Testimony of

Juan C. Zarate

Deputy Assistant Secretary
Terrorism and Violent Crime

U.S. Department of the Treasury

House Financial Subcommittee
Oversight and Investigations

2:00 p.m. February 12, 2002

The United States House of Representatives

2167 Rayburn House Office Building

Chairman Kelly and distinguished members of the House Financial Services Subcommittee, permit me to begin by thanking you for inviting me to testify today about the measures the Treasury Department has taken to disrupt terrorist financing, the lessons we have learned to date about patterns of financing and fundraising, and how the provisions of the recently enacted USA PATRIOT Act (PATRIOT Act) are helping us in our mission. With me today are three individuals who are assisting the Treasury Department in connection with the U.S. government's efforts to investigate the financing of terrorism: John Varrone, Assistant Commissioner, Office of Investigations, U.S. Customs Service; R. Richard Newcomb, Director of the Office of Foreign Assets Control (OFAC); and James F. Sloan, Director of the Financial Crimes Network (FinCEN). Thank you for having us here today to address you.

As you are aware, on September 24, 2001, President Bush stated, "We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding." The President directed Secretary O'Neill to lead the nation's war against the financing of global terrorism, and we have devoted our extensive resources and expertise to fulfill this mandate. In our actions and in our words, the Treasury Department has shown quite clearly that in this war, financial intermediaries and facilitators who infuse terrorist organizations with money, materiel, and support must be held accountable along with those who perpetrate terrorist acts.

The Treasury Department owes this Committee, and Congress in general, a debt of gratitude in helping us with the resources and authority to identify, disrupt, and dismantle terrorist financial networks. Immediately after the horrific attacks of September 11th, Congress worked closely with the Department of the Treasury, along with the Department of Justice and other agencies and departments, to make significant improvements in the law that allows us to

tackle the issue of terrorist financing in a more unified, aggressive manner. Of particular importance to our counter-terrorist efforts, the PATRIOT Act clarifies the law enforcement and intelligence communities authority to share financial information regarding terrorist investigations. These provisions are already being utilized and are bearing fruit in disrupting financing networks.

Before I address the specific issues raised in your invitation letter, allow me to share with you the efforts the Treasury Department has taken to date, along with our sister departments and agencies, to combat terrorist financing.

THE BATTLE AGAINST TERRORIST FINANCING:

Treasury, in close partnership with the State Department, the Defense Department, the Department of Justice, the Federal Bureau of Investigation, the intelligence community, and many other parts of the federal government, has been dealing with terrorist financing on multiple levels. We have concentrated much of our enforcement efforts and resources on identifying, tracing, and blocking terrorist-related assets. In this endeavor, we have collected the financial expertise, information, and authorities that are unique to the Treasury Department to attack terrorist financing on all fronts. We have also engaged the world, in bilateral and multilateral fora, to ensure international cooperation in our anti-terrorist campaign. Allow me to highlight briefly the efforts the Treasury Department has taken to date to tackle the global problem of terrorist financing.

TREASURY ENFORCEMENT ACTIONS

First, the Treasury Department chairs the inter-agency working group that has been targeting and listing individuals and entities pursuant to the President's September 23, 2001 Executive Order. In this inter-agency process, we have assembled experts and policymakers from the Treasury Department, including the Office of Foreign Assets Control (OFAC), the Department of Justice, the Department of State, the Federal Bureau of Investigation (FBI), the intelligence community, and the White House. Through this process, the U.S. Government has designated 168 individuals and entities as terrorist-related entities pursuant to the Executive Order. Since September 11th, the United States and other countries have frozen more than $104 million in terrorist-related assets. Since the attacks, the United States alone has blocked over $34 million. A portion of that amount has since been unblocked for the new Afghan Interim Authority.

In this process, we have identified, among other entities, front companies, charities, banks, and a hawala conglomerate that served as the financial support networks for al-Qaida and other global terrorist groups. We have shut down the operations of these entities in the United States and abroad.

Second, as part of the anti-terrorist financing strategy, we utilized the inter-agency Foreign Terrorist Asset Tracking Center (FTAT), led by Treasury's OFAC, immediately after the September 11th attacks to serve as an analytical center for attacking the problem of terrorist financing. Treasury's OFAC and its FTAT division have served not only to provide essential

analysis on particular targets and networks, but the center is a place where intelligence and law enforcement agencies can share and analyze information for a common purpose. This inter-agency concentration on hunting the sources of terrorist financing complements the work being done by the FBI's Financial Review Group, the Department of Defense and the intelligence community to uncover terrorists. Though FTAT is still in its infancy, it continues to make a significant impact on this cooperative and concentrated venture.

The process of identifying and investigating targets is ongoing, and we are currently investigating other financial entities, businesses, groups, and persons for potential listing. We are focusing on uncovering high-impact financial intermediaries that act as financial conduits and facilitators for terrorist groups. Our ultimate goal is to use all the tools at our disposal to disrupt vigorously terrorist financing in an effort to prevent the perpetration of further terrorist attacks.

Third, on October 25, 2001, Treasury created Operation Green Quest ("Green Quest"), a new multi-agency financial enforcement initiative intended "to augment existing counter-terrorist efforts by bringing the full scope of the government's financial expertise to bear against systems, individuals, and organizations that serve as sources of terrorist funding." Green Quest is aimed at identifying, freezing and seizing the accounts and assets of terrorist organizations that pose a threat to the United States and to all nations of the world. This task force is led by the Customs Service, and includes the Internal Revenue Service, the Secret Service, the Bureau of Alcohol Tobacco and Firearms (ATF), Treasury's Office of Foreign Asset Control (OFAC), FinCEN, the Postal Inspection Service, the Federal Bureau of Investigation (FBI), the Department of Justice, and the Naval Criminal Investigative Service (NCIS). Green Quest brings together the extensive financial expertise of the Treasury Bureaus along with the exceptional experience of our partner agencies and departments to focus on terrorist financing.

Green Quest has complemented the work of OFAC and FTAT in identifying terrorist networks at home and abroad, and it has served as an investigative arm in aid of blocking actions. Green Quest's work has led to 11 arrests, 3 indictments, the seizure of nearly $4 million, and bulk cash seizures—cash smuggling—of over $9 million. Green Quest, along with the FBI and other government agencies, has also traveled abroad to follow leads, exploit documents recovered, and to provide assistance to foreign governments. In this effort, Green Quest has made full use of its overseas Customs Attachés to investigate suspect networks and to gather information for its own use and the use of FTAT. The work of these financial experts is just starting as they have opened numerous terrorist financing investigations and are following leads on a daily basis. Green Quest's work, in combination with the work of OFAC and FTAT, serves as a seminal part of our enforcement efforts.

Finally, we have also been committed fully since the terrorist attacks to the FBI-led investigation into the September 11th mass murders. Immediately after the attacks, Treasury assets were deployed to engage in the FBI efforts to bring the perpetrators and their financiers to justice. Treasury agents and analysts from the Customs Service, IRS-Criminal Investigation Division, U.S. Secret Service, the Bureau of Alcohol, Tobacco, and Firearms, and FinCEN combined efforts with the FBI's Financial Review Group, bringing with them their unique financial investigative capabilities, contacts in the financial sector, and expertise.

For example, the U.S. Secret Service was able to bring its experience in credit card and identity fraud as well as its electronic crimes expertise to bear immediately on the investigation, working with the Department of Justice in the following ways:

- Assisting in developing complete financial profiles of all suspects (living and deceased) in the investigation;
- Identifying other suspects through current and historical financial investigations;
- Contributing to an intelligence assessment regarding possible future acts through analysis of money movement, expenditures, and other financial data;
- Developing an analysis of current credit card usage by the suspects in the investigation; and
- Investigating more than 17,000 leads in support of the Department of Justice investigation.

As you can see, the U.S. Secret Service, along with the other Treasury Bureaus, has made significant contributions in close coordination with the FBI to tracking the perpetrators and facilitators of the September 11th attacks.

INTERNATIONAL COOPERATION

Our efforts cannot be successful if prosecuted unilaterally and are ultimately doomed to failure if we cannot obtain the cooperation of other nations. To date, all but a handful of countries have expressed their support for the international fight against terrorist financing. Currently, 149 countries and jurisdictions around the world can block terrorist assets. The U.S. government is working with a number of countries with respect to technical assistance to strengthen their capacity to freeze terrorist funds. Daily, we are in contact with foreign financial officials and are engaged in bilateral and multilateral discussions regarding international cooperation and action against terrorist activities and financing.

Treasury has engaged in numerous international fora, including the G7, G8, G20, the Financial Action Task Force (FATF), the global network of Financial Intelligence Units (FIUs) of which FinCEN is a key member, and the international financial institutions to combat terrorist financing in a global, systematic way. Treasury has also worked with regional organizations such as APEC and the Manila Framework Group to further coordinate international efforts to stop the financing of terrorism. In March, we, along with the State Department, will be participating in an ASEAN Regional Forum and Pacific Island Forum regarding counter-terrorism and financing issues.

A good example of the work of Treasury, State and Justice on this issue is in the role of the United States in the FATF on Money Laundering, a thirty-one member organization. We have directed the international effort to use the successful FATF to address the issue of terrorist financing. The United States hosted an Extraordinary FATF Plenary session in October of 2001, at which FATF members established 8 Special Recommendations on Terrorist Financing that have quickly become the international standard on how countries can ensure that their financial regimes are not being abused by terrorist financiers. Our delegation just returned from a Plenary Session in Hong Kong in which, among other things, FATF is engaging all countries, including non-members, in a self assessment process concerning measures against terrorist financing in

their respective financial regimes. This FATF effort, along with our continued engagement at a bilateral and multilateral level, will ensure that we are marginalizing terrorist financiers by securing the global financial system.

Also, on November 17, the G20 finance ministers and central bank governors met in Ottawa, Canada and agreed that they would block terrorist assets in their respective countries, and report publicly on precisely which terrorist groups each country has blocked and the amount of actual monies blocked, if any. Meeting the next day, the governing body of the IMF announced that the IMF will take similar steps.

This past weekend, the G7 group of industrial countries met in Ottawa and agreed to an ambitious new work program. In particular, the G7 agreed to develop a mechanism to identify jointly terrorists whose assets would be subject to freezing. This will require even closer cooperation and commitment. We will also develop key principles regarding information to be shared, the procedures for sharing it, and the protection of sensitive information.

Treasury also supports FinCEN's active involvement in the growing network of financial intelligence networks or FIUs. The specialized agencies created by governments to fight money laundering first met in 1995 at the Egmont-Arenberg Palace in Belgium to share experiences. Now known as the Egmont Group, these FIUs meet annually to find ways to cooperate, especially in the areas of information exchange, training, and the sharing of expertise.

This global network of information exchange and cooperation has been a valuable and responsive avenue of terrorist-related information. FinCEN hosted a special meeting of the Egmont Group on terrorist financing in October 2001 to support the unprecedented law enforcement investigation in the wake of the events of September 11. During the special meeting, the Egmont Group agreed to: (1) review existing national legislation to identify and eliminate existing impediments to exchanging information between FIUs, especially when such information concerns terrorist activity; (2) encourage national governments to make terrorist financing a predicate offense to money laundering and to consider terrorist financing one form of suspicious activity for which financial institutions should be on the look out; (3) pass requests for information involving FIUs exclusively between FIUs rather than other government agencies; (4) have FIUs play a greater role screening requests for information; and (5) to pool Egmont Group resources, where appropriate, to conduct joint strategic studies of money laundering vulnerabilities, including Hawala.

THE WORLDWIDE AL-BARAKAAT INVESTIGATION AND FREEZING OF ASSETS

The November 7, 2001 designation of Al-Barakaat as a terrorist-related financial entity is a good example of how Treasury efforts both domestically and abroad, along with the fine work of our inter-agency partners, can lead to results in this war on terrorist financing. Al-Barakaat is a Somali-based hawaladar[1] operation, with locations in the United States and in 40 countries, that

[1] Hawala is a type of alternative remittance system that is common in many parts of the world, including the Middle East and Far East. A hawaladar is an entity that engages in hawala transactions.

was used to finance and support terrorists around the world.[2] OFAC, FinCEN, and intelligence analysis, along with investigative work by the U.S. Customs Service, IRS-Criminal Investigation Division, and the FBI, identified Al-Barakaat as a major financial operation that supported terrorist organizations and was providing materiel, financial, and logistical support to Usama bin Laden and other terrorist groups.

Treasury and the FBI took decisive action to block assets and to take law enforcement actions against Al-Barakaat. On November 7, 2001, federal agents executed search warrants in three cities across the country (Boston, Columbus, and Alexandria) and shut down eight Al-Barakaat offices across the U.S., including locations in the following cities:

- Boston, Massachusetts;
- Columbus, Ohio;
- Alexandria, Virginia;
- Seattle, Washington; and
- Minneapolis, Minnesota.

At the same time, OFAC was able to freeze approximately $1,100,00 domestically in Al-Barakaat-related funds. As part of the Department's international outreach efforts, Treasury also worked closely with the United Arab Emirates to enable the UAE to block Al-Barakaat's assets at its financial center of operations in Dubai. Disruptions to Al-Barakaat's cash flows, resulting from OFAC's designation actions and international cooperation, are estimated to be in excess of $65 million from the United States alone. In addition, the combined work of OFAC, Operation Green Quest, and law enforcement had led to additional leads in the Al-Barakaat investigation.

This is an example of what our combined efforts can accomplish when we join our resources and our expertise to fight the common scourge of terrorist financing.

In sum, Treasury is tapping the full spectrum of our financial forensic expertise as well as the experience and resources of other agencies and foreign governments to execute the President's mission to detect, disrupt, and dismantle the financial infrastructure of terrorist financing.

TERRORIST FINANCING TRENDS

Based on our combined efforts and our experience in this war against terrorist financing, we are beginning to see more clearly the mosaic of terrorist financing and the movement of suspected terrorist funds. Terrorist groups differ from other criminal organizations or networks because of the motive behind the crime. Unlike drug traffickers and organized crime groups that primarily seek monetary gain, terrorist groups usually have non-financial goals: publicity; the dissemination of an ideology; the destruction of a society or regime; and simply sowing terror and intimidation.

[2] Some individuals may have used Al-Barakaat as a legitimate means to transfer value between individuals in different countries without passing through the formal international banking system.

Terrorist financing, therefore, is different than classic money laundering. In cases of money laundering, the proceeds of illicit activity are laundered or layered in ways to make the proceeds appear legitimate, and the ultimate goal is usually the attainment of more money. With terrorist financing, the source of funding or financing is often legitimate – as in the case of charitable donations or profits from store-front businesses – and the ultimate goal is not necessarily the attainment of more funds. The ultimate goal of terrorist financing is destruction.

Uncovering the sources and methods of terrorist financing is a complex endeavor. The complexity stems in part from the sophistication of the individuals attempting to hide their activities. It is also difficult to attribute certain types of activities or movement of money directly to terrorism.

Nevertheless, there are similarities in the way international criminal enterprises and terrorist organizations of global reach, like al-Qaida, move money or attempt to hide their financial tracks. International terrorist groups need money to attract, support, and retain adherents throughout the world as well as to secure the loyalty of other groups that share the same goals. Thus, there is a need to devise schemes to raise, collect, and distribute money to operatives preparing for attacks. This need to move money makes the terrorist funds vulnerable to detection if we have the right safeguards in place.

SOURCES OF TERRORIST FUNDING

There are a plethora of terrorist funding sources, and the means used by particular terrorist organizations varies from group to group. Some terrorist groups, such as those in Europe, East Asia, and Latin America, rely on common criminal activities including extortion, kidnapping, narcotics trafficking, counterfeiting, and fraud to support their heinous acts. Other groups, such as those in the Middle East, rely on commercial enterprises, donations, and funds skimmed from charitable organizations to not only fund their activities but also to move materiel and personnel. Still other groups rely on state sponsors for funding.

The following is a basic summary of the sources of funding and the means used to move money that we believe terrorist organizations and their supporters use to plan attacks and to support their networks.

1. DONATIONS TO CHARITIES

Investigation and analysis by enforcement agencies have yielded information indicating that terrorist organizations sometimes utilize charities to facilitate funding and to funnel money. Charitable donations to non-governmental organizations (NGOs) are commingled and then often diverted or siphoned to groups or organizations that support terrorism. Fundraising may involve community solicitation in the United States, Canada, Europe, and the Middle East or solicitations directly to wealthy donors. Though these charities may be offering humanitarian services here or abroad, funds raised by these various charities are sometimes diverted to terrorist causes. This scheme is particularly troubling because of the perverse use of funds donated in good will to fuel terrorist acts.

We have seen clear examples of this type of scheme in our efforts to identify and freeze terrorist-related assets. In one instance, Hamas, a foreign terrorist organization, used the largest U.S. Islamic charity, the Holy Land for Relief and Development (Holy Land), as a fundraising source for its terrorist activities. Based on preliminary work of the FBI, we acted to designate Holy Land on December 4, 2001, pursuant to E.O. 12334 and to freeze the assets of Holy Land because it was being used as a charitable front to raise and funnel money to Hamas. In another example, on January 9, 2002, the Treasury Department blocked the assets of two foreign charities that were funneling funds to al-Qaida: the Afghan Support Committee and the Pakistan and Afghanistan offices of the Revival of Islamic Heritage Society (RIHS).

The Treasury Department continues to scrutinize the activities of suspect charitable organizations, both in North America and abroad that may have ties to terrorist organizations. In addition, we will continue to work closely with our international partners to ensure that there are monitoring and regulatory mechanisms in place for any such NGOs in their jurisdiction. As we have said before, charities advertising to help refugees, widows and orphans should be doing just that–not being used, wittingly or otherwise, to funnel money to terrorist organizations or to indoctrinate impoverished populations with political-religious extremism and with it a potential breeding ground for future terrorism.

2. COMPANIES AND BUSINESSES

Terrorist groups create front businesses and corporations, transfer funds between them, and "layer" the financial transactions to avoid detection. We have designated several companies, such as the Al-Barakaat companies, as fronts for terrorist organizations pursuant to the President's Executive Order.

Seemingly legitimate businesses have been used by terrorists and their supporters as "fronts" to disguise a variety of criminal activities. These businesses often can be convenience stores, restaurants, or fast food stores. The businesses are usually acquired using funds furnished by a single individual. This investor, in exchange for providing financing, receives a portion of the profits from legitimate business operations until the investment is repaid. In some cases, it is alleged that the "seed" money to acquire the businesses is provided by terrorist groups.

Small retail businesses that deal extensively in cash are ideal for laundering the proceeds from a variety of criminal activities and provide retail outlets for stolen merchandise. They are also ideal locations from which informal money remittors, like hawaldars, can transact business.

Regular fraud schemes frequently result in illegal profits and resulting criminal investigations that ultimately uncover terrorist financing. One clear example of this occurred last year, when an inter-agency task force, involving the FBI, the Bureau of Alcohol, Tobacco, and Firearms, the Immigration and Naturalization Service, and other law enforcement uncovered a contraband cigarette trafficking and fraud scheme involving approximately a dozen Lebanese individuals. In the course of investigating this scheme, the task force uncovered that some of the participants were involved in a military procurement program designed to obtain and send dual use items to Hizbollah operations in Lebannon.

We continue to monitor, analyze, and investigate the links between businesses, in the United States and elsewhere, and terrorist groups. Using Bank Secrecy Act data and analysis provided by FinCEN and other relevant data from various Treasury databases, we are able to target suspicious business activities and anomalous transactions. This type of methodical investigative and analytical work will continue to uncover networks of businesses used to generate and funnel money to terrorist groups.

3. TRADE MISPRICING

International trade may be utilized by terrorist organizations to disguise funding sources. Terrorist front companies might overvalue or undervalue merchandise, or they might use double invoicing or might fabricate shipments altogether. The Treasury Department is looking into this method of raising funds, but there has as yet been no direct link established to terrorist financing.

There are various Customs commercial databases that are capable of identifying trends and anomalies in a particular company or industry. Specifically, the U.S. Customs Service has developed a program known as the Numerically Integrated Profiling Systems (NIPS). NIPS allows for the manipulation of trade data, BSA data, commerce data and I-94 passenger data. Green Quest has applied NIPS in targeting commodities and companies that may be funneling funds in support of terrorism. NIPS is a component of the Green Quest strategy to target trade-based money laundering or terrorist financing systems.

An example of this type of activity involved an analysis conducted by the U.S. Customs Service Offices of Strategic Trade and Intelligence. This analysis involved the exportation of honey to Middle Eastern countries. On October 12, 2001, the Treasury Department named two honey companies as fronts for terrorist funding to al-Qaida. The Customs Service analysis identified anomalies in the packing weight, shipping weight and the reported value of the shipped honey, which may be indicative of trade-based money laundering or terrorist financing.

4. USE OF CREDIT CARDS

While I cannot comment on ongoing investigations into credit card usage, in connection with several regulatory provisions of the USA PATRIOT Act, we are exploring whether whether and what type of further regulatory action is warranted.

5. NARCOTICS TRAFFICKING

From our experience with terrorist groups, we know that some use narco-trafficking to support and fuel their militant activities. We also know that the portion of Afghanistan that the Taliban previously controlled produced at least three-quarters of poppy in the world and that al-Qaida members may have been involved in the heroin trade.
Green Quest and the Customs Service will continue to pursue narcotics investigations for any terrorist related links to further disrupt the funding of any future acts of terrorism against the United States.

METHODS OF MOVING MONEY

Terrorist groups, including al-Qaida, use different means of moving money to support their respective organizations. This money movement around the world, which largely still relies on traditional wire transfers, provides the footprints to where sleeper cells lie and allows us to attempt to disrupt those fund flows. Like other criminal organizations, terrorist groups use various means to move money. The following is a brief summary of ways in which money may be moved to terrorist organizations.

1. USE OF CORRESPONDENT ACCOUNTS AND OFFSHORE SHELL BANKS

There is some evidence to indicate that those who support terrorist groups use shell banks and companies and perhaps correspondent accounts to collect and move money. On November 7, 2001, the Treasury Department listed Bank al-Taqwa, a Bahamian-based shell bank, as a terrorist financing source. In 1997, it was reported that the $60 million collected annually for Hamas was moved to accounts with Bank Al Taqwa. As of October 2000, Bank Al Taqwa appeared to be providing a clandestine line of credit to a close associate of bin Laden and as of late September 2001, bin Laden and his al-Qaida organization received financial assistance from the chairman of that bank.

The Treasury Department continues to monitor the use of shell bank, shell companies, and correspondent accounts to move illicit funds or funds directed for terrorist financing purposes. Though Bank Secrecy Act (BSA) data, including Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs), reflects documented use of correspondent accounts and shell entities for money laundering purposes, it is difficult, without knowing more about the transactions, to link such suspicious activities to terrorism. Nevertheless, over the past twenty months, the Treasury's Financial Crimes Enforcement Network (FinCEN) has enhanced its support to law enforcement in the area of counter-terrorism by proactively analyzing Bank Secrecy Act (BSA) data to help identify activities indicative of the movement of funds that may be associated with terrorism. During this period, tactical information was developed and supplied to law enforcement and others for action, as appropriate. There are ongoing investigations of such companies and banks that I cannot discuss at this time. As part of our ongoing efforts with respect to this threat, FinCEN issued an advisory in January 2002 relating to the Republic of Nauru, pursuant to Section 313 of the USA PATRIOT Act, reminding banks of their obligation to terminate any correspondent accounts provided to foreign shell banks.

The banking sector plays an important role in monitoring and policing correspondent accounts and relationships with shell entities. Banks have actively reported information regarding activity in correspondent accounts that has proven valuable to law enforcement. In addition, some U.S. banks have voluntarily closed correspondent accounts with foreign-based banks when there have been suspicious wire transfers or "shell" entities involved. The reporting and record keeping rules contained in the Bank Secrecy Act ("BSA"), administered by FinCEN, create a paper trail to trace funds through the financial system. Information reported under existing suspicious transaction-reporting rules for banks is currently being forwarded to law

enforcement on an expedited basis through the establishment of a toll-free hotline operated by FinCEN.

The Treasury Department will continue to investigate the use of correspondent accounts and shell entities for terrorist financing for blocking purposes as well as to providing assistance to the Department of Justice.

2. INFORMAL VALUE AND UNDERGROUND BANKING SYSTEMS

Informal systems of moving money may be used by al-Qaida and other terrorist groups operating in Third World countries to support related organizations, sleeper cells, or supporters. One system of transfer is called "hawala" which operates on trust, guaranteed anonymity, outside traditional regulation and with virtually no paper trail. Operators engaged in this system deliver money across borders without physically moving it–assured the account will be settled by money or material goods returned in a future reverse transaction. Used widely in the Middle East and South Asia for centuries, there are indications that the system is being exploited by Al-Qaida and other terrorist organizations.

As mentioned above, on November 7, 2001, the Treasury Department blocked the assets of the al-Barakaat network, which was a global money remitting company being used by Usama bin Laden to support terrorist activities. Though the operations of Al-Barakaat in the United States relied on traditional banking systems, internationally it operated as a hawala network that allowed for funds to be funneled into Somalia through Dubai. This hawala network was not only used to finance bin Laden's organization, but also to provide logistical support for his network. Our actions put that hawala network out of business.

At this stage, FinCEN is examining non-traditional money remittance systems, such as hawala, because funds have the potential of being moved anonymously. In an effort to broaden its understanding of alternate remittance systems, FinCEN is forming an Alternate Remittance Branch which will be responsible for the analysis of BSA data and other information to identify mechanisms and systems used by criminal organizations to move operational funds in support of domestic and international activity. Analysis will focus initially on Informal Value Transfer Systems (IVTS) such as hawala, hundi and other Asian and South American systems as a potentially key but inadequately understood methodology for funds movement; development of indicators of IVTS use by criminal organizations to support law enforcement initiatives to combat criminal activity; and identification of policy implications of IVTS for law enforcement and financial regulators. Analysis will expand to include identification of the methods by which IVTS intersects with regulated funds transfer systems, and then identification of criminal funds movement methodologies based entirely on the legitimate financial industry.

The branch will be responsible for monitoring law enforcement support activities provided by FinCEN as a whole in order to identify trends and patterns in financial or fund raising activities. Strategic products will include trend and pattern analysis; industry/technology vulnerability analysis; methodology bulletins and advisories for law enforcement, regulators and the financial industry; threat assessments; and policy papers. The branch will work jointly and/or coordinate its analytic efforts with appropriate law enforcement and intelligence

organizations in the production of national threat assessments related to the funding of domestic and international criminal activity.

3. BULK CASH SMUGGLING

Law enforcement has always suspected that bulk cash smuggling is used by some terrorist organizations to move large amounts of currency. In response to the September 11th events, Customs utilized an existing outbound currency operation, OPERATION OASIS, and refocused its efforts to target twenty three identified nations involved in the laundering of money for terrorist organizations. After September 11th, Oasis was implemented at seven airports and five courier hubs around the United States. Customs' success with Oasis has led to the nationwide expansion of the operation.

To date, Customs Operation Oasis has seized $9,030,100. The Customs Service has primary jurisdictional authority for enforcing those regulations requiring the reporting of the international transportation of currency and monetary instruments in excess of $10,000 (Title 31 U.S.C. § 5316 et al.). The USA PATRIOT Act has enhanced the Customs Service's ability to investigate terrorist related financial crimes by making inbound and outbound smuggling of bulk cash a criminal offense (Title 31 U.S.C. § 5332(a)). By criminalizing this activity, Congress has recognized that bulk cash smuggling is an inherently more serious offense than simply failing to file a Customs report.

In short, we will continue to pursue all the means and methods that terrorists and their supporters could use to fund and funnel money intended for terrorist acts. Our vigilance will not waiver in this mission.

TOOLS AVAILABLE UNDER TITLE III OF THE USA PATRIOT ACT TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

Title III of the USA PATRIOT Act (PATRIOT Act) supplied Treasury with a host of new and important weapons to both systematically eliminate known risks to our financial system as well as to identify and nullify new risks that develop. The tragic events of September 11 have taught us three key lessons about financial crime: (1) although distinct in important respects, our ability to combat terrorist financing is inextricably linked with our ability to combat money laundering generally; (2) we must remain vigilant in our continuing efforts to identify the new ways in which criminals and terrorists will attempt to use our own financial system to fuel their enterprises; and (3) the ability of governmental entities to obtain and share financial information is critical to our success in identifying and bringing down terrorist networks. Title III of the PATRIOT Act reflects these lessons, providing us with the mechanisms, the authority, and the initiative to take the steps necessary to protect our financial system.

As this Committee is aware, Treasury, with the full cooperation and assistance of the various agencies and departments, continues the ambitious task of implementing the regulatory provisions of Title III under their tight deadlines. To utilize existing resources within the government, we created interagency working groups chaired by Treasury to help develop, and in some cases, draft the regulations. The cooperation and assistance that we have received has been

tremendous. Though the task is daunting, we accept the challenge. Today I repeat the pledge of Deputy Secretary Dam that Treasury will work diligently to attempt to meet these deadlines, while taking the time necessary to ensure that educated and informed policy decisions are made along the way. This is especially true for those provisions of the Act that support our financial war on terrorism. This is a learning process for us. As we focus on each section to draft regulations, we are better able to identify the vulnerabilities of our financial system and how best to eliminate them.

I will briefly highlight some of the significant provisions of Title III that form the foundation of the regulatory side of Treasury's fresh approach to combating money laundering and terrorist financing.

1. Critical Information-Sharing Provisions

One challenge in the financial war on terrorism is to maximize the use of existing information resources to identify the terrorist financing networks. Because different governmental entities and financial institutions maintain important information, we must have the ability to access that information and review it as a whole. Thus, some of the more important provisions of the PATRIOT Act are those permitting greater information sharing among law enforcement and other governmental entities. The information sharing provisions found in section 358 provided an immediate impact in our financial war on terrorism. With this expanded ability to access and share important financial information, law enforcement and the intelligence community are working together to identify better the financing mechanisms of terrorist networks. Section 358 expanded Treasury's ability to share Bank Secrecy Act information with the intelligence community, clarified that the Right to Financial Privacy Act does not preclude the use of financial information to combat international terrorism, and gave law enforcement and intelligence agencies access to credit reports when the inquiry relates to international terrorism.

Similarly, we will shortly issue regulations implementing section 314 of the Act, a provision in which the Congress allowed for and encouraged both the sharing of information among financial institutions as well as the sharing of information between law enforcement and financial institutions. We are confident that the ability of financial institutions to share information concerning suspected terrorists or money launderers will allow the financial institutions—the ones who are uniquely positioned to identify risks early—to work together, discuss their suspicions, and notify law enforcement of potential criminal activity at an early stage. Moreover, while we are still developing our proposal for sharing information between law enforcement and financial institutions, it is clear that open and developed channels of communication are essential. Along with FinCEN's development of a highly secure computer network under section 362, we look to improve the timing and efficiency of information sharing to maximize our ability to identify and respond to threats to our financial system.

With this new information sharing authority, however, comes the responsibility of ensuring that important privacy interests are not sacrificed. A fundamental principle of Treasury's implementation strategy is to respect these privacy interests while achieving our goal of eliminating risks of money laundering and terrorist financing.

2. The Systematic Elimination of Known or Unacceptable Risks

The approach of this Congress to money laundering is as bold as it is simple: identify risky financial practices and accounts at the outset and deny them access to our financial system. Correspondent accounts maintained in the U.S. by foreign banks, under certain circumstances, form the channel through which illicit funds find their way into our system. The public record is replete with evidence of their abuse in connection with money laundering. Thus, eliminating the known risks associated with correspondent accounts was the genesis for several provisions of Title III.

For example, Section 313's prohibition on U.S. financial institutions maintaining correspondent accounts for foreign shell banks and section 312's requirement that financial institutions apply enhanced due diligence when maintaining correspondent accounts for foreign banks located in jurisdictions lacking sufficient anti-money laundering regimes both require financial institutions to minimize the risks associated with correspondent accounts. Section 313 in particular is a bold step forward, sending a strong message about our commitment to cutting off unregulated foreign shell banks. Treasury has already provided guidance to U.S. financial institutions on how to comply with section 313. We will issue a final rule after we have reviewed comments submitted. By the April deadline, Treasury intends to issue regulations setting forth the due diligence procedures required under section 312.

Private banking accounts have likewise proven to present risks of abuse, such as in the *Salinas* case. Under section 312, such accounts for foreign individuals, especially accounts maintained for senior political figures or their family members, are subject to enhanced due diligence procedures by financial institutions, including the identification of the source of funds. Due diligence policies for private banking accounts will also be addressed in regulations under section 312. Similarly, the GAO report on the activities of Raul Salinas described the danger of concentration accounts in which clients' funds are commingled without linking the client to the funds. Under section 325, Treasury and bank regulators are working to ascertain whether regulations governing the use of concentration accounts are needed. Although we have not yet seen the abuse of these accounts in our terrorist financing investigations, elimination of these risks may be appropriate to ensure that they are not abused in the future.

This systematic approach to avoiding unreasonable risk is also embodied in two other important provisions of Title III: sections 326 and 352, which require customer identity verification and anti-money laundering programs, respectively, for all financial institutions. These provisions in particular will allow Treasury to close loopholes in our anti-money laundering regime and make certain that as terrorists and money launderers move toward less traditional financial institutions, they will not be able to avoid our regulatory controls. Treasury is moving aggressively to implement both sections, paying particular attention to financial institutions such as the insurance industry, the mutual fund industry, credit card companies and others that are not currently subject to Bank Secrecy Act requirements. We intend to protect our financial system by preventing migration to these and other unregulated industries. Through this process in particular, however, we are carefully educating ourselves about the industries in order

to derive sensible regulations that accomplish our objectives without imposing undue or unnecessary regulatory burdens.

Also, section 371 addressed the known risks associated with the smuggling of bulk cash and currency by making it an offense under Title 31 not to declare amounts in excess of $10,000 to the Customs Service. With lead responsibility for ensuring the safety of our borders, and primary authority for enforcing section 371, such provisions further aid the Customs Service in its efforts to disrupt terrorism. As noted, this provision has already netted substantial seizures.

3. Authority to Identify and Respond to Specific Risks

Equally as important to a comprehensive anti-money laundering regime is the ability to identify specific risks and take steps necessary to eliminate it. Various provisions in Title III help us to do just that. A cornerstone of the Bank Secrecy Act is our reliance on financial institutions notifying us of suspicious activities. Title III emphasizes the expansion of suspicious activity reporting by directing Treasury develop regulations for securities brokers and dealers, and authorizing such regulations for futures commission merchants, commodities trading advisors, and commodity pool operators. This is not only consistent with Treasury's implementation goal to eliminate regulatory arbitrage, but also provides law enforcement with an increased capacity to identify threats. Similarly, section 365—a provision that Treasury implemented four months ahead of its statutory deadline—provides Treasury and law enforcement with access to currency reports filed by non-financial trades or businesses, a form previously difficult to obtain in light of IRS confidentiality restrictions. Because non-financial trades and businesses were under an existing obligation to file such reports with the IRS, Treasury issued a regulation permitting the filing of a single form to satisfy both statutory requirements.

The provision that best enables Treasury to respond to specific, identified threats is section 311, which authorizes the Secretary of the Treasury to require financial institutions to impose graduated, proportionate measures against a foreign jurisdiction, financial institution, class of transaction, or account designated a primary money laundering concern. The special measures range from increased record-keeping requirements to prohibiting certain types of correspondent or payable through accounts. The statute requires Treasury to define certain key terms in section 311 by regulation. Because some of those same definitions are incorporated in section 312 of Title III, Treasury intends to define such terms in April in conjunction with the regulation outlining the due diligence requirements of section 312. Given the need to define key terms and the significance of naming a jurisdiction or financial institution a primary money laundering concern, Treasury is proceeding cautiously. Care must be taken to assemble sufficient evidence to support the designation and to make sure that the designation will not actually undermine our overall anti-money laundering or anti-terrorist financing strategy. Furthermore, the Secretary of the Treasury is required to consult with both the Attorney General and the Secretary of State prior to making any designation. We are now working on internal procedures for making designations that will ensure compliance with the consultation requirements while still enabling us to respond quickly to identified threats.

Finally, under section 319(b), the Secretary of the Treasury has the authority to issue administrative subpoenas to foreign banks maintaining correspondent accounts in the U.S. for documents related to those accounts, regardless of whether the documents are located in the U.S. Treasury has already issued interim guidance and a proposed rule covering the record-keeping portion of this provision. Given the potential impact of this provision on existing forms of information sharing between the U.S. and foreign governments, such as mutual legal assistance treaties, Treasury is looking to create internal procedures for exercising that authority with due regard for existing practices.

IDENTIFIED LOOPHOLES IN THE ANTI-TERRORIST FINANCING OR ANTI-MONEY LAUNDERING REGIME

As we continue to expand our efforts to undermine the financial underpinnings of terrorism, we learn more about the vulnerabilities of our system. Through the process of analyzing the applicability of the various provisions of Title III to the wide range of financial institutions and drafting implementing regulations, we learn more about how our regulatory regime can be used to eliminate those vulnerabilities. To this point, our focus has been, first and foremost, to locate and seize terrorist assets in order to prevent any further attacks. With regard to the PATRIOT Act, we have spent our time doing everything we can to meet the aggressive implementation deadlines. As Deputy Secretary Dam noted two weeks ago, we have not yet identified a need for additional legislation and, correspondingly, we have not identified any obvious loopholes in the forthcoming regulatory regime. But I stress that we are only at the beginning of the process of implementing regulations; thus, we may discover loopholes as we work through the issues.

We are especially aware of the need to carefully examine the proposed regulatory regime being imposed on those entities not previously subject to Bank Secrecy Act regulation. These include, for example, the insurance industry and the commodity futures industry. At this moment, we are working with industry representatives to understand how they operate, how they can best be regulated under the Bank Secrecy Act, and whether we have the necessary statutory authority.

Also, as I discussed previously, we are concerned with the ability of alternative remittance systems or informal money transfer systems to avoid regulation. Section 359 of the Act requests that Treasury notify Congress in October 2002 of the need for additional legislation. With FinCEN's initiatives in this area, Treasury will be well positioned to offer suggestions. We look forward to continuing to work with this Committee as issues develop.

CONCLUSION

I was heartened to read the words of Committee Chairman Michael G. Oxley regarding this hearing when he stated the following: "Make no mistake -- we are in this battle against terrorist financing for the long haul." Indeed, as President Bush has stated on numerous occasions, this is a long-term war that will require us to uproot the networks of terror. As part of this war, the battle against terrorist financing is a long-term mission for the Treasury Department and the entire U.S. government. We must work tirelessly as a government to choke the flow of

funds so as to prevent further acts of terror such as those we witnessed on September 11th. Ours is a long-term campaign to save lives by denying the terrorists the funds they need to train, to plan, to travel, to hide, and to attack. By denying these evil doers dollars and yen, we are depriving them of bullets and bombs.

This is a war we must win, with every tool at our disposal, because there is no other alternative. I thank you for your support. I will be happy to answer any questions you may have.