia in the first quarter of fiscal year 2006 to conduct an on-site assessment and provide various presentations (covering, for example, information exchange issues) to employees of the Saudi FIU. In addition, FinCEN's activities for fiscal year 2005 included providing training (either abroad or at FinCEN) to FIU representatives from various nations, such as Argentina, Brazil, China, Guatemala, South Korea, Paraguay, and Sri Lanka. For fiscal year 2004, FinCEN reported that

it joined with the United Arab Emirates to host representatives from Afghanistan, Bangladesh, Maldives, Pakistan, and Sri Lanka on developing FIUs. Also, FinCEN's reported activities for fiscal year 2003 include

- conducting personnel exchanges with Egmont Group allies from several Baltic nations (i.e., Estonia, Latvia, and Lithuania), Bolivia, Turkey, South Korea, Ukraine, and Russia;
- co-hosting regional training workshops in Malaysia and Mauritius; and
- sponsoring Bahrain, Mauritius, and South Africa as new members into the Egmont Group—with the latter two countries representing Africa's first representatives in the group.

Similarly, according to the State Department, recent activities of Treasury's Office of Technical Assistance include (1) providing training and technical assistance to FIUs in Paraguay and Peru, (2) helping the Senegal FIU achieve operational status, and (3) working with Ukraine to streamline its national FIU.¹³

Generally, U.S. government assistance in creating and strengthening FIUs can be viewed as being one strategic element among several designed to enhance the capacity of global partners. For instance, the training and technical assistance that U.S. agencies provide to vulnerable countries are intended to help the countries develop five elements that, according to the State Department, are needed for an effective anti-money-laundering and counter-terrorism-financing regimes—a legal framework, a financial regulatory system, law enforcement capabilities, judicial and prosecutorial processes, and an appropriate FIU. However, despite the formation of an interagency coordination entity—the Terrorist Financing Working Group—U.S. efforts to coordinate the delivery of training and technical assistance lack an integrated strategic plan, as we recently reported.¹⁴ Among other matters, our October 2005 report noted disagreements between the State and Treasury departments on procedures and practices for delivering training and technical assistance as well as disagreements

¹³Department of State, Bureau for International Narcotics and Law Enforcement Affairs, *International Narcotics Control Strategy Report, Volume II, Money Laundering and Financial Crimes* (March 2006).

¹⁴GAO, *Terrorist Financing: Better Strategic Planning Needed to Coordinate U.S. Efforts to Deliver Counter-Terrorism Financing Training and Technical Assistance Abroad*, [GAO-06-19](#) (Washington, D.C.: Oct. 24, 2005).

regarding interagency leadership and coordination responsibilities. The report recommended that the Secretary of State and the Secretary of the Treasury develop an integrated strategic plan and enter into an agreement specifying the roles of each department, bureau, and office with respect to conducting needs assessments and delivering training and technical assistance. In March 2006, the State Department provided the Congress a written statement (as required under 31 U.S Code § 720) regarding action taken on the recommendation. State commented that several steps were being taken to enhance interagency coordination. The written statement noted, for example, that the National Security Council and the departments of State, Justice, the Treasury, and Homeland Security were reviewing the work of the Terrorist Financing Working Group in light of recent years' experience, with a view to making any appropriate updates and adjustments to enhance its effectiveness.

Also, during our review, State Department officials noted one area where they would like to augment U.S. assistance to nascent FIUs. This area involves ensuring that nascent FIUs have appropriate information technology (hardware and software). The officials emphasized that such technology is essential to appropriately functioning FIUs. In this regard, the officials said that the State Department and FinCEN are engaged in ongoing discussions on how to augment such assistance.

Further regarding future directions, FinCEN's Deputy Director (who also chairs the Egmont Committee¹⁵) commented that there will be continuing efforts to establish new FIUs, particularly in priority regions (such as the Middle East and Central Asia) critical to combating money laundering and terrorist financing. Moreover, given the dynamic growth in the Egmont Group's membership, the Deputy Director noted that the Egmont Committee will be giving more attention to improving the capabilities or effectiveness of existing FIUs.

¹⁵The Egmont Committee is composed of a chair, two co-vice chairs, the chairs of the Egmont Group's five working groups (information technology, legal, operational, training, and outreach), and regional representation from Africa, Asia, Europe, the Americas, and Oceania. The committee functions as the consultation and coordination mechanism for FIU heads and the five working groups.

Capabilities of Financial Intelligence Units: Some Aspects Are Covered in Assessments of Compliance with FATF Recommendations

Generally, FIUs are evaluated as part of an overall methodology designed to assess a country's compliance with the international standards contained in the FATF 40 plus 9 recommendations for combating money laundering and terrorist financing (see app. II).

As mentioned previously, FATF recommendations provide international standards for combating money laundering and terrorist financing. In this regard:

"A key element in the fight against money laundering and the financing of terrorism is the need for countries to be monitored and evaluated, with respect to these international standards. The mutual evaluations conducted by the FATF and the FATF-style regional bodies, as well as assessments conducted by the IMF and the World Bank, are a vital mechanism for ensuring that the FATF Recommendations are effectively implemented by all countries."¹⁶

Our research and inquiries identified one published study that presented comparative or multicountry results based on mutual evaluations of nations' compliance with the FATF recommendations. The study—*Twelve-Month Pilot Program of Anti-Money-Laundering and Combating the Financing of Terrorism (AML/CFT) Assessments—Joint Report on the Review of the Pilot Program*, March 10, 2004—was prepared jointly by IMF and the World Bank. The study summarized the results of the mutual evaluations of 41 jurisdictions, conducted during the 12-month period that ended in October 2003.¹⁷ The assessments used a common methodology adopted by FATF and endorsed by the Executive Boards of IMF and the World Bank.¹⁸ Of the 41 assessments, 33 were conducted by IMF or the World Bank, and 8 were conducted by FATF and the FATF-style regional bodies.

¹⁶International Monetary Fund, Legal Department, *AML/CFT Standards and Reference Materials*, April 2004.

¹⁷At the time of the March 2004 report by IMF and the World Bank, the FATF recommendations were 40 plus 8. Later, in October 2004, FATF published a ninth special recommendation on terrorist financing (see app. II).

¹⁸The common methodology reflects the principles of the FATF recommendations. See International Monetary Fund and World Bank, *Joint Report on the Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations—Supplementary Information* (March 16, 2004). Also, appendix II of this report briefly discusses an updated version of the methodology—*Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations* (updated as of February 2005).

In their March 2004 joint report, IMF and the World Bank presented assessment findings for the 41 jurisdictions in a summary format, rather than associating compliance levels or deficiencies with any individual country. For instance, the report made the following general observations:

- “Overall compliance with the FATF 40+8 Recommendations is uneven across jurisdictions. Many jurisdictions show a high level of compliance with the original FATF 40 Recommendations. The most prevalent deficiency among all assessments is weaker compliance with the Eight Special Recommendations on terrorist financing.”
- “There is generally a higher level of compliance in high and middle income countries than in low income countries. Higher income countries typically have well developed AML/CFT regimes but with specific gaps, especially concerning the Eight Special Recommendations on terrorist financing.”

The joint report did not separately present or discuss assessment findings related to the functioning or effectiveness of FIUs. However, two of the 13 main weaknesses identified are directly related to FIUs. These two weaknesses (see table 1) are topic 12 (no requirement to report promptly to the FIU if financial institutions suspect that funds stem from criminal activity) and topic 13 (poor international exchange of information relating to suspicious transactions and to persons or corporations involved).

Table 1: Main Weaknesses Identified in Assessments of Compliance with FATF Recommendations for Combating Money Laundering and Terrorist Financing

Reference number	Topic	Weakness identified	Total number of countries assessed	Assessed countries found “materially noncompliant” or “noncompliant”	
				Number	Percent of total
1	Poor assistance to other countries’ financing of terrorism investigations		40	19	48%
2	Poor attention to transactions with higher risk countries.		41	18	44
3	Poor detection and analysis of unusual large or otherwise suspicious transactions		40	17	43
4	No criminalization of the financing of terrorism and terrorist organizations		40	17	43
5	Inadequate systems to report suspicious transactions linked to terrorism		39	16	41
6	Inadequate anti-money-laundering programs in supervised banks, financial institutions or intermediaries; authority to cooperate with judicial and law enforcement		40	16	40
7	Inadequate guidelines for suspicious transactions’ detection		41	16	39
8	Inadequate measures to freeze and confiscate terrorist assets		40	14	35
9	No requirement to take reasonable measures to obtain information about customer identity		41	14	34
10	Inadequate procedures for mutual assistance in criminal matters for production of records, search of persons and premises, seizure and obtaining of evidence for money laundering investigations and prosecutions		41	14	34
11	Inadequate internal policies, procedures, controls, audit, and training programs		40	13	33
12	No requirement to report promptly to the financial intelligence unit if financial institutions suspect that funds stem from a criminal activity		41	13	32
13	Poor international exchange of information relating to suspicious transactions and to persons or corporations involved		41	13	32

Source: International Monetary Fund and World Bank, *Twelve-Month Pilot Program of Anti-Money-Laundering and Combating the Financing of Terrorism (AML/CFT) Assessments—Joint Report on the Review of the Pilot Program* (March 10, 2004, annex II, table 12, p. 55).

Notes: The assessments were conducted during the 12-month period ending in October 2003.

According to the joint report, the 41 assessments in the pilot program included compliance ratings for 27 of the FATF 40 Recommendations and 7 of the 8 Special Recommendations. Some recommendations were not rated because they had not yet fully come into force or they were not explicitly assessable, given their nature. The assessment methodology called for use of a four-grade rating scale—compliant, largely compliant, materially noncompliant, and noncompliant.

The joint report noted that assessments using the common methodology are increasingly used as a diagnostic tool to identify technical assistance needs, including assistance for creating and strengthening FIUs.

Although not published, an overview of more recent FIU-related assessment findings was presented on July 1, 2005, in Washington, D.C., at the annual plenary meeting of the Egmont Group. Specifically, an IMF representative presented summary information covering 29 countries, whose names were not disclosed. The IMF representative noted that the information was derived from the results of mutual evaluations or assessments conducted during 2003 to 2005 using the common methodology endorsed by FATF, IMF, and the World Bank. According to the presentation, the findings of the assessments indicated that many of the FIUs had shortcomings, such as a shortage of staff (one-third of the total), a lack of political independence (one-fourth), and legal obstacles to international cooperation (one-third). Other shortcomings cited were (scope not quantified) lack of clear legal framework, lack of strategic analysis tools, lack of access to appropriate information and databases, excessive transmission of information to law enforcement agencies, lack of guidelines on the identification of suspicious behavior, lack of feedback, lack of powers to sanction failure to report, and legal obstacles to the transmission of suspicious transaction reports.

In its January 2006 response to our inquiry, the State Department said that the U.S. government and other major donors generally are well informed about the existence of FIUs (and their capabilities and deficiencies) in those jurisdictions in which the donors wish to participate. State commented that while mutual evaluations are but one source of information and can be outdated before being discussed at meetings of the FATF-style regional bodies, these evaluations are useful in identifying deficiencies and prompting corrective action by the respective jurisdiction.

Dealing with FIU Shortcomings or Noncompliance with Standards Is a Responsibility of the Egmont Group

According to FinCEN's Deputy Director (and chair of the Egmont Committee), the Egmont Group is responsible for dealing with its members' shortcomings or noncompliance with standards. That is, even though influential, FinCEN has only one vote within the 101-member Egmont Group. Therefore, FinCEN's efforts to improve the capabilities of foreign FIUs must be achieved through cooperation, collaboration, and consensus.

To better address Egmont Group members' shortcomings or noncompliance with standards, the Deputy Director commented that his preference is for full transparency of assessment findings. In this regard, in its most recent annual report, FATF announced a new process for reporting assessment teams' findings that are compiled in mutual assessment reports. Specifically, according to FATF,

"A summary of each report will be published on the FATF website and FATF members have agreed in principle to make public the full mutual evaluation reports (with the ultimate decision being left to each FATF member for its own report). The FATF intends to provide comprehensive information on its members' actions in combating money laundering and terrorist financing."¹⁹

The Deputy Director also commented that the most significant functional change for the Egmont Group in recent years was expansion of the definition of an FIU in response to the terrorist attacks of September 11. Shortly thereafter, at an October 2001 special meeting of the Egmont Group in Washington, D.C., the members expressed a sense that the group's operational functions should expand beyond money laundering to address terrorist financing. Later, at the Egmont Group's 12th plenary meeting—held during June 21 to 25, 2004, and hosted in Guernsey, Channel Islands—the definition of "financial intelligence unit" was amended to include a reference to terrorist financing. This new definition is reflected in the *Statement of Purpose of the Egmont Group of Financial Intelligence Units*, which resulted from the Guernsey plenary meeting. Thus, combating terrorist financing now is included in the definition of tasks an FIU is required to perform.

According to the Deputy Director, existing FIUs have a grace period of at least 2 years to become compliant with the new definition. He noted that

¹⁹Financial Action Task Force on Money Laundering, *Annual Report 2004-2005*, June 10, 2005, p. 9.

throughout the history of the Egmont Group, no member has ever been excluded from continuing participation. The Deputy Director added, however, that plenary meetings in recent years have begun to address the issue of noncompliance. For example, according to documentation of Egmont Group meetings:²⁰

- The 11th Egmont Group plenary, held July 21 to 25, 2003, in Sydney, Australia, marked the “first attempt to establish a procedure for dealing with members that may no longer meet Egmont standards.”
- At the 12th Egmont plenary session, held June 21 to 25, 2004, in Guernsey, Channel Islands, “a paper was drafted which outlines the procedures to address those Egmont members that may no longer meet the established definitions and standards of the Egmont Group, or that fail to exchange information.”

The Deputy Director said that a paper on noncompliance was also presented at the most recent Egmont plenary meeting, held June 30 to July 1, 2005, in Washington, D.C. He added that the issue will be revisited at the 2006 plenary meeting in Cyprus. He explained that dealing with noncompliance will be a difficult issue and likely will reflect a go-slow approach. For instance, the Deputy Director opined that before administrative action (such as exclusion) is taken, the noncompliant member probably would be offered ameliorating assistance over an extended period of time.

²⁰Egmont Group, “Egmont Meetings at a Glance,” www.egmontgroup.org (2006).

FinCEN Is Taking Various Actions to Maximize Its Performance as a Global Partner, but More Comprehensive Feedback from Financial Intelligence Units Would Be Useful

Since the events of September 11, FinCEN's most important operational priority has been to provide counterterrorism support to the law enforcement and intelligence community. In January 2006, to enhance its support role, FinCEN assigned an analyst to the FBI's Terrorist Financing Operations Section. Also, among other actions to maximize performance as a global partner in combating money laundering and terrorist financing, FinCEN is modernizing the Egmont Secure Web—the Internet-based system developed and maintained by FinCEN and used by FIUs worldwide to exchange information. Further, FinCEN is allocating additional staff resources to facilitate responding to foreign requests for assistance and is developing a new case management system. However, FinCEN's most recent customer satisfaction survey of FIUs had limited coverage and a very low response rate, partly because there was no follow-up with nonrespondents. Future surveys would need to be more inclusive and incorporate better survey development and administration practices, such as follow-up efforts to achieve higher response rates, if the surveys are to serve as a useful management information tool for monitoring and enhancing performance.

Challenges for FinCEN Include Redirecting Its Efforts to More Complex Cases as well as Supporting the Nation's Focus on Detecting and Preventing Terrorist Financing

FinCEN has recognized that it faces various challenges, such as redirecting its efforts to more complex cases, some of which inevitably have international linkages. Another important challenge is to support the nation's focus on detecting and preventing terrorist financing, which also can involve international linkages.

At a congressional hearing held on April 29, 2004, the FinCEN Director testified that FinCEN must step up its international engagement with counterparts around the world by, among other means, enhancing

“the FinCEN analytical product we provide to our global counterparts when asked for information. Today, we are primarily providing the results of a data check. We think we owe our colleagues more. ... [W]e will also be making more requests for information and analysis from our partners—particularly when the issue involves terrorist financing or money laundering.”²¹

²¹Statement of William J. Fox, Director, FinCEN, at a hearing (“Counterterror Initiatives and Concerns in the Terror Finance Program”) before the Senate Committee on Banking, Housing, and Urban Affairs, April 29, 2004.

Similarly, FinCEN's strategic plan for fiscal years 2006 to 2008 noted that "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."²² Also, the strategic plan stated:

"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 ... supporting the Department of the Treasury's new focus on detecting and preventing terrorist financing. ... 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."

Further elaboration of planned efforts to enhance FinCEN's analytical capabilities is presented in Treasury's budget submission for fiscal year 2006:

"FinCEN must upgrade the quality of its analysis related to terrorist financing and money laundering. FinCEN has begun a major initiative to enhance the ability of FinCEN analysts to consider all information sources, including, as appropriate, classified data, when analyzing money laundering and terrorist financing methods. To be successful, this will require an overall upgrade to the security environment, significant investments in training and building analytical skills relating to terrorist financing, upgrade of the analytical software related to text mining, enhanced availability of classified sources ... and an increase in overall personnel security classifications to allow the integration of all information sources."²³

A primary data source used by FinCEN analysts is the government's database of BSA-related forms, including suspicious activity reports (SARs) filed by financial institutions. An integral part of FinCEN's counterterrorism strategy involves reviewing and referring all SARs related to terrorist financing to law enforcement and intelligence agencies. For instance, as of September 2005, FinCEN reported that it had proactively developed and referred a total of 526 potential terrorist

²²Financial Crimes Enforcement Network, *Strategic Plan, FY 2006-2008: Safeguarding the Financial System from the Abuse of Financial Crime* (February 2005).

²³Department of the Treasury, Financial Crimes Enforcement Network, *Fiscal Year 2006 Congressional Budget Submission* (Feb. 7, 2005), p. 4.

financing leads to appropriate agencies, such as the FBI's Terrorist Financing Operations Section and Joint Terrorism Task Forces.

In 2004, the FBI contacted the Director of FinCEN and requested bulk access to BSA reports for ingestion into the FBI's system, the Investigative Data Warehouse (IDW). The FinCEN Director recognized the benefits of having the data available in this format and approved the request. According to the FBI:

"[The IDW] is a centralized, web-enabled, closed system repository for intelligence and investigative data. This system, maintained by the FBI, allows appropriately trained and authorized personnel throughout the country to query for information of relevance to investigative and intelligence matters. In addition to BSA data provided by FinCEN, IDW includes information contained in myriad other law enforcement and intelligence community databases. The benefits of IDW include the ability to efficiently and effectively access multiple databases in a single query. As a result of the development of this robust information technology, a review of data that might have previously taken days or months now takes only minutes or seconds."²⁴

The FBI noted that FinCEN provides the IDW with regular updates of the BSA data. Also, the FBI told us that it has not had any discussions with FinCEN regarding ways to enhance FinCEN's link-analysis capability. Generally, link analysis involves use of data mining and other computerized techniques to identify relationships across organizations, people, places, events, etc. Rather, the FBI noted that it requested FinCEN to assign an analyst to the FBI's Terrorist Financing Operations Section. Such an assignment, the FBI explained, would provide FinCEN access to additional data sources, which would be useful to FinCEN in performing its various roles. FinCEN told us that it accepted this offer almost immediately, and, subsequently, in January 2006, the designated FinCEN analyst reported to the FBI to begin initial training (2 weeks) with Terrorist Financing Operations Section personnel. More recently, in March 2006, in providing us feedback on this arrangement and other interactions, the FBI commented that it highly values its strong partnership with FinCEN.

²⁴Statement of Michael F. A. Morehart, Section Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI, at a hearing before the House Committee on Financial Services (May 26, 2005).

In further reference to analyzing SARs and developing counterterrorism-related leads, we note that FinCEN developed and transmitted a total of four referrals to FIUs during the past 4 fiscal years, 2002 through 2005. Of these four referrals, according to FinCEN, two were sent to Spain's FIU, one was sent to the United Kingdom's FIU, and one was sent to both Canada's FIU and the United Kingdom's FIU. In addition to these proactive referrals, FinCEN emphasized that it regularly interacts with foreign FIUs to explore opportunities for working on issues of mutual interest. These efforts, according to FinCEN, essentially achieve the same goals and results as proactive referrals—and perhaps in a more tailored and effective manner.

Modernizing the Egmont Secure Web: Technology Is Critical to Information Sharing, a Core Function of Financial Intelligence Units

Facilitating the cross-border exchange of information is a core function of FIUs. FinCEN plays a key role in fostering the secure exchange of information among FIUs, given that FinCEN operates and maintains the Egmont Secure Web. An Internet-based system, the Egmont Secure Web is used by FIUs primarily for its encrypted e-mail capability to exchange sensitive case information. In 1997, FinCEN initially launched the Egmont Secure Web, and its development was funded solely by the Treasury Forfeiture Fund.²⁵

Operationally, according to FinCEN, the Egmont Secure Web is of paramount importance to FIUs. For instance, the Egmont Group's guidelines—*Best Practices for the Exchange of Information between Financial Intelligence Units*—state that, where appropriate, FIUs should use the Egmont Secure Web, which permits secure online information sharing among members. According to FinCEN, the system has encouraged unprecedented cooperation among FIUs because of security, ease of use, and quick response time. Also, FinCEN officials explained that the Egmont Secure Web provides online access to many reference materials, such as official Egmont procedural documents, FIU contact information, case examples, recently noted trends, and minutes from all Egmont meetings.

²⁵The Treasury Forfeiture Fund is the receipt account for the deposit of nontax forfeitures made pursuant to laws enforced or administered by the Internal Revenue Service-Criminal Investigation and Department of Homeland Security components (including U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Secret Service, and U.S. Coast Guard).

A large majority (96) of the Egmont Group’s 101 members are connected to the Egmont Secure Web. As of February 2006, 67 of the 96 FIUs each had one Egmont Secure Web user account, and 29 other FIUs each had two or more user accounts (see table 2). With 49 user accounts, FinCEN’s total is nearly three times that of Belgium’s FIU, which has the second largest number of user accounts (18). For fiscal year 2004, FinCEN reported that it supported 844 law enforcement cases via information exchanges with foreign jurisdictions and that an estimated 98 percent of FinCEN’s responses to these jurisdictions went through the Egmont Secure Web.

Table 2: Financial Intelligence Units Connected to Egmont Secure Web and Number of User Accounts per Country (as of February 2006)

Number of Egmont Secure Web user accounts per country	Number and names of countries connected to Egmont Secure Web		Total number of Egmont Secure Web user accounts
	Number of countries	Names of countries	
1	67	Albania, Andorra, Anguilla, Aruba, Austria, Bahrain, Barbados, Belize, Bermuda, Bolivia, Bosnia and Herzegovina, Brazil, Bulgaria, Cayman Islands, Colombia, Cook Islands, Costa Rica, Croatia, Cyprus, Czech Republic, Dominica, Dominican Republic, Egypt, Estonia, Finland, Germany, Gibraltar, Grenada, Guatemala, Guernsey, Hong Kong, Hungary, Iceland, Ireland, Isle of Man, Israel, Japan, Jersey, Lebanon, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Marshall Islands, Mexico, Monaco, Netherlands Antilles, New Zealand, Panama, Paraguay, Peru, Portugal, Qatar, Romania, Russia, San Marino, Singapore, Slovakia, St. Vincent and the Grenadines, Sweden, Switzerland, Taiwan, Turkey, United Arab Emirates, Vanuatu, and Venezuela	67
2	15	Antigua & Barbuda, Denmark, France, Georgia, Italy, Korea, Latvia, Liechtenstein, Mauritius, Montenegro, Norway, Poland, Serbia, South Africa, and United Kingdom	30
3	5	Bahamas, Chile, Indonesia, Netherlands, and Slovenia	15
4	2	Honduras and Spain	8
5	2	Argentina and Canada	10
6	2	Thailand and Ukraine	12
12	1	Australia	12
18	1	Belgium	18
49	1	United States	49
Total	96		221

Source: FinCEN data.

Note: An Egmont Secure Web user account is issued to an authorized user within an FIU that has been admitted into the Egmont Group. The request for a user account is submitted to FinCEN by an official within the foreign FIU. The account grants access to the Egmont Secure Web system and enables "view only" use of the Web content, including pages and documents posted for all FIUs. Also, the account includes the use of secure e-mail-enabling exchange of sensitive documents between FIUs.

FinCEN is in the process of modernizing the system by acquiring upgraded hardware and software. FinCEN officials estimated that the upgrade will be completed by mid-2006 and cost approximately \$631,000. Further, the officials noted the following information:

- The U.S. government is the owner of the system and all other users are stakeholders. In effect, FinCEN is providing a service to a group (i.e., the Egmont Group)—of which, FinCEN itself is a member.
- The Egmont Secure Web meets or exceeds the requirements for information systems that handle sensitive but unclassified information.
- The issuance of a digital certificate gives some assurance that users have met security requirements, but the burden is on the respective FIU to be responsible.²⁶

As a further safeguard, the officials noted that the Egmont Secure Web does not give foreign FIUs access to FinCEN's internal systems—for example, the FIUs have no direct access to BSA data.

Management Information and Customer Feedback Are Important Tools for Monitoring and Improving Performance

Important tools for monitoring and improving performance of any organization include implementing an effective management information system and obtaining feedback from customers. Such tools are particularly relevant for FinCEN, a networking organization that has a significant role and responsibilities in combating international financial crime.

²⁶Generally, before obtaining access to a federal computerized information system, a potential user must first be issued a digital certificate by a government-approved certificate authority. A digital certificate essentially is an electronic "credit card" that establishes a person's credentials when doing business or other transactions on the Web. The certificate contains the person's name, a serial number, expiration date, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. FinCEN is the authority for issuing digital certificates for use of the Egmont Secure Web.

Case Management: New Information System Being Developed to Better Manage Requests for Assistance

In response to our inquiry about what trends are reflected in data regarding the timeliness of FinCEN’s responses to foreign FIU requests for assistance, FinCEN officials said that their management information system does not lend itself easily to the identification of trends. The officials noted, however, that FinCEN was developing a new case management system to make statistical information more readily available. According to FinCEN officials, full implementation of the new system is scheduled for the last quarter of fiscal year 2008. The officials told us that as of March 2006, no decision had been reached on the new system’s hardware or software platform. However, the officials noted that in developing the new system, FinCEN is coordinating with Treasury’s Enterprise Architecture Office and also is complying with applicable guidance from the Office of Management and Budget.

Available case-management statistics show that FinCEN receives more requests from foreign FIUs than it submits to these counterparts. As table 3 indicates, the number of incoming requests to FinCEN has been about twice the number of outgoing requests in recent fiscal years.

Table 3: Case-Management Statistics—Foreign FIU and FinCEN Requests for Assistance

Fiscal year	Foreign FIU requests to FinCEN (incoming requests)	FinCEN requests to foreign FIUs (outgoing requests)
2002	510	341
2003	529	211
2004	612	292
2005 (through 7/25/05)	561	238

Source: FinCEN data.

Note: The data in table 3 quantify only those requests in which FinCEN was a party that either received or submitted a request for information. Thus, the data do not include, for example, requests submitted by a foreign FIU to another foreign FIU.

In managing and processing incoming requests, FinCEN’s policy is to give priority to terrorism-related requests and other “expedite” requests, such as those involving imminent law enforcement action or other extenuating time-sensitive circumstances. FinCEN officials said that responses are prepared to meet these deadlines. Otherwise, the officials said that requests from foreign FIUs are to be handled on a first-come, first-served basis. Generally, the officials noted that the timeliness of FinCEN in responding to requests from foreign FIUs can depend on a variety of

factors, such as the volume of requests, the types and amount of information being requested, the number of subjects involved (e.g., persons and accounts), whether additional clarifications of the requests are needed, and even the extent of time zone differences between FinCEN and the foreign FIUs.

According to FinCEN data, the average time for responding to foreign requests was 106 days in fiscal year 2002 and increased to 124 days in fiscal year 2004. The FinCEN officials attributed this increase to various reasons, including the growing number of FIUs and a loss of contract staff who handled the majority of the requests from foreign FIUs. More recently, FinCEN officials said that the average response time had decreased to 63 days for fiscal year 2005 (through July 25, 2005). To further improve response times, the officials indicated that FinCEN was (1) shifting additional employees to its Office of Global Support (within the Analysis and Liaison Division), which is responsible for processing requests from foreign FIUs, and (2) hiring contract staff to specifically handle FIU requests for information.

Customer Satisfaction Survey
of Financial Intelligence Units:
Limited Coverage and Low
Response Rate

For fiscal year 2005 (through July 25, 2005), a total of 561 requests were made to FinCEN by 75 foreign customers, primarily FIUs. Sixteen FIUs accounted for two-thirds of the total requests, as table 4 shows.

Table 4: Number and Names of Foreign Customer Entities That Requested Assistance from FinCEN in Fiscal Year 2005 (as of July 25, 2005)

Foreign customers (75) that requested assistance from FinCEN		Foreign requests to FinCEN for assistance	
Number	Jurisdiction and entity	Number of requests	Percentage of total foreign requests
1	Ukraine FIU	44	
2	Belgium FIU	40	
3	Isle of Man FIU	39	
4	Russia FIU	28	
5	Poland FIU	27	
6	Hungary FIU	26	
7	Bulgaria FIU	23	
8	Romania FIU	19	
9	Brazil FIU	18	
10	France FIU	18	
11	Ireland FIU	18	
12	Switzerland FIU	16	
13	Israel FIU	15	
14	Spain FIU	15	
15	Latvia FIU	14	
16	Croatia FIU	13	
Subtotal (1 through 16)		373	66
All 59 others (17 through 75)^a		188	34
Total		561	100

Source: FinCEN.

^aThe number of requests submitted by each of these 59 entities (primarily FIUs) ranged from 1 to 9. Foreign customers other than FIUs were relatively few and included, for example, Interpol.

One management priority of FinCEN is to periodically conduct customer satisfaction surveys. The purpose of such surveys is to “identify strengths and opportunities to improve services to external clients.”²⁷ FinCEN contracted with an independent research organization to conduct the most recent survey, which was designed and implemented during August to October 2005.²⁸ To obtain feedback on FinCEN’s support for investigative

²⁷Financial Crimes Enforcement Network, *Strategic Plan FY 2006 – 2008, Safeguarding the Financial System from the Abuse of Financial Crime* (February 2005, p. 22).

²⁸FinCEN’s previous survey was conducted in September to October 2003.

cases, one survey instrument was used for both domestic law enforcement customers (federal, state, and local) and international customers (FIUs). The survey instrument was designed to obtain feedback on various aspects of FinCEN's services provided during fiscal year 2005, such as the ease of making requests, the timeliness of responses, and the value or usefulness of information provided.

To facilitate distribution of the survey instrument, FinCEN provided the contractor with a list of 325 customers, a total consisting of both domestic and international customers. According to FinCEN, this total represented all customers who had requested assistance from FinCEN in fiscal year 2005 and for whom FinCEN had valid e-mail addresses. All 325 customers were invited via e-mail to participate in the Web-based survey.

Of the 325 customers, 41 were FIUs. In answering our inquiry, FinCEN officials were unable to explain why all FIUs that requested assistance from FinCEN in fiscal year 2005 were not included in the survey.

Subsequently, from the 325 domestic and international customers invited to participate in the survey, a total of 78 responses were collected, giving an overall response rate of 24 percent. Although not broken out separately in the contractor's final report, the FIU-related response rate was much lower, with only 2 of the 41 FIUs responding.

As a result of the low response rate from the FIUs, insufficient information was received to help FinCEN identify strengths and opportunities to improve services to external clients. FinCEN did receive feedback on the level of satisfaction for two FIUs, which is helpful; however, the experiences of the two FIUs cannot be interpreted as representing the experiences of other FIUs.

Generally, in conducting a survey, various efforts to promote the highest possible response rate can be considered during both survey development and survey administration. During survey development, consideration can be given to individual and organization characteristics that may affect the prospective respondents' level of cooperation in completing the survey. For instance, the prospective respondents may not want to be critical of the survey's sponsor. Another factor that affects cooperation is the burden that completing the survey instrument imposes on prospective respondents in terms of their time and the level of effort required to understand the questions and formulate responses. Pretesting the survey instrument is a way to help evaluate whether the potentially adverse effects of these types of factors have been minimized. Further, during

survey administration, follow-up efforts with prospective respondents can help to promote the highest possible response rate. Such follow-up efforts can include e-mail messages, letters, or telephone calls. FinCEN officials told us they were unaware why the response rate from FIUs was low or whether the survey included any follow-up efforts to obtain responses from additional FIUs.

In perspective, periodic surveys of customers are not the only method used by FinCEN to obtain performance feedback. For instance, in responding to each request for assistance from FIUs, the practice of FinCEN is to include an accompanying form that solicits feedback regarding the timeliness of FinCEN's response and the usefulness of the specific information provided. According to FinCEN officials, many of the feedback forms either are not returned or are returned with annotations indicating, for example, that the usefulness of the information provided by FinCEN may not be known until some future date. However, even if request-specific feedback is obtained, FinCEN officials recognize the benefits of conducting more comprehensive efforts, such as the periodic customer satisfaction surveys. This recognition, as mentioned previously, is reflected in FinCEN's *Strategic Plan*.

Conclusions

FinCEN plays a critically important role in international efforts to combat money laundering and terrorist financing. It has been a leader in the adoption and implementation of international money laundering countermeasures and supporting and advancing the Egmont Group's principles and activities. A key part of FinCEN's international role has been its efforts to respond to requests for information related to possible international financial crime. Yet, FinCEN's method for obtaining performance feedback data from global partners is flawed. Relevant feedback data include whether FIUs find the information provided by FinCEN to be substantive, timely, and useful—or how information-sharing efforts could be improved. Without such data, FinCEN is not in the best position to help the international community combat financial crime.

In its *Strategic Plan*, FinCEN recognizes the importance of periodically surveying its customers to “identify strengths and opportunities to improve services.” However, FinCEN's most-recent customer satisfaction survey of its global partners had limited coverage—with less than one-half of all FIUs being invited to participate. Also, the response rate was very low, with no follow-up efforts directed specifically at nonresponding FIUs. In the future, FinCEN's customer satisfaction surveys of FIUs need to be more inclusive and reflect higher response rates if the surveys are to serve as a useful management information tool for monitoring and enhancing

performance. The importance of monitoring and improving performance by obtaining feedback from customers is highlighted by the new operational role of FIUs in combating terrorist financing—a role in which the sharing or exchanging of information can be especially time critical.

Recommendation for Executive Action

We recommend that the Director of FinCEN take appropriate steps in developing and administering future customer satisfaction surveys to help ensure more comprehensive coverage of and higher response rates from FIUs. For example, such steps could include pretesting the survey instrument and following-up with nonresponding FIUs.

Agency Comments and Our Evaluation

We provided a draft of this report for comment to the departments of the Treasury, State, Homeland Security, and Justice, and the Federal Reserve Board. We received written responses from each agency.

The Department of the Treasury responded that it supports our recommendation that the Director of FinCEN take appropriate steps in developing and administering future customer satisfaction surveys to help ensure more comprehensive coverage of and higher response rates from FIUs. The Department of the Treasury commented that it is committed to ensuring that customer surveys provide reliable performance feedback.

The Department of State commented that our October 2005 report—*Terrorist Financing: Better Strategic Planning Needed to Coordinate U.S. Efforts to Deliver Counter-Terrorism Financing Training and Technical Assistance Abroad (GAO-06-19)*—was not relevant for discussion in this report. In our view, however, the October 2005 report provides relevant perspectives on interagency coordination and strategic planning, so we retained a brief discussion of it in this report. The Department of State also provided a technical comment regarding section 311 of the USA PATRIOT Act, which we incorporated where appropriate.

The Department of Homeland Security and the Federal Reserve Board responded that they had no comments on this report. The Department of Justice provided technical comments only, which we incorporated in this report where appropriate.

As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days after the date of this report. At that time, we will send copies of this report to

interested congressional committees and subcommittees. We will also make copies available to others on request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report or wish to discuss the matter further, please contact me at (202) 512-8777 or stanar@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other key contributors to this report were Danny Burton, Frederick Lyles, Natasha Ewing, Thomas Lombardi, and Evan Gilman.

Sincerely yours,



Richard M. Stana
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from the Chairman, House Committee on the Judiciary, we reviewed the global or international-related efforts of the Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN) to combat money laundering and terrorist financing. Section 330 of the USA PATRIOT Act expresses the sense of the Congress that the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury, in consultation with the Board of Governors of the Federal Reserve, to seek to enter into negotiations with foreign jurisdictions that may be utilized by a foreign terrorist organization in order to further cooperative efforts to ensure that foreign banks and other financial institutions maintain adequate records of transactions and account information relating to any foreign terrorist organization or member thereof.¹ The negotiators should also seek to establish a mechanism whereby those records would be made available to U.S. law enforcement officials and domestic financial institution supervisors, when appropriate.

Section 361 of the USA PATRIOT Act established FinCEN as a statutory bureau in the Treasury Department and listed FinCEN's various duties and powers, which include coordinating with foreign counterparts—that is, financial intelligence units (FIUs) in other countries.² These units are specialized governmental agencies created to combat money laundering, terrorist financing, and other financial crimes. Each FIU is the respective nation's central agency responsible for obtaining information (e.g., suspicious transaction reports) from financial institutions, processing or analyzing the information, and then disseminating it to appropriate authorities.

Specifically, our review focused on the following questions regarding efforts under sections 330 and 361 of the USA PATRIOT Act to combat money laundering and terrorist financing:

¹Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 330, 115 Stat. 272, 320.

²Codified as amended at 31 U.S.C. § 310.

- Under section 330 of the USA PATRIOT Act, how has the Department of the Treasury interacted or negotiated with foreign jurisdictions to promote cooperative efforts to combat money laundering and terrorist financing?
- Under section 361, how has FinCEN contributed to establishing FIUs in foreign countries and enhancing the capabilities of these units to combat money laundering and terrorist financing?
- What actions is FinCEN taking to maximize its performance as a global partner in combating money laundering and terrorist financing?

Scope and Methodology

Initially, in addressing the principal questions, we reviewed sections 330 and 361 of the USA PATRIOT Act and relevant legislative histories. Also, we reviewed information available on the Web sites of federal entities, including the departments of the Treasury (and FinCEN), Justice, State, and Homeland Security. Similarly, we reviewed information available on the Web sites of relevant multilateral or international bodies, such as (1) the Financial Action Task Force on Money Laundering (FATF), an intergovernmental entity whose purpose is to establish international standards and to develop and promote policies for combating money laundering and terrorist financing;³ (2) the various FATF-style regional bodies; (3) the International Monetary Fund; (4) the World Bank; and (5) the Egmont Group of FIUs.⁴ To obtain additional background and overview perspectives, we conducted a literature search to identify relevant reports, studies, articles, and other documents—including congressional hearing testimony—regarding U.S. and multilateral efforts to combat money laundering and terrorist financing.

³FATF has issued “Forty Recommendations on Money Laundering” and “Nine Special Recommendations on Terrorist Financing.” Collectively, FATF’s “40 plus 9” recommendations are widely recognized as the international standards for combating money laundering and terrorist financing.

⁴On June 9, 1995, representatives of various nations (including the United States) and international organizations met at the Egmont-Arenberg palace in Brussels, Belgium, to discuss ways to enhance mutual cooperation in combating the global problem of money laundering. A result was creation of the Egmont Group, whose members are the specialized anti-money-laundering organizations known as FIUs.

Treasury Department Efforts to Accomplish Goals Articulated under Section 330 of the USA PATRIOT Act

Regarding section 330 of the USA PATRIOT Act, to determine how the Department of the Treasury has interacted or negotiated with foreign jurisdictions to promote cooperative efforts to combat money laundering and terrorist financing, we interviewed responsible officials at and reviewed relevant documentation obtained from the departments of the Treasury, Justice, and State and the Federal Reserve Board. Also, because our preliminary inquiries indicated that efforts to accomplish the goals articulated under section 330 largely involve interactions with multilateral organizations—particularly FATF—we focused especially on the efforts of Treasury’s Office of Terrorist Finance and Financial Crime, which leads the U.S. delegation to FATF and is the department’s policy and enforcement entity regarding money laundering and terrorist financing.

Further, because section 330 does not specify any consequences or penalties for noncooperative parties or countries, we determined the availability of incentive or pressure mechanisms that could be used in conjunction with negotiations. In this regard, on the basis of Treasury’s response to our inquiry, we identified federal actions taken under USA PATRIOT Act section 311, which authorizes the Secretary of the Treasury—in consultation with the Secretary of State and the Attorney General—to find that reasonable grounds exist for concluding that a foreign jurisdiction, a financial institution, a class of transactions, or a type of account is of “primary money laundering concern.”⁵ If such a finding is made, U.S. financial institutions could be required to take certain “special measures” against the applicable jurisdictions, institutions, accounts, or transactions. The special measures can range from enhanced record keeping or reporting obligations to a requirement to terminate correspondent banking relationships with the designated entity.

FinCEN Contributions to Establishing FIUs in Foreign Countries and Enhancing Their Capabilities

In addressing this topic, we first obtained data on the annual growth in the number of FIUs over the past decade—from 1995, when the Egmont Group of FIUs was formed, to the present. Also, we obtained overview information on the history, purposes, and functioning of FIUs. For instance, the overview information—which was available on the Egmont Group’s Web site (www.egmontgroup.org) or was otherwise published—included the following:

⁵Codified as amended at 31 U.S.C. § 5318A.

- *Statement of Purpose of the Egmont Group of Financial Intelligence Units,*
- *Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases,*
- *Best Practices for the Exchange of Information between Financial Intelligence Units,* and
- International Monetary Fund and World Bank, *Financial Intelligence Units—An Overview, 2004.*

In further reference to establishing FIUs and enhancing their capabilities, we obtained information on the efforts (e.g., training and technical support) of FinCEN and other federal contributors, such as Treasury's Office of Technical Assistance and the State Department. In so doing, we interviewed responsible officials at and reviewed relevant documentation obtained from FinCEN, Treasury, and State. The federal officials we contacted included FinCEN's Deputy Director, who chairs the Egmont Committee, which functions as the consultation and coordination mechanism for FIU heads and the Egmont Group's five working groups (information technology, legal, operational, training, and outreach).⁶ The documentation we reviewed included FinCEN's annual reports and strategic plans as well as the international narcotics control strategy reports released annually by the State Department's Bureau for International Narcotics and Law Enforcement Affairs—reports that present information on FinCEN's and other federal agencies' efforts to create and improve FIUs. In identifying these federal efforts, we did not attempt to disaggregate or separately quantify contributions attributable to the respective federal agency. Rather, we made inquiries regarding any potential issues involving interagency coordination of federal efforts.

Further regarding the capability of FIUs, we identified and reviewed available studies or reports. In particular, we reviewed a report prepared by the International Monetary Fund (IMF) and the World Bank that presented comparative or multicountry results based on mutual evaluations of nations' compliance with the FATF recommendations. The study—*Twelve-Month Pilot Program of Anti-Money-Laundering and*

⁶The Egmont Committee is composed of a chair, two co-vice chairs, the chairs of the Egmont Group's five working groups, and regional representation from Africa, Asia, Europe, the Americas, and Oceania.

Combating the Financing of Terrorism (AML/CFT) Assessments—Joint Report on the Review of the Pilot Program, March 10, 2004—summarized the results of the mutual evaluations of 41 jurisdictions, conducted during the 12-month period that ended in October 2003. The assessments used a common methodology adopted by FATF and endorsed by the Executive Boards of IMF and the World Bank.⁷

To obtain more current transnational perspectives on the capability of FIUs, we attended (as an observer) the most recent annual plenary meeting (June 30 to July 1, 2005) of the Egmont Group. At the plenary meeting, held in Washington, D.C., a summary of FIU-related assessment findings was presented. The information was derived from the results of mutual evaluations or assessments (of 29 countries) conducted from 2003 to 2005 using the common methodology endorsed by FATF, IMF, and the World Bank.

Actions FinCEN Is Taking to Maximize Its Performance as a Global Partner in Combating Money Laundering and Terrorist Financing

We inquired about FinCEN's efforts to update or modernize the Egmont Secure Web, which is the Internet-based communications system developed and maintained by FinCEN and used by FIUs worldwide to share or exchange information. Generally, the Egmont Secure Web is considered to be of paramount importance to the operations of FinCEN and foreign FIUs. For instance, the Egmont Group's guidelines—*Best Practices for the Exchange of Information between Financial Intelligence Units*—state that, where appropriate, FIUs should use the Egmont Secure Web, which permits secure online information sharing among members. FinCEN is in the process of modernizing the system's 1997 architecture by acquiring upgraded hardware and software. A large majority (96) of the Egmont Group's 101 members are connected to the Egmont Secure Web.

Also, we reviewed annual statistical information on international-related requests for assistance in developing or investigating cases. Specifically, for fiscal years 2002 to 2005, we obtained statistics on requests for

⁷The common methodology reflects the principles of the FATF recommendations. See International Monetary Fund and World Bank, *Joint Report on the Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 8 Special Recommendations—Supplementary Information* (March 16, 2004). The common methodology was updated in 2005—*Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations* (updated as of February 2005).

assistance submitted by foreign FIUs to FinCEN. To the extent permitted by available data, we analyzed the statistical information on incoming requests in reference to the subject matter of the request, the country of submission, and the timeliness of FinCEN's response to the submitting FIU. We did not analyze the quality of FinCEN's responses to the incoming requests for assistance. However, we reviewed the results of the most recent customer feedback survey conducted by FinCEN. Also, we inquired about FinCEN's efforts to better monitor or improve timeliness performance by developing a new case management system and assigning additional employees to the Office of Global Support, which is responsible for processing requests from foreign FIUs.

Further, we inquired about FinCEN's efforts to enhance its analytical capabilities to handle more complex cases and support the nation's focus on detecting and preventing terrorist financing. For example, we contacted the Federal Bureau of Investigation's (FBI) Terrorist Financing Operations Section and the Foreign Terrorist Tracking Task Force.

Data Reliability

We conducted our work from June 2005 to March 2006 in accordance with generally accepted government auditing standards. Regarding the statistical information we obtained from FinCEN—i.e., information concerning requests for assistance submitted by foreign FIUs to FinCEN—we discussed the sources of the data with FinCEN officials and worked with them to resolve discrepancies we identified with the data they provided. As resolved and presented in this report, we determined that these data were sufficiently reliable for the purposes of this review.

Appendix II: Financial Action Task Force and Related Regional Bodies

This appendix presents summary information regarding the purposes and functioning of the Financial Action Task Force on Money Laundering and the various FATF-style regional bodies—international entities whose mission focuses on combating money laundering and terrorist financing. The summary information is derived largely from FATF’s Web site (www.fatf-gafi.org), which provides links to the regional bodies. Also, we discussed the information with Treasury Department officials.

The Financial Action Task Force and Related Regional Bodies Encompass Member Jurisdictions around the Globe

Initially, FATF was created in 1989 by the G7 nations in response to growing concerns about money laundering.¹ However, after the events of September 11, FATF’s mission was expanded to combat the financing of terrorism. The mission of FATF consists of three principal activities—(1) setting standards for combating money laundering and terrorist financing, (2) evaluating the progress of nations in implementing measures to meet the standards, and (3) identifying and studying methods and trends regarding money laundering and terrorist financing. In fulfilling this mission, FATF is assisted by various FATF-style regional bodies that have been established since 1992. As table 5 indicates, FATF and the related regional bodies encompass member jurisdictions around the globe.

¹The group of G7 nations—Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States—has been expanded to include Russia. Annual G8 summits bring together the leaders of these nations—with participation of the European Union (represented by the President of the European Council and the President of the European Commission)—to discuss a broad-based agenda of international, economic, political, and social issues.

**Appendix II: Financial Action Task Force and
Related Regional Bodies**

Table 5: Establishment Dates and Membership of FATF and FATF-Style Regional Bodies

FATF and FATF-style regional bodies	Year established	Number and names of member jurisdictions (as of July 2005)	
		Number	Names
FATF	1989	33	Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, China, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Kingdom of the Netherlands, New Zealand, Norway, Portugal, the Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States, the European Commission, ^a and the Gulf Cooperation Council ^b
Caribbean Financial Action Task Force	1992	30	Antigua and Barbuda, Anguilla, Aruba, The Bahamas, Barbados, Belize, Bermuda, the British Virgin Islands, the Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Republic of Haiti, Honduras, Jamaica, Montserrat, the Netherlands Antilles, Nicaragua, Panama, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname, the Turks and Caicos Islands, Trinidad and Tobago, and Venezuela
Asia/Pacific Group on Money Laundering	1997	29	Australia, Bangladesh, Brunei Darussalam, Cambodia, Chinese Taipei, Cook Islands, Fiji Islands, Hong Kong (China), India, Indonesia, Japan, Republic of Korea, Macau (China), Malaysia, the Marshall Islands, Mongolia, Nepal, New Zealand, Niue, Pakistan, Palau, the Philippines, Samoa, Singapore, Sri Lanka, Thailand, Tonga, the United States, ^c and Vanuatu
Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)	1997	27 ^d	Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Liechtenstein, Lithuania, Macedonia, Malta, Moldova, Monaco, Poland, Romania, the Russian Federation, San Marino, Serbia and Montenegro, Slovakia, Slovenia, and Ukraine
Eastern and South Africa Anti-Money Laundering Group	1999	12	Botswana, Kenya, Malawi, Mauritius, Mozambique, Namibia, Swaziland, Seychelles, Tanzania, Uganda, Zambia, and Zimbabwe
GAFISUD (South America)	2000	9	Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, and Uruguay.
Eurasia FATF	2004	6	Belarus, China, Kazakhstan, Kyrgyz Republic, the Russian Federation, and Tajikistan
Middle East and North Africa FATF	2004	14	Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, the United Arab Emirates, and Yemen

Source: GAO, based on review of Web sites of FATF and regional bodies and verification by Treasury Department officials.

^aThe European Commission is the executive arm of the European Union and is responsible for implementing the decisions of the European Parliament and the Council of the European Union.

^bThe Gulf Cooperation Council—officially known as the Cooperation Council for the Arab States of the Gulf—was established in 1981 to promote stability and economic cooperation among the Persian Gulf nations of Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates. Although the Gulf Cooperation Council is a full member of FATF, the individual member countries are not.

^cThe United States is a founding member of the Asia/Pacific Group on Money Laundering.

^dIn addition to its 27 permanent members, MONEYVAL has 2 temporary members designated on a 2-year basis by the FATF presidency. For the period 2005-2006, the 2 temporary members are France and the Netherlands.

**FATF
Recommendations
Provide a Set of
Countermeasures
against Money
Laundering and
Terrorist Financing**

FATF recommendations are designed to ensure that each nation has in place a set of countermeasures against money laundering and terrorist financing. In 1990, FATF issued its “Forty Recommendations on Money Laundering.” In October 2001, the month following the terrorist attacks in the United States, FATF issued “Eight Special Recommendations on Terrorist Financing.” More recently, in October 2004, FATF published a ninth special recommendation on terrorist financing to target cross-border movements of currency and monetary instruments. Table 6 summarizes the “Forty Recommendations on Money Laundering” and the “Nine Special Recommendations on Terrorist Financing.”

Table 6: FATF Recommendations on Money Laundering and Terrorist Financing

Forty Recommendations on Money Laundering

Number	Recommendation
1	<i>Scope of the criminal offense of money laundering:</i> Countries should criminalize money laundering on the basis of United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention). Countries should apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses. Predicate offenses may be described by reference to all offenses, or to a threshold linked either to a category of serious offenses or to the penalty of imprisonment applicable to the predicate offense (threshold approach), or to a list of predicate offenses, or a combination of these approaches.
2	<i>Criminal intent/legal persons:</i> Countries should ensure that (a) The intent and knowledge required to prove the offense of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances. (b) Criminal liability and, where that is not possible, civil or administrative liability should apply to legal persons. This should not preclude parallel criminal, civil, or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate, and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.
3	<i>Provisional measures and confiscation:</i> Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their respective competent authorities to confiscate property laundered, proceeds from money laundering or predicate offenses, instrumentalities used in or intended for use in the commission of these offense, or property of corresponding value, without prejudicing the rights of bona fide third parties.
4	<i>Financial secrecy:</i> Countries should ensure that financial institution secrecy laws do not inhibit implementation of FATF recommendations.
5	<i>Customer due diligence:</i> Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names. Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers.
6	<i>Politically exposed persons:</i> Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures (a) have appropriate risk management systems to determine whether the customer is a politically exposed person, (b) obtain senior management approval for establishing business relationships with such customers, (c) take reasonable measures to establish the source of wealth and source of funds, and (d) conduct enhanced ongoing monitoring of the business relationship. Examples of politically exposed persons include individuals who are heads of state or of government; senior politicians; senior government, judicial, or military officials; senior executives of state-owned corporations; and important political party officials.
7	<i>Cross-border correspondence:</i> Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; (b) assess the respondent institution's anti-money-laundering and terrorist financing controls; (c) obtain approval from senior management before establishing new correspondent relationships; (d) document the respective responsibilities of each institution; and (e) with respect to payable-through accounts, be satisfied that the respondent bank has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.
8	<i>Non-face-to-face business relationships or transactions:</i> Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.

Forty Recommendations on Money Laundering

Number Recommendation

- 9 *Intermediaries/introduced business*: Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements...of the customer due diligence process or to introduce business, provided that...[specified] criteria...are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.
- 10 *Record keeping*: Financial institutions should maintain, for at least 5 years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least 5 years after the business relationship is ended. The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.
- 11 *Attention to complex, unusual transactions*: Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.
- 12 *Customer due diligence and record keeping for designated nonfinancial businesses and professions*: The customer due diligence and recordkeeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in...[certain] situations. [Note: These entities include casinos; real estate agents; dealers in precious metals and stones; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers.]
- 13 *Suspicious transaction reporting*: If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit.
- 14 *Protection for suspicious transaction reporting/tipping off*: Financial institutions, their directors, officers, and employees should be (a) protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory, or administrative provision, if they report their suspicion in good faith to the financial intelligence unit, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred and (b) prohibited by law from disclosing the fact that a suspicious transaction report or related information is being reported to the financial intelligence unit
- 15 *Internal policies and controls/screening, training, audit*: Financial institutions should develop programs against money laundering and terrorist financing. These programs should include (a) the development of internal policies, procedures, and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees; (b) an ongoing employee training program; and (c) an audit function to test the system.
- 16 *Suspicious transaction reporting and internal controls for designated non-financial businesses and professions*: The requirements set out in Recommendations 13 to 15 and 21 apply to all designated non-financial businesses and professions, subject to... certain] qualifications.
- 17 *Sanctions*: Countries should ensure that effective, proportionate, and dissuasive sanctions, whether criminal, civil, or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.
- 18 *Shell banks*: Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.
- 19 *Cross-border transportation of currency*: Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

**Appendix II: Financial Action Task Force and
Related Regional Bodies**

Forty Recommendations on Money Laundering

Number Recommendation

- 20 *Application to other businesses and professions:* Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk. Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.
- 21 *Attention to transactions with problem countries:* Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate counter-measures.
- 22 *Application to branches and subsidiaries:* Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above, are also applied to branches and majority-owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.
- 23 *Supervision/regulation; prevention of criminals from positions:* Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measure to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.
- 24 *Supervision/regulation for designated non-financial businesses and professions:* Designated non-financial businesses and professions should be subject to regulatory and supervisory measures ... Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures....Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing.
- 25 *Guidelines for detecting suspicious transactions/providing feedback:* The competent authorities should establish guidelines and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.
- 26 *Financial intelligence unit establishment/powers:* Countries should establish a financial intelligence unit that serves as a national center for the receiving (and, as permitted, requesting), analysis, and dissemination of suspicious transaction reports and other information regarding potential money laundering or terrorist financing. The financial intelligence unit should have access, directly or indirectly, on a timely basis to the financial, administrative, and law enforcement information that it requires to properly undertake its functions, including the analysis of suspicious transaction reports.
- 27 *Designated law enforcement resources; investigative techniques:* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations, and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialized in asset investigation, and cooperative investigations with appropriate competent authorities in other countries.
- 28 *Document production, search and seizure powers:* When conducting investigations of money laundering and underlying predicate offenses, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.
-

Forty Recommendations on Money Laundering

Number Recommendation

- 29 *Supervisory powers to monitor:* Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorized to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements. "Supervisors" refers to designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.
- 30 *Adequate resources for competent authorities:* Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human, and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.
- 31 *Domestic cooperation:* Countries should ensure that policymakers, the financial intelligence, law enforcement and supervisors have effective mechanisms in place which enable them to cooperate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.
- 32 *Maintenance of statistics:* Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the suspicious transaction reports received and disseminated; on money laundering and terrorist financing investigations, prosecutions, and convictions; on property frozen, seized, and confiscated; and on mutual legal assistance or other international requests for cooperation.
- 33 *Use of legal persons; beneficial ownership:* Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate, and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.
- 34 *Transparency for legal arrangements/trusts:* Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate, and timely information on express trusts, including information on the settler, trustee, and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.
- 35 *International conventions:* Countries should take immediate steps to become a party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, and the 2002 Inter-American Convention against Terrorism.
- 36 *Mutual legal assistance:* Countries should rapidly, constructively, and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should (a) not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance, (b) ensure that they have clear and efficient processes for the execution of mutual legal assistance requests, (c) not refuse to execute a request for mutual legal assistance on the sole ground that the offense is also considered to involve fiscal matters, and (d) not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality. Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts. To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Forty Recommendations on Money Laundering

Number Recommendation

- 37 Provision of mutual legal assistance without dual criminality: Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality. Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offense within the same category of offense or denominate the offense by the same terminology, provided that both countries criminalize the conduct underlying the offense.
- 38 Freezing, seizing, and confiscating at foreign request; sharing confiscated assets: There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize, and confiscate property laundered, proceeds from money laundering or predicate offenses, instrumentalities used in or intended for use in the commission of these offenses, or property of corresponding value. There should also be arrangements for coordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.
- 39 *Extradition*: Countries should recognize money laundering as an extraditable offense. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without delay to its competent authorities for the purpose of prosecution of the offenses set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offense of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions. Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.
- 40 *International cooperation and exchange of information*: Countries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon requests, of information relating to both money laundering and the underlying predicate offenses. Exchanges should be permitted without unduly restrictive conditions. In particular, (a) competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters; (b) countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide cooperation; and (c) competent authorities should be able to conduct inquiries and, where possible, investigations on behalf of foreign counterparts. Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterparts, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Cooperation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance. Countries should also establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorized manner, consistent with their obligations concerning privacy and data protection.
-

Nine Special Recommendations on Terrorist Financing

Number Recommendations

- I Ratification and implementation of UN instruments: Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.
- II Criminalizing the financing of terrorism and associated money laundering: Each country should criminalize the financing of terrorism, terrorist acts, and terrorist organizations. Countries should ensure that such offenses are designated as money laundering predicate offenses.
- III Freezing and confiscating terrorist assets: Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts. Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organizations.
-

Nine Special Recommendations on Terrorist Financing

Number Recommendations

- IV Reporting suspicious transactions related to terrorism: If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations, they should be required to report promptly their suspicions to the competent authorities.
- V *International cooperation*: Each country should afford another country, on the basis of a treaty, arrangement, or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries, and proceedings relating to the financing of terrorism, terrorist acts, and terrorist organizations. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts, or terrorist organizations, and should have procedures in place to extradite, where possible, such individuals.
- VI *Alternative remittance*: Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil, or criminal sanctions.
- VII *Wire transfers*: Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address, and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address, and account number).
- VIII *Non-profit organizations*: Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused (a) by terrorist organizations posing as legitimate entities; (b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and (c) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.
- IX *Cash couriers*: Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation. Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed. Countries should ensure that effective, proportionate, and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

Source: GAO, based on review of FATF materials.

Collectively, these “40 plus 9” recommendations issued by FATF are recognized as the international standards for combating money laundering and terrorist financing. Although the FATF recommendations do not constitute a binding international convention, many countries—e.g., member nations of FATF and the FATF-style regional bodies—have made a political commitment to combat money laundering and terrorist financing by implementing the recommendations. Moreover, the international community has recognized the need for monitoring to ensure that countries effectively implement the FATF recommendations.

A Widely Adopted Methodology Is Used for Monitoring Compliance with Financial Action Task Force Recommendations

One of the means for monitoring compliance with FATF recommendations is a mutual evaluation process whereby a team of experts conducts on-site visits to assess the progress of member countries. To guide the assessment of a country's compliance with international standards, a widely adopted methodology is used—*Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations* (updated as of February 2005).² In addition to its use by FATF mutual evaluation teams, the *Methodology* has also been approved or endorsed by the FATF-style regional bodies and the Executive Boards of the International Monetary Fund and the World Bank.

The *Methodology* reflects the principles and follows the structure of the FATF recommendations. For each of the recommendations, the *Methodology* enumerates elements (“essential criteria”) that should be present for full compliance. For instance, table 3 shows the essential criteria used for assessing implementation of FATF Recommendation 26, which calls for each nation to establish and empower a financial intelligence unit.

²Copy available at www.fatf-gafi.org.

**Appendix II: Financial Action Task Force and
Related Regional Bodies**

Table 3: Essential Criteria Used in the Methodology for Monitoring Implementation of FATF Recommendation 26

Essential criterion reference number	Subject of the essential criteria
26.1	Countries should establish an FIU that serves as a national center for receiving (and if permitted, requesting), analyzing, and disseminating disclosures of suspicious transaction reports and other relevant information concerning suspected money laundering or financing of terrorism activities. The FIU can be established either as an independent governmental authority or within an existing authority or authorities.
26.2	The FIU or another competent authority should provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms and the procedures that should be followed when reporting.
26.3	The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative, and law enforcement information that it requires to properly undertake its functions, including the analysis of suspicious transaction reports.
26.4	The FIU, either directly or through another competent authority, should be authorized to obtain from reporting parties additional information needed to properly undertake its functions.
26.5	The FIU should be authorized to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect money laundering or the financing of terrorism.
26.6	The FIU should have sufficient operational independence and autonomy to ensure that it is free from undue influence or interference.
26.7	Information held by the FIU should be securely protected and disseminated only in accordance with the law.
26.8	The FIU should publicly release periodic reports, and such reports should include statistics, typologies, and trends as well as information regarding its activities.
26.9	Where a country has created an FIU, it should consider applying for membership in the Egmont Group.
26.10	Countries should have regard to the Egmont Group <i>Statement of Purpose</i> and its <i>Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases</i> . (These documents set out important guidance concerning the role and functions of FIUs and the mechanisms for exchanging information between FIUs.)

Source: GAO, based on review of FATF materials.

Appendix III: The Egmont Group of Financial Intelligence Units

This appendix presents summary information regarding the growth of the Egmont Group, which is an informal global association of governmental operating units created to support their respective nation's or territory's efforts to combat money laundering and terrorism financing. More detailed information about the purposes and functioning of the Egmont Group and its members is available at the entity's Web site (www.egmontgroup.org).¹

The Egmont Group of Financial Intelligence Units Has Grown Significantly since 1995

On June 9, 1995, representatives of various nations (including the United States) and international organizations met at the Egmont-Arenberg palace in Brussels, Belgium, to discuss ways to enhance mutual cooperation in combating the global problem of money laundering. A result was creation of the Egmont Group, whose members are the specialized anti-money-laundering organizations known as financial intelligence units. In attendance at the 1995 meeting were representatives of 14 of these governmental units ("disclosure-receiving agencies") that became the first Egmont Group members. In the decade since 1995, the group's membership has increased significantly, reaching a total of 101 jurisdictions as of July 2005 (see table 8).

¹Another useful resource is a handbook prepared jointly by the International Monetary Fund and the World Bank, *Financial Intelligence Units: An Overview* (2004).

Table 8: Egmont Group Membership by Year and Jurisdiction

Calendar year	Financial intelligence units admitted into Egmont Group membership during the year		Cumulative number of Egmont Group members (as of year end)
	Number	Jurisdiction (countries and territories)	
1995	14	Australia, Austria, Belgium, France, Iceland, Luxembourg, Monaco, the Netherlands, Norway, Slovenia, Spain, Sweden, United Kingdom, and the United States	14
1996	0	None	14
1997	14	Aruba, Chile, the Czech Republic, Denmark, Guernsey, Hong Kong, Hungary, Ireland, Isle of Man, Italy, Mexico, New Zealand, Panama, and Slovakia	28
1998	10	Croatia, Cyprus, Finland, Greece, Jersey, the Netherlands Antilles, Paraguay, Switzerland, Taiwan, and Turkey	38
1999	10	Bermuda, Bolivia, Brazil, British Virgin Islands, Bulgaria, Costa Rica, Latvia, Lithuania, Portugal, and Venezuela	48
2000	5	Colombia, the Dominican Republic, Japan, Estonia, and Romania	53
2001	5	The Bahamas, Cayman Islands, El Salvador, Liechtenstein, and Thailand	58
2002	11	Andorra, Barbados, Canada, Israel, Marshall Islands, Poland, Russia, Singapore, South Korea, United Arab Emirates, and Vanuatu	69
2003	15	Albania, Anguilla, Antigua and Barbuda, Argentina, Bahrain, Dominica, Germany, Guatemala, Lebanon, Malaysia, Malta, Mauritius, Serbia, South Africa, and St. Vincent and the Grenadines	84
2004	10	Belize, Cook Islands, Egypt, Georgia, Gibraltar, Grenada, Indonesia, Macedonia, St. Kitts and Nevis, and Ukraine	94
2005 ^a	7	Bosnia and Herzegovina, Honduras, Montenegro, Peru, Philippines, Qatar, and San Marino.	101

Source: FinCEN.

^aThe admissions in calendar year 2005 and the cumulative total are as of July 2005.

The Egmont Group Provides a Network for Exchanging Information

The common purpose of every FIU is to combat money laundering and terrorism financing. This purpose is reflected in the Egmont Group's definition of an FIU, which is as follows:

"A central, national agency responsible for receiving, (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:

- I. concerning suspected proceeds of crime and potential financing of terrorism, or
- II. required by national legislation or regulation, in order to combat money laundering and terrorism financing."²

²Egmont Group, *Statement of Purpose of the Egmont Group of Financial Intelligence Units*, www.egmontgroup.org (2006).

This definition, which was adopted in June 2004 at the Egmont Group’s plenary meeting in Guernsey, reflects an expansion of the role of FIUs to include combating terrorist financing.

Facilitating cross-border information sharing is a core goal of the Egmont Group. To enhance such sharing and provide guidelines, the Egmont Group has generated two documents—(1) *Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases* and (2) *Best Practices for the Exchange of Information between Financial Intelligence Units*. In part, the *Principles* document provides that

- “FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. Such exchange, either upon request or spontaneously, should provide any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information and the persons or companies involved.”
- “An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.”
- “Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.”
- “The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.”

The *Best Practices* document specifies that “the exchange of information between FIUs should take place as informally and as rapidly as possible and with no excessive formal requirements, while guaranteeing protection of privacy and confidentiality of the shared data” and that, where appropriate, FIUs should use the Egmont Secure Web. Further, among other guidelines, the document provides that

- “If necessary the requesting FIU should indicate the time by which it needs to receive an answer. Where a request is marked ‘urgent’ or a deadline is indicated, the reasons for the urgency or deadline should be explained.”

- “FIUs should give priority to urgent requests. If the receiving FIU has concerns about the classification of a request as urgent, it should contact the requesting FIU immediately in order to resolve the issue. Moreover, each request, whether or not marked as ‘urgent,’ should be processed in the same timely manner as domestic requests for information.”
- “As a general principle, the requested FIU should strive to reply to a request for information, including an interim response, within 1 week from receipt in the following circumstances:
 - if it can provide a positive/negative answer to a request regarding information it has direct access to;
 - if it is unable to provide an answer due to legal impediments.”
- “Whenever the requested FIU needs to have external databases searched or query third parties (such as financial institutions), an answer should be provided within 1 month after receipt of the request.”
- “If the results of the enquiries are still not all available after 1 month, the requested FIU should provide the information it already has in its possession or at least give an indication of when it will be in a position to provide a complete answer. This may be done orally.”
- “FIUs should consider establishing mechanisms in order to monitor request-related information, enabling them to detect new information they receive regarding transactions, STRs [suspicious transaction reports], etc., that are involved in previously received requests. Such a monitoring system would enable FIUs to inform former requesters of new and relevant material related to their prior request.”

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548