



## **DEPARTMENT OF THE TREASURY OFFICE OF PUBLIC AFFAIRS**

Embargoed Until Delivery  
December 15, 2003

Contact: Tara Bradshaw  
(202) 622-2014

**Testimony of Lee Jeffrey Ross, Jr  
Senior Advisor, Executive Office for Terrorist Financing & Financial Crimes  
U.S. Department of the Treasury  
Before the  
House Committee on Government Reform  
Joint Subcommittees on Government Efficiency and Financial Management and on  
Technology, Information Policy, Intergovernmental Affairs and the Census  
December 15, 2003**

Chairmen Putnam and Platts and distinguished members of the Committee, permit me to begin by thanking you for inviting me to testify today about Treasury and other government achievements in our efforts, at home and abroad, to identify, disrupt and dismantle sources of terrorist financing; the *2003 National Money Laundering Strategy* with special emphasis on interagency coordination; and, the United States Government efforts to use technology to identify and attack terrorist financing.

Money serves both as the fuel for the enterprises of terror, narco-trafficking and organized crime, as well as a significant vulnerability. Money flows leave a signature, an audit trail, and provide a road map of terror, money laundering, and organized crime which, once discovered, might well prove the best single means of identification and capture of terrorists and their facilitators, narco-trafficking cartels and infrastructure and organized crime worldwide. Thus, stopping the flow of money to terrorists, narco-traffickers and other organized criminals may be one of the very best ways we have of stopping the supported criminal activity altogether. If we and our international partners can follow and stop the money, we will have gone a long way toward destroying the infrastructure supporting these criminals.

Thus, the Department of the Treasury strongly believes that “targeting the money,” especially when applied on a systemic basis, is a key pursuit, in and of itself, to identify and attack all kinds of other criminal activity, including the financing of terrorism,

narcotics trafficking, white collar crime including securities frauds, organized crime, and public corruption. We believe that resources devoted to fighting money laundering and financial crimes reap benefits far beyond merely addressing the underlying financial crimes they directly target. Financial investigations lead upstream to those who are generating the underlying financial crimes, as well as downstream to provide a roadmap to those who facilitate the criminal activity, such as broker-dealers, bankers, lawyers and accountants. These investigations lead to the recovery and forfeiture of illegally-obtained assets as well as facilitating property both at home and abroad.

To pursue this “follow the money” approach in the Department’s efforts to combat terrorist financing, money laundering, and other financial crimes, on March 3, 2003, the Department of the Treasury established the Executive Office for Terrorist Financing and Financial Crimes (EOTF/FC). EOTF/FC, supervised by a Deputy Assistant Secretary who reports to the Deputy Secretary of the Treasury, works closely with other Treasury offices, other Federal and state government agencies, foreign government counterparts, and the private sector to prevent terrorists, money launderers, criminal tax evaders and other financial criminals from abusing the domestic and international financial systems, and to identify, block, and dismantle sources of terrorist financing, money laundering and other financial crimes. Since March, EOTF/FC has been leading the United States Government’s interagency and international effort to identify, freeze and return Iraqi assets, including both governmental funds and those looted by the former regime.

The Treasury Department is grateful to this Committee and the Congress for the additional resources, authorities, and support given to the Executive Branch to assist Treasury attack terrorist financial networks and money launderers. Of particular importance to these efforts, the USA PATRIOT Act expands the law enforcement and intelligence community's ability to access and share critical financial information regarding terrorist investigations. We at the Treasury have used and will continue to use the enhanced powers given us aggressively, but judiciously, and have made every effort to work directly with our private financial sector partners in these efforts.

### **Tampa-Anti-Money Laundering/Terrorist Financing**

It is altogether fitting that this hearing on money laundering and terrorist financing is occurring in Tampa. Tampa law enforcement has been and is on the cutting edge of investigating and prosecuting both. More than a decade ago, the Bank of Commerce and Credit International (BCCI) case, filed here in Tampa, established the global implications of money laundering. The “BCCI” case has become a by-word for the complexity, global reach and potential abuse of financial institutions and systems by money launderers. Nor is large scale money laundering restricted to international businessmen. Not too long ago, in Tampa, Haywood “Don” Hall was convicted of using his Greater Ministries International Church to bilk more than 18,000 “investors,” and launder almost \$500 million in a classic *Ponzi* scheme. This past February, an indictment here was returned charging more than \$18 million in a securities fraud and money laundering scheme.

According to the U.S. Department of Justice's Bureau of Justice Statistics Report, issued this past July, Tampa ranks sixth in the nation in money laundering investigations (55) referred for prosecution in 2001. FinCEN reports that from January 1, 2001 to October 31, 2003, Tampa banks and other depository institutions filed some 1410 SARs reporting 1557 possible violations. One SAR reported possible terrorist financing. Money service businesses have had to file SARs since January 1, 2002. From that date until October 31, 2003, some 190 such SARs were filed. Three of those SARs reported possible terrorist financing.

On the terror financing front, the Department of Justice's February 2003 RICO indictment here of Sami al-Arian and others on fifty counts, including a conspiracy to provide material support to the Palestinian Islamic Jihad, and a conspiracy to make and receive contribution to and from a specially designated terrorists, is of immense importance and points out the importance of using the money trail to find criminal conduct.

### **I. Attacking Terrorist Financing**

The financial trail left by terrorists and their facilitators represents a vulnerability that must be pursued and exploited. It is crucial to remember that the horrific end result of terrorist activities require the raising, movement and use of large volumes of funds. The terrorist act itself, no matter how basic and inexpensive, cannot be accomplished without a sophisticated financial and operational infrastructure that collectively cost millions, if not tens of millions of dollars. Terrorism's financial and operational infrastructure--"safe havens" that must be purchased, "martyrs" families that must be supported, the costs of indoctrination, logistical and personnel training and support and the costs of medical clinics and schools that some groups use to win support and recruits, and finally the purchase of the weapons-- represent a significant vulnerability that we and our international partners must attack. The terrorist leaves bloody footprints in the global financial systems, and these footprints must be pursued forward to identify future perpetrators and facilitators, and backwards to identify and dismantle supporting entities and individuals.

In the United States and overseas, the war on terrorist financing is being waged via the following:

- (i) an Executive Order using the powers granted by the Congress through the International Emergency Economic Powers Act that raises the standards of conduct and due diligence of financial intermediaries, and explicitly targets underwriters of terror for the freezing of their assets;
- (ii) UN Security Council resolutions and conventions that internationalize asset freezes and mandate the criminalization of terrorist financing;
- (iii) the formal designation by the Secretary of State of foreign terrorist organizations, resulting in the freezing of assets and other sanctions;

(iv) more scrutiny at the gateway to U.S. financial markets that has been provided under the USA PATRIOT Act;

(v) law enforcement criminal investigations, prosecutions, and foreign intelligence operations aimed at terrorist supporters and terrorist financiers;

(vi) extensive diplomatic efforts, including the engagement of central bankers and finance ministries, to champion the wisdom of and need for international vigilance against terrorist financing and the taking of appropriate action to address it;

(vii) outreach to the private sector for assistance in the identification, location and apprehension of terrorists and their bankers; and,

(viii) bilateral and multilateral efforts to build laws and systems that will help prevent terrorists from corrupting the financial system in developing countries around the globe, followed by training missions dispatched to those countries to help their officials strengthen and administer those laws.

One of the most visible and effective weapons on the financial front of the war has been the public designation of terrorists and their support network coupled with the freezing of their assets. The Executive Order imposing economic sanctions under the International Emergency Economic Powers Act permits the public designation of not only terrorists and terrorist organizations, but also supporters, facilitators and underwriters of terror as well. Once these individuals and entities are designated, this order freezes the assets of the designee held by U.S. persons. Action under this order is not “criminal” and does not require proof beyond a reasonable doubt. Designation accomplishes many results:

- (i) shutting down the pipeline by which designated parties moved money and operated financially in the mainstream financial sectors;
- (ii) informing third parties who may be unwittingly financing terrorist activity of their association with supporters of terrorism;
- (iii) deterring undesignated parties that might otherwise be willing to finance terrorist activity;
- (iv) exposing terrorist financing “money trails” that may generate leads to previously unknown terrorist cells and financiers;
- (v) forcing terrorists to use more costly informal means of financing their activities;
- (vi) supporting our diplomatic efforts to strengthen other countries’ capacities to combat terrorist financing; and
- (vii) supporting criminal prosecutions for willful violations of the requirements of IEEPA.

To date, some 344 individuals and entities have been designated, and over \$136 million frozen worldwide. Numbers designated and funds frozen, however, must never be construed as the ultimate barometer of the effectiveness of our financial war on terrorism. Only a small measure

of success in the campaign is counted in the dollars of frozen accounts. The larger balance is found in the changes that the global attacks have caused in the methodologies of raising, moving and using the financing of terror. All engaged in terror financing systems are at increased risk and scrutiny—at home from enhanced regulatory scrutiny mandated in the USA PATRIOT Act, in Saudi Arabia and elsewhere from the increased scrutiny given to charities, in the Middle East and Pakistan on the use of alternative remittance systems, and elsewhere. Compelled changes in financing methodologies disrupt systems, increase the risk of detection, and ultimately dry up the financial pipelines.

In addition, the Secretary of State, in consultation with the Secretary of Treasury and the Attorney General, can formally designate terrorist groups as Foreign Terrorist Organizations (FTOs). Such designations, authorized under the 1996 Antiterrorism and Effective Death Penalty Act, result in the freezing of assets in the United States of designated groups, and make it a criminal offense for U.S. persons to provide funds or other forms of material support to the designated groups. Members as well as leaders of FTOS are made ineligible for visas to the United States. Currently 36 groups are designated as FTOs.

The Subcommittees have asked the Department to address the importance of interagency cooperation and coordination in our war on terrorist financiers. Terrorist financing is a complicated and multi-dimensional problem that implicates a range of legal, regulatory, financial, intelligence and law enforcement interests. It is axiomatic then that any successful attack on systemic terrorist financing must adopt vigorous interagency (law enforcement, regulatory, diplomatic, intelligence, defense, as appropriate) consultation and cooperation.

To accomplish this result, shortly after the attacks of September 11, in furtherance of developing and implementing a coordinated interagency attack on terrorist financing, the National Security Council established a Policy Coordinating Committee on Terrorist Financing. The purpose of the Committee is to (i) recommend strategic policy direction to the National Security Council on issues relating to terrorist financing; (ii) vet and approve proposed public action against targeted terrorists and terrorist financiers; and (iii) coordinate the United States' efforts on issues relating to terrorist financing. The Treasury Department has chaired that Committee since October 2001.

The Committee structure ensures that we are working toward achieving the goals of the committee; however, we have purposefully kept the process flexible, informal, collaborative and iterative. It is a process that has worked well to vet and coordinate proposed policy, diplomatic, and other actions by the United States on the financial front of the war on terrorism.

From the domestic law enforcement perspective, IRS-CI participates on the FBI's JTTFs and the Attorney General's Anti-terrorism Advisory Councils, concentrating on the financial infrastructure and fundraising activities of domestic and international terrorist groups. IRS-CI works closely with the FBI, other law enforcement agencies, the Department of Treasury, and the Department of Justice (DOJ) to disrupt and dismantle the financial components of terrorist organizations. IRS-CI places considerable emphasis and focus on the use of alternative remittance systems and tax-exempt organizations suspected of facilitating the movement of funds used to support terrorism. IRS-CI and FinCEN also participate in the interagency Foreign

Terrorist Asset Targeting Group (FTAT-G) that vets possible terrorist financing targets. The FTAT-G reports to the PCC on Terrorist Financing.

### **Terrorist Financing Successes**

Among the noteworthy achievements in this area are the following:

- On September 24, 2001, President Bush issued Executive Order 13244, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism." Section 1 of the Order states: "All property and interests in property of the following persons. . .that are in the United States or that hereafter come within the United States, or that hereafter come within the possession or control of United States persons are blocked."
- 344 terrorist-related entities and individuals, including 23 charities, are currently designated by the United States pursuant to this E.O. The international community has frozen over \$136.8 million in over 1400 accounts and transfers worldwide. \$64 million of additional terrorist-related assets have been seized worldwide.
- Almost 700 terror-related accounts blocked worldwide including 100 in United States have been blocked.
- 172 countries have blocking orders in force against the assets of terrorists, and 52 countries have submitted names to the United Nations Sanctions Committee for designation.
- 80 countries have introduced new terror-related legislation, and 84 countries now have established Financial Intelligence Units.
- On November 13, 2002, the Department of the Treasury, with the Department of State, established a Counter Terrorist Financing Rewards Program, funded with \$5 million from Treasury's Counter-Terrorism Fund.
- Creation of, and FBI/IRS-CI training for, the Saudi Arabia/United States Joint Task Force on Terrorist Financing.
- Use of IRS-CI's 41 interagency SAR Review teams, including one in Tampa, to download and review approximately 140,000 SARs annually for possible leads to terrorist financing.
- November 2003 suspension by the IRS and the Department of the Treasury of tax-exempt status of the previously-designated Global Relief Foundation, Inc., the Benevolence International Foundation, Inc. and the Holy Land Foundation for Relief and Development.
- The Departments of State, Treasury and Justice also established an interagency Terrorist Financing Working Group, chaired by the State Department, to coordinate government efforts to identify, prioritize and assess those countries vulnerable to terrorist exploitation. To date, groups of experts, including DOJ prosecutors, interagency law enforcement and regulatory members, have provided extensive on-the-ground assessments to 16 countries to help build or reinforce their terrorist financing/money laundering regimes.
- On October 31, 2001, the FATF issued the Eight Special Recommendations on Terrorist Financing, including criminalizing the financing of terrorism, freezing and confiscating of terrorist assets, requiring SAR reporting relating to terrorist financing, extending anti-

money laundering requirements to alternative remittance systems, ensuring that non-profit organizations cannot be misused for terrorist financing, and requiring financial institutions to include accurate and meaningful originator information in wire transfers.

- Development and publication by Treasury of voluntary “best practices” for U.S. charities.
- May 2002 acceptance by over 40 countries of the *Abu Dhabi Declaration on Hawalas*.
- On October 1, 2002, FinCEN’s secure link with certain financial institutions (PACS) became operational.
- Since passage of the USA PATRIOT Act, more than 14,000 money service businesses, including money remitters have registered with FinCEN, and are now subject to SAR reporting.
- *U.S.-Saudi Joint Designations* --On March 11, 2002, the United States participated in its first joint designation of a terrorist supporter. Acting with Saudi Arabia, we jointly designated the Somalia and Bosnia-Herzegovina offices of Al Haramain, a Saudi-based NGO linked to al Qaida, and jointly forwarded the names of these organizations to the UN Sanctions Committee for inclusion under the UNSCR 1333/1390 list. On September 9, 2002, the United States and Saudi Arabia jointly referred to the Sanctions Committee Wa'el Hamza Julaidan, an associate of Usama bin Laden and al Qaida supporter.
- *G7 Joint Designation*--On April 19, 2002, the United States and the other G7 members jointly designated nine individuals and one organization. Most of these groups were European-based al Qaida organizers and terrorism financiers. Because of their al Qaida links, all ten names were forwarded to the UN Sanctions Committee for inclusion under the UNSCR 1333/1390 list.
- *U.S.-Italy Joint Designation*--On August 29, 2002, the United States and Italy jointly designated 11 individuals linked to the Salafist Group for Call and Combat designated in the original U.S. Annex to E.O. 13224, and 14 entities that are part of the Nada/Nasreddin financial network run by two terrorist financiers designated on earlier E.O. 13224 lists.
- *Jemaa Islamiyya Leaders (JI)*--In October 2002, fifty (50) nations combined jointly to designate (JI), an al-Qaida related terrorist network in Southeast Asia, as a terrorist group - the most widespread show of support of any terrorist designation to date.
- *OAS/CICAD/CICTE*: In November 2003, the Group of Experts to Control Money Laundering of the Organization of American States’ Inter-American Drug Abuse Control Commission (OAS/CICAD), during a session chaired by the Department of Justice, prepared final draft model provisions to guide legislators in adopting criminal offenses of terrorist financing, mechanisms to immediately block terrorist assets in accordance with United Nations Security Council resolutions, and to control alternative remittance systems. The OAS Inter-American Committee Against Terrorism (CICTE) is planning training for prosecutors and judges in member countries on terrorism and terrorist financing.
- Since September 11, 2001, the Department of Justice has prosecuted over 45 individuals for “providing material support” to terrorists or for operating illegal transmitting businesses which illegally transferred millions of dollars to Iraq and other Middle Eastern countries. These cases include:

- On February 19, 2003, a Federal grand jury indicted Professor Sami Al-Arian, three overseas leaders of Palestinian Islamic Jihad (PIJ), and four members of the Tampa, Florida, PIJ cell headed by Al-Arian, for conspiracy to commit racketeering, murder, and for knowingly providing material support to PIJ, a designated foreign terrorist organization (FTO). PIJ, based in Syria and Lebanon, has, as part of the Palestinian-Israeli conflict, engaged in a campaign of suicide bombings and armed attacks that have killed hundreds of innocent people, including American visiting, working or studying in Israel.
- A recent North Carolina-based multi-agency cigarette smuggling case revealed a massive cigarette smuggling and tax evasion scheme, in which Lebanese members of a Charlotte, North Carolina, Hizballah Cell were smuggling untaxed cigarettes from North Carolina to Michigan and using the proceeds to provide financial support and military equipment to terrorists in Beirut, Lebanon. The case culminated in Federal prosecutors convicting 18 people for material support of terrorism and other crimes involved in the smuggling scheme. The lead defendant, Mohammed Hammoud, was sentenced in February 2003, to 155 years in prison.
- In March 2003, federal prosecutors in Brooklyn unsealed indictments against two recently-extradited from Germany Yemeni nationals, including Mohammed Ali-Hassan al-Moayad who boasted that he had provided some \$20 million to Usama bin Laden, for engaging in a plot to raise funds from U.S. sources for al Qaida and HAMAS.
- In August 2003, a criminal complaint was filed against Hemant Lakhani and Yehuda Abraham, a New York diamond merchant. The complaint charged Lakhani with material support for terrorist and Abraham with conspiracy to operate an illegal money remitter. Both defendants allegedly were apprehended as a result of an FBI “sting” operation in which an alleged terrorist attempted to purchase 50 shoulder-fired missiles for a terrorist organization.
- On December 18, 2002, a Federal grand jury in Dallas, Texas, returned a superceding indictment (following an initial indictment in February 2002), charging Ghassen Elashi, the chairman of the Holy Land Foundation for Relief and Development and HAMAS leader Mousa Abu Marzook, the Holy Land Foundation’s most significant early donor, for prohibited financial dealings with terrorists.
- On February 10, 2003, Enaam Arnaout, Executive Director of the Benevolence International Foundation, pleaded guilty in Chicago to operating his charity as a Racketeer Influenced Corrupt Organization (RICO) enterprise and failing to tell donors that their money was being used to support violent *jihad*. In August, he

was sentenced to more than 11 years imprisonment and restitution to the United Nations High Commission on Refugees in the amount of \$315,000.

- On February 26, 2003, a Federal prosecutor unsealed criminal charges and brought criminal cases against persons in Syracuse, New York and Boise, Idaho, for allegedly financing terrorism through charities known as “Help the Needy” and “The Islamic Association of North America.”

## **II. 2003 National Money Laundering Strategy (2003 Strategy)**

Last month, the Department, in close cooperation with the Department of Justice, and numerous other agencies and departments, released the *2003 Strategy*. The *2003 Strategy* provides a framework for the U.S. government’s ongoing commitment to attack money laundering and terrorist financing on all fronts.

The 2003 Strategy has three overarching Goals:

**Safeguard the International Financial System from Money Laundering and Terrorist Financing.** Through a variety of bilateral and multilateral means, the U.S. will continue to promote international cooperation in using intelligence, law enforcement, and administrative powers--including strengthening the legal, financial, and regulatory infrastructure of countries around the world--to better secure the international financial system against abuse by terrorist financiers and non-terrorist criminal organizations.

**Enhance the United States Government’s Ability to Identify, Investigate, and Prosecute Major Money Laundering Organizations and Systems.** Money laundering must be made a primary--not merely an ancillary--component of any attack on substantive crimes that generate illicit proceeds and/or that facilitate terrorism.

**Ensure Effective Regulation.** Among other things, the U.S. will continue to strengthen and refine the anti-money laundering regulatory regime for all financial institutions; improve the effectiveness of anti-money laundering controls through greater communication, guidance, and information sharing with the private sector; and enhance regulatory compliance and enforcement efforts.

These Goals are focused on six key objectives:

- ***Blocking terrorist and illicit assets and cutting off worldwide channels of terrorist and illicit funding.***
- ***Establishing and promoting international standards to be adopted by countries to ensure that their financial systems are adequately protected from abuse by terrorist and other criminal organizations.***
- ***Ensuring that countries throughout the world consistently implement these international standards.***

- *Focusing efforts on financing mechanisms suspected of being of particular use by terrorist and other criminal organizations.*
- *Facilitating international information sharing.*
- *Enhancing outreach and cooperation with the private sector.*

#### **A. Enhancing Law Enforcement Attack on Interagency Basis**

A core principle of the *2003 Strategy* is enhancing our ongoing efforts to combat money laundering by ensuring that law enforcement agencies and task forces, including HIFCA, OCDEF, SAR Review Teams and HIDTA Task Forces use and share all available financial databases and analytical tools; focus law enforcement personnel and other resources on high-impact targets and financial systems; and improving Federal government interaction with the financial community.

**HIFCAs** HIFCAs (currently in New York/New Jersey, San Juan Puerto Rico, Los Angeles, San Francisco, Chicago, Miami, and a Bulk Cash HIFCA along the Southwest Border) have been created specifically to identify and address money laundering in designated geographical areas. HIFCA Task Forces seek to improve the quality of federal money laundering and other financial crime investigations by concentrating the expertise of the participating Federal and state agencies in a unified task force, utilizing all FinCEN, Drug Enforcement Agency (DEA) Special Operations Division, and DHS/ICE Money Laundering Coordination Center financial databases. In addition, FinCEN supplies direct analytical support, either at the HIFCA or from Headquarters. The Departments of the Treasury and Justice continue to review the operation of the HIFCAs in order to enhance their potential and ensure that they complement other appropriate interagency initiatives and task forces, and are preparing a report for the Congress on past operations.

**Interagency Narcotics Financing Strategy Center** Effectively attacking the financial infrastructure of the most significant drug trafficking organizations requires us to focus, as a primary, not ancillary matter, on the mechanisms and financial systems used to move and launder billions of dollars of illicit funds. As stated in the *2003 Strategy*, “the interagency law enforcement community is taking aggressive steps to develop an interagency anti-drug-money laundering financial intelligence center, to serve as a drug-money laundering intelligence and operations center. It is anticipated that this center, currently in the planning stages, will consist of money laundering investigators, prosecutors, and analysts dedicated exclusively to reviewing and acting upon all law enforcement and other financial information in order to develop the highest value targets, identify and disseminate information about developing trends and patterns, and help coordinate financial attacks on the systems, geographic locations, and individuals by and through which drug proceeds are moved and laundered.” This effort is ongoing.

**Asset Forfeiture** We also are continuing our efforts aggressively to utilize asset forfeiture laws and regulations to deprive money launderers and terrorists of their financing infrastructures, as well as all instrumentalities of their crimes. We are succeeding. The Treasury Executive Office for Asset Forfeiture reports that in FY 2003, receipts into the Treasury fund exceeded \$250 million. FY 2002 receipts totaled just under \$174 million. These are funds and other assets that

criminals not only are deprived of, but that can be put to good use either as compensation for victims, or for law enforcement purposes.

**Specially Designated Narcotics Traffickers (SDNTs) Program** A very potent financial weapon in our war against drug money laundering systems is that wielded by Treasury through the Office of Foreign Assets Control (OFAC). Treasury, through OFAC, in conjunction with the Department of Justice, enforces the IEEPA narcotics trafficking sanctions against Colombian drug cartels under Executive Order 12978. The objectives of the SDNT program are to identify, expose, isolate and incapacitate the businesses and agents of the Colombian drug cartels and to deny them access to the U.S. financial system and to the benefits of trade and transactions involving U.S. businesses and individuals. Targets are identified in consultation with the Drug Enforcement Administration and the narcotics and Dangerous Drug Section of the Department of Justice. Since the inception of the SDNT program in October 1995, some 958 business and individuals have been identified as SDNTs, consisting of 14 Colombian drug “kingpins,” 379 businesses and 565 other individuals.

**Foreign Narcotics Drug Kingpin Act Program** OFAC also administers the Foreign Narcotics Kingpin Designation Act (“Kingpin Act”). The Kingpin Act, enacted in December 1999 operates on a global scale and authorizes the President to deny significant foreign narcotics traffickers, and their related businesses and operatives, access to the U.S. financial system and all trade and transactions involving U.S. companies and individuals these actions when he determines that those foreign narcotics traffickers present a threat to the national security, foreign policy, or economy of the United States. During 2003, the President named 7 new kingpins, including a Colombian narco-terrorist guerilla army, a Colombian narco-terrorist paramilitary force and a Burmese narco-trafficking ethnic guerilla army, bringing the total number designated to 38. Since the inception of the Kingpin Act and after multi-agency consultations, 11 foreign businesses and 15 foreign individuals in Mexico and the Caribbean have been named as derivative (“Tier II”) designations by OFAC. These derivative designations are flexible, and permit OFAC to attack the financial infrastructure of these kingpins. This is an ongoing process.

Further, although terrorist financing and drug money laundering differ in some respects, they utilize many of the same financial systems and methods. Two recent cases highlight these connections.

**AUC Case** On December 4, 2002, federal prosecutors in Houston indicted several individuals, including two high ranking members of Autodefensas Unidas de Colombia (AUC/United Self Defense Forces of Colombia), the Colombian right-wing designated terrorist organization, with drug conspiracy and conspiracy to provide material support or resources to AUC. To date, two of the defendants have pled guilty to the material support § 2339B charge and the drug conspiracy charges. The AUC principals are in Costa Rican custody awaiting extradition.

**FARC Case** On March 7, 2002, a grand jury in the District of Columbia returned an indictment charging the leader of the 16th front of the Fuerzas Armadas Revolucionarias de Colombia (FARC), and six others, with participating in a drug trafficking conspiracy. Two superseding indictments have added Jorge Briceno-Suarez, the second in command of the FARC and two Peruvian drug traffickers, the Aybar brothers. The Aybar brothers also were indicted in the

Southern District of Florida for providing material support to a terrorist organization by supplying 10,000 AK-47s to the FARC in exchange for cocaine and money.

## **2. Regulatory Effectiveness**

One fact is inescapable--even the most unsophisticated of money laundering and terrorism financing operations likely will intersect the regulated financial system at some point. Pursuant to the *2003 Strategy*, we are taking full advantage of the combination of regulatory and criminal enforcement, including the vital role played by the financial sector, in helping to deter and detect money laundering and terrorist financing. Title III of the USA PATRIOT Act mandates the greatest number of substantial changes to the United States anti-money laundering regulatory regime in recent memory.

Since passage of Title III of the USA PATRIOT Act, Treasury, the Financial Crimes Enforcement Network (FinCEN), the financial regulators, and the Department of Justice have worked together to draft and issue extensive regulations that implement the Act's provisions. Among other things, we have published regulations that --

- (i) Permit and facilitate the sharing of critical information between law enforcement and the financial community, as well as among financial institutions themselves;
- (ii) Close off our financial borders to foreign shell banks, require additional due diligence for correspondent accounts maintained for foreign financial institutions, and require foreign banks with correspondent accounts in the United States to supply the name of a US agent for service of process as well as the identities of their owners;
- (iii) Require US financial institutions to establish customer identification and verification procedures for all new account holders;
- (iv) Expand the universe of financial institutions reporting potentially suspicious activities to FinCEN; and
- (v) Expand our basic anti-money laundering regime to include a wide range of financial service providers, such as the securities and futures industry and money services businesses.

Our work is not yet finished. We are working to complete several regulatory packages. First on the list is the issuance of a final regulation that will delineate the scope of the obligation of US financial institutions to conduct due diligence and enhanced due diligence on correspondent accounts maintained for foreign financial institutions and private banking accounts for high net worth foreign individuals. Although the banking, securities, and futures industries have been operating under an interim rule since last year, important questions regarding the application of this statutory provision remain.

We also will complete final regulations requiring other categories of financial institutions, such as those in the insurance and hedge fund industries, to establish anti-money laundering programs. This is an integral component of our anti-money laundering and anti-terrorist financing efforts -- to ensure that all available avenues for financial crime are blocked by this basic protection. Similarly, now that we have issued final regulations requiring the banking, securities, futures, and mutual fund industries to establish customer identification programs, we will be drafting regulations applicable to financial institutions in other industries that offer their

customers accounts. Finally, we are continuing to explore the appropriate application of the suspicious activity reporting regulations to additional categories of financial institutions. We recently issued a final rule requiring futures commissions merchants to begin reporting in early 2004. We have already proposed to require mutual funds and insurance companies to file such reports as well.

I would like to highlight two of the more significant provisions and how we are implementing them.

### ***USA PATRIOT Act Section 311***

A particularly important provision is Section 311 of the Act, which provides the Secretary with the necessary ability to protect the US financial system against specific terrorist financing and money laundering threats posed by foreign financial institutions, accounts, transactions, or even entire jurisdictions. The Secretary can require US financial institutions to take appropriate countermeasures against such threats, countermeasures which include requiring the termination of any correspondent accounts involving the threat. We have utilized this authority in the money laundering context, most recently last month against Burma and two Burmese banks, and we are presently considering its use in connection with the financing of terrorism.

Most importantly, the mere possibility of a Section 311 designation has caused nations to make changes to their legal and regulatory regimes that enhance the global anti-money laundering and anti-terrorist financing infrastructure. That said, however, the Treasury Department will continue to seek out appropriate opportunities to utilize these new powers aggressively, but judiciously, to protect the U.S financial system from corruption by money launderers and terrorist financiers.

### **USA PATRIOT ACT Section 314a**

Additionally, we have created a system pursuant to section 314(a) of the PATRIOT Act to enable law enforcement to locate quickly the accounts and transactions of those suspected of money laundering or the financing of terrorism. While we are still working closely with law enforcement and the financial community on the operation of the system, since its creation, the system has been used to send the names of 256 persons suspected of terrorism financing to financial institutions. This has resulted in 1,739 matches that were passed on to law enforcement.

## **III. Technology**

Just as criminals benefit from enhancements in technology, so must the anti-terrorist financing community. Technology holds one of the keys to our success in the financial war on terrorism. This involves the ability to marshal and synthesize all available information to proactively identify possible instances of the raising, movement and use of illicit funds. More than ever before, we require our financial institutions to produce data and information. Several initiatives should be highlighted. For example, FinCEN is at the first phase of a project involving assistance from the Business Executives for National Security and the Wharton School of the University of Pennsylvania in developing technology that will allow financial institutions to

report suspicious transactions more easily and quickly. In addition, as part of an overall plan to enhance our technological platform, FinCEN is developing a new system to manage the Bank Secrecy Act (“BSA”) database. “BSA Direct” will involve a significant upgrade to the platform on which the BSA database is maintained, and will provide users with web-based, secure access that allows for faster and easier searching. Finally, we will continue to work to assist financial institutions in developing proactive software to better identify potential terrorist financing activities.

Information developed cannot be applied in a vacuum. Congress recognized that fact when it made enhanced information sharing a central theme of the USA PATRIOT Act. While we have taken substantial steps toward this goal, our challenge remains to find better ways of providing information and feedback. This is not simple. Often the information we develop is highly protected intelligence information that cannot be disclosed, and we are always wary of providing our enemies with a roadmap or a “how-to” guide to manipulating our defenses. That said, we understand the importance of, and are searching for, better ways to share information among ourselves, with the private sector and our global partners.

One example of the use of technology to identify possible sources of terrorist financing is a pilot counterterrorism project undertaken by IRS-CI in Garden City, New York. The Garden City Counterterrorism Lead Development Center is dedicated to providing research and nationwide project support to IRS-CI and the Joint Terrorism Task Force (JTTF) counterterrorism financing investigations. Relying on modern technology, the Center is comprised of a staff of IRS Special Agents, Intelligence Analysts, and civil components from the Service’s Tax Exempt/Government Entities Operating Division, who will research leads and field office inquiries concerning terrorism investigations. Center personnel specializing in terrorism issues will develop case knowledge, identify trends, and provide comprehensive data reports to IRS field agents assigned to JTTFs or to those conducting CI counterterrorism financing investigations.

The Center may also serve to de-conflict related investigations among multiple field offices, and will have distinctive analytical capabilities to include link analysis, data matching, and pro-active data modeling. Using data from tax-exempt organizations and other tax-related information that is protected by strict disclosure laws, the Center will analyze information not available to or captured by other law enforcement agencies. Thus, a complete analysis of all financial data will be performed by the Center and disseminated for further investigation. This research, technology, and intuitive modeling, coupled with CI’s financial expertise, maximize IRS-CI’s impact against sophisticated terrorist organizations.

In conclusion, let me provide you with some sense of how we are using the USA PATRIOT Act powers and enhanced technology, as well as the implementing regulations to combat terrorist financing. Although the process is ongoing, we do have some indication of their effectiveness. For example, as noted earlier, the section 314(a) system has been used in many cases and has resulted in a substantial number of leads. The additional reporting and recordkeeping authorities have enhanced the database FinCEN uses for its research and analysis in supporting terrorism investigations – since September 11th, FinCEN has supported 2,692 terrorism investigations. The Terror Hotline established by FinCEN has resulted in 789 tips passed on to law enforcement. Since the World Trade Center Attacks, FinCEN has made 519 proactive case referrals to law enforcement based upon an analysis of information in the Bank Secrecy Act

database. FinCEN also is implementing an Electronic Reports program that will be able to issue these reports in an electronic format, thus enhancing law enforcement's ability better to utilize the information. With the expansion of the suspicious activity reporting regime, financial institutions nationwide have filed 2,842 suspicious activity reports ("SARs") reporting possible terrorist financing. In addition to passing these reports on to law enforcement, FinCEN has and will continue to support these activities.

I will be happy to answer any questions you may have.

-30-