S. HRG. 109–1073

EXAMINING TREASURY'S ROLE IN COMBATING TERRORIST FINANCING FIVE YEARS AFTER 9/11

HEARINGS

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

ON

WHERE THE GOVERNMENT HAS PROVED SUCCESSFUL, LESS THAN SUCCESSFUL, AND WHAT IT HAS LEARNED AS A RESULT TO IMPROVE ON ITS EFFORTS TO COUNTER THE FINANCING OF TERRORISTS, WHETHER STATE-SPONSORED OR NOT, AS WELL AS THOSE SEEKING WEAPONS OF MASS DESTRUCTION

TUESDAY, SEPTEMBER 12, 2006

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.access.gpo.gov/congress/senate/senate05sh.html

U.S. GOVERNMENT PRINTING OFFICE

50–301 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

RICHARD C. SHELBY, Alabama, *Chairman*

ROBERT F. BENNETT, Utah
WAYNE ALLARD, Colorado
MICHAEL B. ENZI, Wyoming
CHUCK HAGEL, Nebraska
RICK SANTORUM, Pennsylvania
JIM BUNNING, Kentucky
MIKE CRAPO, Idaho
JOHN E. SUNUNU, New Hampshire
ELIZABETH DOLE, North Carolina
MEL MARTINEZ, Florida

PAUL S. SARBANES, Maryland
CHRISTOPHER J. DODD, Connecticut
TIM JOHNSON, South Dakota
JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
EVAN BAYH, Indiana
THOMAS R. CARPER, Delaware
DEBBIE STABENOW, Michigan
ROBERT MENENDEZ, New Jersey

WILLIAM D. DUHNKE *Staff Director*
STEVEN B. HARRIS, *Democratic Staff Director and Chief Counsel*
SKIP FISCHER, *Senior Staff Professional*
JOHN V. O'HARA, *Senior Investigative Counsel*
TRAVIS TEDROW, *Legislative Assistant*
STEPHEN R. KROLL, *Democratic Special Counsel*
JOSEPH R. KOLINSKI, *Chief Clerk and Computer Systems Administrator*
GEORGE E. WHITTLE, *Editor*

C O N T E N T S

TUESDAY, SEPTEMBER 12, 2006

WITNESSES

EXAMINING TREASURY'S ROLE IN COMBATING TERRORIST FINANCING FIVE YEARS AFTER 9/11

TUESDAY, SEPTEMBER 12, 2006

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met in room SD–538, Dirksen Senate Office Building, Hon. Richard Shelby, Chairman of the Committee, presiding.

OPENING STATEMENT OF SENATOR RICHARD SHELBY

Chairman SHELBY. The Committee will come to order.

Five years ago yesterday the United States was attacked and our nation was changed forever. On that day, we were united in our shock and horror as we watched people we knew meet an unimaginable fate. As the days passed, however, our collective anger and outrage gave way to a national determination to see our enemy for who they really were and bring them all to justice.

With a unanimous sense of urgency, the instruments of the Federal Government were marshaled toward that end. Both the President and the Congress worked hand in hand to not only find those responsible, but also to ensure, to the best of our ability, that it would never happen again. One component of that joint effort was to combat the means by which terrorist organizations and their supporters raised and moved the money required to carry out their attacks.

Since September 11, 2001, this Committee, the Committee on Banking, has conducted a series of hearings into the Federal Government's structure and diligence in waging the war against terror financing, as well as its criminal component, money laundering. During this time, a number of banks and other financial institutions have continued to violate Federal laws and regulations intended to prevent money laundering and terror financing.

In addition, the issue of State support for terrorism is a continual reminder of the scale of the challenges that lie ahead. There is no question, then, that there have been successes in the effort at impeding the flow of money used to fund terrorist operations. Cooperation with other nations and the financial services industry have seriously reduced the flow of money to organizations like Al Qaeda and Hamas.

International charities, once a key source of illicit revenue are now monitored much more closely, and in the instances of those

found to be actively supporting terrorist organizations are shut down. Much remains to be done, however. While we must continue our current efforts to stop the flow of money to terrorists, we must be mindful of our enemies' ability to adapt and to defeat our efforts.

For example, charities closed by governments have resurfaced under new names. Exploitation of formula banking systems have been replaced by the increasing use of buck cash couriers.

And of particular concern to this Committee, the use of shell and front companies continue to constitute a serious weakness in even our own anti-money laundering and terror finance regulatory regimes. This hearing continues the Banking Committee's examination of the structure of the Federal Government to combat terror financing, as well as the challenges confronting us abroad.

Today we will focus on the Department of Treasury. A future hearing, as part of our ongoing oversight, will include a broader spectrum of agencies with responsibilities for combating terror financing and money laundering.

For 5 years we have been spared another attack, and it is not because our enemies no longer have an interest in attacking us. Quite the contrary. They hope to inflict even greater damage the next time. Five years can feel like a long time, memories fade, life goes on, and we tend to get complacent. Al Qaeda is not complacent. They plan every day for the next attack and we must continue to do everything within the law to stop it.

Since 9/11, the Department's increased focus on combating terror finance has been a work in progress. We will hear today about that progress from key officials from the financial front war on terror.

Daniel Glaser is the Deputy Assistant Secretary for Terrorism Financing and Financial Crimes.

Robert Werner is Director of the Financial Crimes Enforcement Network, which is responsible for the administration of the Bank Secrecy Act, one of the key statutory and regulatory regimes for combating money laundering and terror finance.

Adam Szubin is the Director of the Office of Foreign Assets and Control, which administers and enforces U.S. economic sanctions.

Eileen Mayer is the Director of Fraud and Bank Secrecy Act at the Internal Revenue Service's Small Business, Self-employment Division.

We thank all of you for your service. We thank you for appearing before the Committee today. Senator Sarbanes sends his regret. He is unable to be with us today, but we have Senator Hagel and I am sure we will have others.

Senator Hagel, any opening statement?

Senator HAGEL. No, Mr. Chairman. Thank you.

Chairman SHELBY. All of your prepared statements will be made part of the hearing record.

We will start with you, Mr. Glaser.

STATEMENT OF MR. DANIEL L. GLASER, DEPUTY ASSISTANT SECRETARY OF TERRORIST FINANCING AND FINANCIAL CRIMES, DEPARTMENT OF TREASURY

Mr. GLASER. Chairman Shelby, Senator Hagel, distinguished members of the Committee, thank you for the opportunity to speak

today about the Treasury Department's efforts and achievements in the financial war on terrorism, and to discuss the challenges that lay ahead. This Committee has played an important role in ensuring that we have the necessary authorities to combat terrorist financing.

Indeed, over the last 5 years, we have witnessed a revolution in the role the finance ministries can play in international security affairs. We have increased substantially our understanding of vulnerabilities in the international financial system, and how terrorists and other illicit financial——

Chairman SHELBY. Can you bring your mic just a little closer to you, please? Thank you.

Mr. GLASER. We have increased substantially our understanding of vulnerabilities in the international financial system, and how terrorists and other illicit financial networks exploit those vulnerabilities.

At the same time, we have steadily enhanced our skill and sophistication in applying the financial tools that we have at our disposal to close those vulnerabilities, disrupt and dismantle illicit financial networks, and apply pressure on the States that provide terrorists support and comfort.

The U.S. has led the way in this development of financial authorities through the establishment of the Treasury Department's Office of Terrorism and Financial Intelligence, the first office of its type in the world. TFI's mission is to marshal the Department's policy, enforcement, regulatory, and intelligence functions in order to sever the lines of financial support to international terrorists, WMD proliferators, narcotics traffickers, and other threats to our national security.

We seek to meet this responsibility by striving to reach two overarching goals. First, identifying and closing vulnerabilities in the U.S. and international financial system. And second, identifying, disrupting, dismantling the financial networks that support terrorists, organized criminals, WMD proliferators, and other threats to international security.

My written testimony presents a comprehensive and strategic overview of our ongoing efforts to advance these two overarching goals. In assessing the effectiveness of our efforts over the past 5 years, it is clear that we are on the right track. We have elevated the costs, risk, and difficulty for terrorists to raise and move funds in support of their operations. We know that our actions are having a disrupting effect on the financial capabilities of terrorist cells and terrorist organizations.

Through a range of actions, initiatives, and authorities we have raised awareness and strengthened protective measures across the international financial system and vulnerable sectors like charities. We have also closed down terrorist financing sources, conduits, and support networks. These efforts have forced terrorists to devote more time, attention, and resources to reconstructing their financial organizational infrastructure and otherwise meet basic financial needs, and this means less time and resources to plan and execute terrorist attacks.

The success of our strategic approach in identifying and disrupting terrorists and their support networks is becoming increas-

ingly recognized by the international community. Growing support for targeted financial measures is evident at the United Nations, the Financial Action Task Force, various regional organizations, and an increasing number of our bilateral relationships. As the international community continues to look for effective ways to combat terrorists and other threats to international security, much of our current work is focused on working with these organizations and our counterparts in finance ministries around the world to facilitate greater capability in developing and applying financial measures to shut down terrorists and their support structures.

Recent developments in the international financial sector also reflect a growing recognition of the power of financial measures in disrupting terrorists and other international security threats. Through our strategic outreach efforts we have shown that Treasury's targeted financial measures, even if initially applied in a unilateral fashion, can be quite effective globally, in part because they unleash market forces. By highlighting risks associated with terrorist financing networks, their State sponsors, and corrupt financial institutions, our targeted financial measures encourage prudent and responsible financial institutions to make the right decisions about the businesses in which they are engaging.

Recognizing the risks inherent in doing business with terrorists and other illicit support elements, the Treasury has targeted through its financial authorities, financial institutions around the world have taken steps of their own to protect against these risks. These steps by foreign financial institutions include reconsidering the nature of their business relationships with high risk customers, such as North Korean and Iranian entities.

In fact, Treasury Under Secretary Levy and Assistant Secretary O'Brien this very week are in Europe and the Middle East respectively meeting with foreign finance ministries and financial sector authorities and private financial institutions discussing those very matters.

As we review the developments at Treasury since 9/11 it is clear that we have come a long way in reshaping Treasury's role to focus on closing down vulnerabilities in the international financial system and applying financial measures to disrupt to dismantle the networks that support terrorists and other international security threats.

I am grateful for the support that Congress has provided us as we have refined our mission under the development of TFI Treasury. I will be happy to answer any questions.

Thank you, Mr. Chairman.

Chairman SHELBY. Mr. Szubin. Is it Szubin? How do you say it?

STATEMENT OF MR. ADAM J. SZUBIN, DIRECTOR OF THE OFFICE OF FOREIGN ASSETS CONTROL, DEPARTMENT OF THE TREASURY

Mr. SZUBIN. Yes, Sir. Szubin.

Chairman SHELBY. Szubin. I got it right. Thank you.

Mr. SZUBIN. Chairman Shelby, Senator Hagel, members of this Committee, thank you very much for this opportunity to discuss the role played by the Office of Foreign Assets Control, or OFAC, in combating terrorism since those deadly attacks of September 11.

Over the last 5 years this Committee has demonstrated its absolute commitment to combating terrorist financing and ensuring that the government has all of the necessary tools to do this work aggressively and appropriately. I am therefore particularly pleased to be here today to introduce myself to the members of this Committee and to thank you for your leadership and support.

In a way, it is fitting that this hearing marks my first public appearance as the Director of OFAC. Combating terrorist financing has been a principle focus of mine almost since that terrible day 5 years ago. My introduction to this area came as an attorney in the Justice Department's Federal Programs Branch, actually representing OFAC. Since then, I have worked on terrorist financing issues in the Deputy Attorney General's Office, and with Under Secretary Levy here at TFI.

I can assure you that, 5 years later, my colleagues across the government continue to display extraordinary focus, creativity, and passion in tracking and disrupting terrorist financing in all of its forms. Following the horrific events of September 11th, the President issued Executive Order 13224, authorizing the Secretaries of the Treasury and State to wield broad financial authorities against terrorist organizations and their support networks. In the 5 years since, OFAC has designated approximately 375 individuals and entities as supporters of terrorism, blocking their assets and, more importantly, cutting them off from the U.S., and often the international, financial system.

I would like to highlight just a few of our most recent actions. Last month, we designated overseas branches of the International Islamic Relief Organization, or IIRO, which is headquartered in Saudi Arabia, as well as Abd al Hamid Sulaiman Al-Mujil, the head of IIRO's branch in the Eastern Province of Saudi Arabia. These branch offices, while holding themselves out as purely charitable organizations, were bankrolling the al Qaeda network in Southeast Asia. We also took a string of recent actions to disrupt and undermine Hezbollah's financial network. The U.S. has, of course, long recognized Hezbollah as a deadly terrorist organization, but the recent fighting in Lebanon provided a stark reminder of just how dangerous and well-supplied this terror organization is. Two weeks ago, we designated the Islamic Resistant Support Organization, IRSO, a Hezbollah charity, that offered donors the option of earmarking their donations to equip Hezbollah fighters or to purchase rockets. Just last week, OFAC designated Bayt al-Mal and the associated Yousser Company, which together functioned as Hezbollah's unofficial treasure in Lebanon. These actions, driven by the excellent work of TFI's Office of Intelligence and Analysis exposed and struck at some of Hezbollah's most prominent financial entities. The world financial community is now on notice as to their true character. Of course, one cannot hope to apply effective financial pressure against a group like Hezbollah, so long as it maintains massive inflows of cash from a State sponsor of terrorism, in this case Iran. OFAC administers a range of sanctions against Iran, the worlds leading government sponsor of terror, aimed at limiting the regime's financial reach and pressuring it to cease its hostile and destabilizing activities.

We have historically allowed Iranian banks to access the U.S. financial system indirectly through third country intermediaries. This past Friday, OFAC action to cutoff Iran's Bank Saderat from even indirect access to the U.S. financial system. We took this action because Bank Saderat has been a significant facilitator of Hezbollah's financial activities and has served as a conduit between the Government of Iran and a range of Middle East terrorist groups.

One question frequently posed to OFAC is how meaningful are these actions when the U.S. acts by itself, and a target does not hold assets in the United States. Or, to put it another way, are unilateral actions effective?

As it turns out, even when we initially act alone, our sanctions can have a dramatic impact. There are two main reasons for this. First, to paraphrase an old saying, all financial roads today lead to New York. When a designated party in the Gulf, for example, tries to send money to Southeast Asia, that transfer will often pass through a United States bank, if only for an instant. The result is, typically, that these funds are frozen or blocked and that OFAC will receive a phone call or a blocking report.

In addition, it is important to remember that U.S. persons and branches situated abroad are also subject to U.S. law, and must comply with our regulations as if they were in the United States.

Our second force multiplier is that international financial institutions frequently implement our sanctions voluntarily, even when they are under no legal obligation to do so from their host countries. These institutions may be following our regulations and designations because they simply do not want to be hosting the business of a terror organization, even if it is permissible or they may be concerned of reputational harm. But whatever the cause, the OFAC list, as it is known, is being run on the computer screens of banks around the world.

As a result, our unilateral actions are anything but, and can have a decisive impact against terrorist supporters, WMD facilitators, and narcotics traffickers. In all of these arenas, OFAC is working hand in hand with the other organizations testifying today; with TFI's Office of Intelligence and Analysis and our interagency colleagues brought together under the leadership of Under Secretary Levy, our offices provide a range of financial authorities that allow us to take focused and effective action to disrupt, deter, and disable threats to our national security.

OFAC will continue to draw on all of its resources to keep our country safe. I look forward to continuing our work with you on these important issues, and I would be happy to answer your questions.

Chairman SHELBY. Mr. Werner.

STATEMENT OF MR. ROBERT W. WERNER, DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK

Mr. WERNER. Chairman Shelby and distinguished members of the Committee, I appreciate the opportunity to appear before you today to discuss the Financial Crimes Enforcement Network's ongoing initiatives in efforts to combat money laundering and terrorist financing in the post-9/11 world.

This hearing is especially appropriate following yesterday's fifth anniversary of the vicious terrorist attacks against this country. In fact, my difficulties getting to today's hearing due to a suspicious vehicle causing the closing of Constitution Avenue is just another reminder of the world we live in today.

As the Director of finCEN, which is the agency responsible for administering the Bank Secrecy Act, the United States primary anti-money laundering, counterterrorist financing regulatory regime, I welcome the opportunity to work with the members of this Committee in our united fight to safeguard the U.S. financial system against financial crime.

I am also pleased to be testifying with my colleagues from other components of Treasury. Each of these offices plays an important role in the global fight against money laundering and terrorist financing, and our collaboration on these issues has greatly improved the effectiveness of our efforts.

As I discuss in greater detail in my written testimony, FinCEN has aggressively worked on multiple fronts to fulfill its mission, which is to safeguard the financial industry from illicit financial activity. This is achieved through a broad range of interrelated activities, including administering the Bank Secrecy Act, supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of financial intelligence, and building global cooperation and technical expertise among financial intelligence units throughout the world.

The BSA data received through currency transaction reports, suspicious activity reports, and other forums have proved to be highly valuable to our law enforcement customers who use the information on a daily basis as they work to investigate, uncover, and disrupt the vast networks of money launderers, terrorist financiers, and other criminals.

FinCEN's ultimate goal is to increase the transparency of the U.S. financial system so that money laundering, terrorist financing, and other economic crime can be deterred, detected, investigated, prosecuted, and, ultimately, prevented. Our ability to tie together and integrate our regulatory, international, and law enforcement efforts assists us to achieve consistency and effectiveness when administering the Bank Secrecy Act.

I understand the Committee would like to discuss a number of issues today, so in the interest of time, Mr. Chairman, I would like to conclude by thanking you and the members of this Committee for all of the support and guidance you have provided over the past 5 years, and I look forward to answering your questions.

Thank you.

Chairman SHELBY. Ms. Mayer.

STATEMENT OF MS. EILEEN C. MAYER, DIRECTOR, FRAUD/ BANK SECRECY ACT OF SMALL BUSINESS/SELF EMPLOYMENT DIVISION, INTERNAL REVENUE SERVICE

Ms. MAYER. Good morning Chairman Shelby, Senator Hagel, and Senator Martinez. I am pleased to be with you this morning to discuss the IRS role in administering the BSA and helping to detect and disrupt terrorist financing.

As you know, IRS is responsible for examining for BSA compliance all financial institutions currently not examined by a Federal functional regulator. These entities include money service businesses, such as check cashers, wire remitters, and issuers of traveler's checks, casinos, certain credit unions, dealers in jewelry and precious metals, and certain insurance companies.

The largest of these groups is the MSBs. No one is sure just how big the universe of MSBs may be or how many of them are required to register with FinCEN under the BSA. What we do know is that currently there are more than 27,000 registered MSBs.

The IRS is committed to our important role in enforcing the BSA. As evidence of that, in late 2004, we created the Office of Fraud/Bank Secrecy Act within the Small Business Self-Employed Division. That is the office I now head. The creation of this organization includes the dedication of a full-time staff of field agents whose sole responsibility is to examine MSBs, casinos, and other entities covered by the BSA but not monitored by traditional Federal regulators. Today there are approximately 350 BSA examiners in the field.

With the full support of the Commissioner, we are working diligently to increase the field staff to 385 and expect to be at that level in the not too distant future. Then we will work to keep the number there.

This dedicated workforce is reflected in the number of Title 31 exams we have been able to conduct. In fiscal year 2005 we examined 3,680 MSBs. This year, we have far exceeded that total and expect to examine over 6,000 by the end of the fiscal year. In addition, we have put special emphasis on our case building process, which was redesigned and launched at the beginning of this fiscal year.

Because we could never examine all entities that fit into the categories of non-bank financial institutions over which we have jurisdiction, case building based on risks is essential. We are also leveraging our resources with those of the States. In late April, Commission Everson announced agreements with 33 States and Puerto Rico to begin sharing BSA information. These agreements allow the United States and participating States to join forces and share information as we work to insure that MSBs are complying with their Federal and State responsibilities.

We recognize, Mr. Chairman, that the money service business industry provides valuable financial services, especially to individuals who may not have ready access to the formal banking sector. It is longstanding Treasury policy that a transparent, well-regulated money service business sector is vital to the health of the world's economy.

We find it regrettable that the compliant MSBs are being rejected by banks over fears of potential noncompliance with BSA requirements. Our examinations do not support those fears. Of the thousands of MSBs we have examined in the last two fiscal years, there has been only a very small percentage that examiners believed merited referral to FinCEN for consideration of civil penalties or the IRS CI for possible criminal penalties. Indeed, for the most part, the violations that we find in the MSB industry are

minor or technical in nature and can be corrected easily, and usually are.

Finally, I would like to quickly address BSA Direct and what we are doing now that FinCEN has issued a permanent stop work order on its construction of what they call the retrieval and sharing portion of the system. Our people have been working very hard with FinCEN since early this year to transfer all of their law enforcement customers to the new IRS Currency, Banking, and Retrieval web-based system, known as Web CBRS.

CBRS houses all of the BSA and U.S.A. PATRIOT Act data, which is filed pursuant to FinCEN regulations. The IRS began developing a web application for CBRS approximately 5 years ago. The implementation of Web CBRS is on or ahead of schedule. On September 30th, the IRS intends to take the old integrated data base management system offline. At that point, Web CBRS will be the only firsthand source of the Bank Secrecy Act and U.S.A. PATRIOT Act available.

We are committed to continue our cooperation with FinCEN to improve the usefulness of BSA data that is available through Web CBRS. The key to this process is having clear requirements from FinCEN and the funding for development.

Mr. Chairman, I appreciate being asked to speak this morning, and I am happy to respond to any questions you or the Committee may have.

Chairman SHELBY. Thank you. I am going to first recognize Senator Hagel.

I have a lot of questions for the record, but I will—Senator Hagel.

Senator HAGEL. Mr. Chairman, thank you.

And to our witnesses, we appreciate your efforts and good work and please convey to your colleagues our appreciation, as well.

Mr. Szubin, you noted in your testimony, which has received considerable attention in the press, that the Treasury has suspended the ability of the Iranian-owned bank to deal with any of our U.S. financial system organizations.

My first question about this issue, is this an expansion of the current sanctions regime on Iran?

Mr. SZUBIN. Yes, Sir.

Senator HAGEL. Why was this action not taken prior to your announcement last week?

Mr. SZUBIN. The timing of any of our actions of this nature is obviously driven by a range of factors, which are going to include intelligence, foreign policy, and, of course, our regulatory programs here at Treasury.

We took this action on Friday because we have particular concerns about this bank, Bank Saderat, acting, as I mentioned, as a facilitator of Hezbollah's financial activity and, although the information is not information I can discuss in this setting, it is compelling and disturbing—and acting as a conduit for the government of Iran to support groups like, of course, Hezbollah, but also Hamas, Palestinian Islamic Jihad, and the PFLPGC.

On that basis we have said that Bank Saderat can no longer have any dealings with anyone in the United States, even indirect.

That will mean, also, that Bank Saderat will be cut off from its ability to access the U.S. dollar.

Senator HAGEL. And has Treasury planned to pursue similar sanctions against Iranian financial institutions?

Mr. SZUBIN. I cannot discuss what we may or may not be planning for the future. What I can say is that, as Mr. Glaser mentioned, our Under Secretary Stuart Levey is, at this moment, in Europe, and our Assistant Secretary, Pat O'Brien, is in the Gulf discussing with our allies the range of actions that we can be considering together to take against the government of Iran.

Of course, Iran's behavior, in terms of both supporting terrorism and its WMD pursuit is something that we believe should be of concern to all civilized nations. It is tremendously more impactful when we act in a unified form. That is what is driving those trips that I mentioned. It is also—I believe this Saderat action is going to be high up on the list of actions that they will be discussing with their counterparts.

Senator HAGEL. Would you say that our allies are in complete agreement with our actions on this particular decision, as well as other actions that may be taken regarding financial institutions in Iraq?

Mr. SZUBIN. Our action against Bank Saderat is obviously very fresh. It was just taken this past Friday. I will be very interested to hear the reports from Under Secretary Levey and Assistant Secretary O'Brien as to our allies' responses and reactions to it.

I can say that I believe our allies do share our concerns about the threat that is behind this action, namely Iran's support for terrorist groups and Iran's pursuit of WMD. Obviously, those two trends that Iran continues to follow are disturbing each in their own right, but, when merged together, present the prospect of Iran supplying a weapon of WMD to terrorism, which is our paramount concern. And I think our allies are sensitive to that, as well.

Senator HAGEL. Would you single out any of our allies who have not been particularly helpful?

Mr. SZUBIN. I would not want to do that. No, Sir.

Senator HAGEL. Because that is not the case?

Mr. SZUBIN. Well, as I said, I think we have received broad support. I think that support has extended throughout the world. Under Secretary Levey has been traveling on previous trips to meet with counterparts in the Gulf, in Europe, in Asia, and I can tell you, there is quite grave concern throughout the world about what is going on there.

Senator HAGEL. What about China and Russia?

Mr. SZUBIN. I, myself, have not been on those trips, but I would actually defer to Mr. Glaser who has been on recent trips to discuss some of these issues.

Senator HAGEL. Mr. Glaser.

Thank you.

Mr. GLASER. Thank you, Senator.

I think Director Szubin is exactly correct. There is an increased sensitivity throughout the world, I think among all governments, that Iran is using the international financial system to fund both its WMD programs and to engage in terrorist financing, and to en-

gage in other destabilizing activities throughout the world, and particularly in the Middle East.

I think what you are seeing now with the Bank Saderat action being the first action, and we are, of course, going to be continuing to monitor the international financial sector to look for other potential actions that there is an increased focus now on taking action to deal with that. We are just really beginning this effort to put direct pressure on illicit Iranian activity in the international financial system.

I think that the jury is very much still out on achieving a complete international consensus on it, but I do think the initial signs are very positive. I think the important point to emphasize here, and what is really unique and innovative about what we are trying to do right now is not only the outreach we are doing to international and to foreign governments, but the direct outreach that we are doing to the international financial sector, to the actual financial institutions and you are seeing a market reaction to that. Banks such as UBS have publicly stated that they are going to be cutting down on their Iranian business. Other banks in Europe have publicly stated that they are going to be cutting on their Iranian business.

And what you are seeing is a market reaction to information that we are putting out there and actions that we are taking that is going to make it increasingly difficult for Iran to do business anywhere, be it in Europe, be it in Asia.

As I said, we are just at the beginning of this, but I think this is a very promising strategy. And, as Adam said, it is precisely what the Under Secretary and Assistant Secretary are pursuing right now in Europe and in the Middle East.

Senator HAGEL. Do we communicate this in any way to Iran, decisions we are contemplating, decisions we are making, decisions we are going to make?

Mr. GLASER. Well, I suppose that would be a question that the State Department can answer better than I can. We certainly——

Senator HAGEL. The Treasury does not.

Mr. GLASER. We certainly do not give Iran advance notice when we are going to take action to disrupt their financial networks. No, absolutely not.

Senator HAGEL. Anyone else want to add to this?

Thank you, Mr. Chairman.

Chairman SHELBY. Thank you.

Senator Martinez.

STATEMENT OF SENATOR MEL MARTINEZ

Senator MARTINEZ. Mr. Chairman, thank you very much.

Mr. Glaser, I just want to follow up on Senator Hagel's question. How can we effectively have a sanctions regime if it is not applied by other nations, particularly the significant trading partners of Iran?

Mr. GLASER. Well, it is a great point. And certainly anything that we do becomes more effective the more countries that do it, and we work very, very hard to work multilaterally with our partners and allies. We are working on that in the United Nations right now.

As I have said, we have very, very high level Treasury officials who are in Europe and the Middle East. Secretary Paulson will be in Singapore at the bank fund meetings next week. This is very, very high on his agenda, as well. We are doing everything we can to achieve international action on this.

That said, we believe that the actions that we take can have a direct impact even when they are initially applied unilaterally for a couple of reasons. I think Director Szubin hit on a couple of these. First of all, we do control access to dollar clearing, and when we take action with respect to a particular financial institution that conducts international transactions, that is a very, very powerful action and it is a very important thing that we have the ability to take away from them and make it—again, disrupt their activity. And that is what we are trying to do; we are trying to disrupt financial networks.

Second, I do think it is important to shine the light on these bad actors. And that leads into what I was discussing with Senator Hagel, which is that the new dynamic that we see is that the actions that we take unleash market forces and create dynamics within the international financial system that makes it increasingly difficult for bad actors such as Iran to find efficient and effective financial services.

I think you see that most directly with the actions we have taken with respect to North Korea and North Korean entities. And I think what you are finding is a lot of the systemic structural things that we have worked so hard to create over the years, the anti-money laundering compliance programs, the counterterrorist financing compliance programs, the focus on the risk-based approach. All of this now is feeding into that system, and you have a situation in which we can take actions here and it has a ripple effect throughout the global community. And I think we are becoming more and more sophisticated in how we apply that.

Senator MARTINEZ. Yes, that brings another point, because a lot of bankers in my State of Florida complain that some of the anti-money laundering compliance is overly burdensome and, frankly, disruptive of normal business transactions because of the amount threshold being so low and things like that.

What can I say to those bankers in terms of the necessity for the continuing of the same level of regiment, and is there any opportunity for there to be relief in some sense which does not impair our overall effort?

Mr. WERNER. Let me try and handle that, OK? We administer—FinCEN administers the Bank Secrecy Act.

We have had extensive engagement with many of your constituents, and we have gone to conferences put on by FUBA and other trade groups. We recognize that this is a tension within the system, but I think that what we have begun to do is get better—the burden is obviously clear to the industry because they are the ones with grappling with implementing the risk-based approach. But we are getting better at doing is articulating the value that the government and that the industries are deriving from these systems.

It is really a two-tiered approach. The AML programs that the institutions are putting in place result in a prophylactic effect for those institutions, which is very, very important. And beyond that,

the programs also result in the collection and reporting of information through FinCEN to the U.S. Government. And that information has also proved to be extremely valuable, not only in terms of specific investigations and case work, but in understanding systemic vulnerabilities to the system, which has then been able to impact our regulations.

What we understand we need to do is to continue to assess and reassess that burden benefit balance. But going forward, what I think we need to recognize is that, post-9/11, a lot of the BSA compliances—it is a relatively young system. I think as we are working through a lot of the issues associated with it, we are getting to the point where it is being tailored in a way where institutions are going to understand how they can play their part while at the same time permitting legitimate business to flow through the system.

Senator MARTINEZ. It is a continuing source of complaints, and I understand that we are asking you to try to do two things. On the one hand, curtail the use of illegal funds for purposes that we do not want to see funded, but also to allow business these normal transactions to take place.

Mr. Szubin, I wanted to first of all commend you on the great work that your office has been doing as it relates to Cuba enforcement, which I think is an important consideration and one that had really been relegated to—maybe just to be ignored, but this Administration has had a prominent shift.

My question to you is, with all of the other responsibilities that you have, do you have sufficient personnel to cover all of the things that you are trying to do, because the world is complicated? Is it feasible? Is it possible? Are you sufficiently staffed to be able to undertake the mission that you have been given, which is incredibly important?

Mr. SZUBIN. Thank you, Senator. The world and the world financial system is, as you say, an increasingly complicated place, and we need to stay abreast with, if not ahead of, those who are trying to avoid all of the financial measures that we are putting in place, be they narco-traffickers, terrorists, or regimes that are under our sanctions programs.

We are pleased that the President's budget for fiscal year 2007 supports an OFAC request for significant resources for us to continue our work against terrorists and against State sponsors of terrorism, as well as against WMD proliferation, which are our two main focus areas.

We believe, with those additional resources, we will be able to continue to do our job effectively.

Senator MARTINEZ. Thank you, Mr. Chairman.

Chairman SHELBY. Thank you, Senator.

I have a number of questions I will get into in a minute, but following up in the theme of Senator Hagel, I saw the other day, and it was rather troubling to me, I believe it was announcement by Total, the large French oil company, that they had no intention of ceasing doing business in Iran. In other words, they were going straight into it.

And to do that, they are going to have some financing of some banking, probably some French banks. I know that is not the subject of this hearing today, but that is troubling because if we do not

have the support of our allies in all aspects, if it is sanctions, or money laundering, or everything else, then it makes your challenge that much greater. Although, I know in a lot of areas, we do, and a lot of it you are not at ease and should not talk about in a public hearing here today.

But having said that, I have got a number of questions for the record.

I will start with you, Mr. Werner.

The 9/11 Commission Report emphasized that quick access to financial information is necessary to identify and disrupt terrorist operations directed against the U.S. Cross-border, wire transfers contain a treasure trove of information we know is useful to counterterrorist investigators such as yourself. Today, we have learned from your testimony that FinCEN has completed at least its initial outreach on the cross-border issue to the financial community and law enforcement.

FinCEN has also learned lessons from the regimes used in Canada and Australia. It seems to me that capturing information from the hundreds of thousands—maybe millions, I do not know—of daily wire transfers is a much larger logistical and progressing challenge faced by either Canada or Australia because of the size of our financial institutions.

Is there an initial conclusion yet, the question is, that the process and technology is available to make the adjustment here? In other words, do you have the technology to do it? Do you need it?

Mr. WERNER. Mr. Chairman, you are quite right. Although Canada and Australia have found tremendous value in their cross-border——

Chairman SHELBY. They have——

Mr. WERNER [continuing]. Programs, the number of transactions——

Chairman SHELBY. They have been quite useful to us.

Mr. WERNER. It has. But the number of transactions that they deal with, as you point out, are considerably less than is involved in the U.S. system. I think that we estimate that we could have as many as 500 million transactions annually that would be captured by this requirement.

And so, being very mindful of that, as we have looked at the value, we also have tried to be very realistic about what it will take to build an infrastructure that can accommodate that kind of information. We believe it is feasible, but as we move our recommendations forward through Treasury, it is going to be very important for the Secretary and other policymakers in Treasury to, again, do that cost benefit analysis——

Chairman SHELBY. Do you have a timeline involved? You might not want to say, but——

Mr. WERNER. We hope as quickly as possible, because the schedule for implementing the program, if it goes ahead, is very aggressive. It is a complicated issue, and I think we forwarded only very recently our study——

Chairman SHELBY. Can you do that in-house? Do you have the personnel do that in-house, or will you have to reach out, or have you made that decision yet?

Mr. WERNER. We would not be able to implement that system with in-house. That would have to be through contracted services.

Chairman SHELBY. That is good.

Mr. Glaser, front companies. The trail of many financial crimes leads through front or shell companies, as you pointed out. These companies are routinely used, as well, for the illegal acquisition of military-sensitive technologies.

The Pakistani and former Iraqi nuclear weapons programs both relied on the use of front companies to evade restrictions or sanctions. The nuclear black market—Dr. Khan made extensive use of such companies. North Korean front companies played a central role in the counterfeiting and are still doing it—and money laundering activities.

More mundane financial crimes like that involving a trade-based laundering and tax evasion scheme involving Brazilian men utilized front companies in Delaware, Panama, and the British Virgin Islands.

Given the importance of front and shell companies to the successful execution of all manner of illicit activities, is it your opinion that Congress should consider measures to restrict their use, and how would we do this if we are working with you?

Mr. GLASER. Thank you for your question, Mr. Chairman.

I think you have touched on a very important issue, and I think that it is important for all of us to be focusing on this issue and sort of grappling——

Chairman SHELBY. Would you focus on that with the IRS, for example? You would be dealing with them.

Mr. GLASER. Sure. The question that you asked I would say has two parts to it. You discussed some foreign shell companies, and then shell companies domestically here in the United States.

I think on the foreign end of it—what the Treasury is trying to achieve—I think what the international community is trying to achieve is a level of transparency in the financial system that shell companies tend to work against. The designations that OFAC does are only made more effective if we know who is really behind these companies, and how we can get to the people who are actually manipulating the front companies and conducting their illicit activities through those companies. And that is not only true for Treasury designations, that is true for law enforcement activities.

What we try to do internationally is set international standards and assess countries against those standards to the FATF. I think that has been relatively successful, although there are clearly some holdouts. One of the main problems, frankly, is shell companies here in the United States. It is something that we have long been aware of. We frequently receive complaints about it from foreign law enforcement officials. It has been identified as a problem by the GAO. It has been identified as a problem, I think, very significantly, in the money laundering threat assessment that the U.S. Government just put out. I think probably the first time the U.S. Government has articulated that so clearly and emphatically.

The United States was just reviewed by the Financial Action Task Force, a 300-page assessment of our anti-money laundering regime, which was, by and large, very, very positive, and I think

deservedly so, though with some criticisms in it, as well. We are criticized, actually, fairly severely on the issue of shell companies.

So, I think that there is a growing recognition that this is something that we should all be looking at. In the money laundering strategy that we are going to be issuing very shortly we do address this issue. I do not think anybody is saying that we have any silver bullet, right now. One of the problems is that corporate law is not federalized in this country, so it becomes a State by State issue for us.

I think we do need to be doing more outreach with the States. I think we do, working with FinCEN, need to explore some of the opportunities that the Bank Secrecy Act might afford us. And I certainly think a dialog with Congress is also very important on looking at some other potential solutions.

So, I think you have put your finger on a very important issue. It is one that we are becoming increasingly focused on. Maybe it is overdue. I do think there are any number of solutions that we might have at our disposal for this.

Chairman SHELBY. Prepaid cards. It is a big business. Much has been made, of late, concerning this $64 billion prepaid card boom. $64 billion.

Of particular concern are so-called open system cards that can be used at almost any retailer, or even as ATM cards that not only can be replenished, but will allow someone to withdraw the amount put on the card anywhere in the world, is my understanding.

In one case, for example, a Mexican criminal caught at the border used stolen credit cards to transfer funds onto a prepaid card. I mean, they are very resourceful people. The question, then, here is whether those cards can be used for more frightening purposes. If they can be used for that, you know, they can be used for something else.

The 9/11 hijackers were identified by their bank accounts, card signatures, and wire transfers. Had those terrorists used prepaid cards to cover those expenses, would the government have been able to identify the terrorists today?

Mr. GLASER. Well, thank you again, Mr. Chairman——

Chairman SHELBY. Is that troubling to you, the use of these cards?

Mr. GLASER. Stored-value cards and other new payment systems are an important issue and I think that we need to focus on them for the same reason why we need to focus on shell companies, and that is because, if not set up properly, they could tend to reduce the level of transparency in the international financial system. And that, in turn, works against our ability to take effective action against money laundering, or terrorist financing, or WMD proliferation.

The thing with store-value cards and any of these new technologies is that they are very important commercial vehicles. They are very important. They are very efficient, useful financial tools that we want people to be using. So, we have to draw a balance between insuring that everyone has access to these useful financial commodities.

Chairman SHELBY. For legitimate reasons.

Mr. GLASER. For perfectly legitimate reasons. And that we have a regulatory structure.

I think that there are some examples in which you see new payment systems being created almost along the contours of our regulatory policy to try to find the cracks and holes in that. That is a constant examination that we are doing. Again, we are doing it internationally. I know Director Werner is doing this within FinCEN, and it is something that I know FinCEN is quite focused on.

Chairman SHELBY. Mr. Werner, the Wells Fargo inquiry.

When did FinCEN and the Federal banking regulators conclude a memorandum of understanding for information sharing about banks under examination for BSA deficiencies?

Mr. WERNER. The MOU was completed at the end of September of 2004.

Chairman SHELBY. When did FinCEN learn the OCC, Office of Comptroller of the Currency, examination of Wells Fargo, and was there consultation with FinCEN before any decision was made regarding the potential for BSA enforcement actions up to and including a cease and desist order?

Mr. WERNER. I think we first learned of a potential Wells Fargo issue from the OCC in December of 2004. I think we actually learned of the informal action the OCC had taken in June of 2005. And I think the report on the Wells Fargo case points out some disconnects of how our MOU was working at that time, but I am happy to be able to report that we have resolved that. There was a misunderstanding on the operative language on the MOU.

Chairman SHELBY. Given the findings of the Treasury's Inspector General's recent report on the OCC's supervision of Wells Fargo concerning the timely communication of OCC to FinCEN about potential BSA enforcement actions, what we have been talking about, can you comment here on whether FinCEN is satisfied with the level of cooperation it received from the Office of the Comptroller of the Currency?

Mr. WERNER. Thank you, Mr. Chairman, because I would like the opportunity to address that, because I think the Wells Fargo case actually turned out to be a positive thing for the development of FinCEN and the OCC's relationship. I think that case really highlighted the fact that the MOU terms had not been fully engaged by both agencies.

In the wake of that case, we really have been able to resolve a lot of the ambiguities in our relationship and the way we exchange information.

Chairman SHELBY. Do you think the relationship has improved considerably?

Mr. WERNER. Dramatically. Comptroller General Dugan has been very engaged with me since I have become the Director of FinCEN. Not only has he been very active in communicating with me, but he has taken the time to come over to FinCEN and receive presentations. It has been very improved.

Chairman SHELBY. Is FinCEN generally satisfied with the supervision and enforcement programs of the OCC—and you said yes, but other regulatory banking agencies in the BSA area?

Mr. WERNER. Again, in general——

Chairman SHELBY. A lot of people operating here.

Mr. WERNER. Yes, sir.

In general, I think the answer to that is yes. As we have heard from comments from members of the Committee, it is a very complicated regulatory regime where we are having to balance the burden to our industry with the benefits of the system. It is a risk-based system.

So that, in order to have that function properly, we really have to make very difficult judgments, sometimes, about what level of enforcement action we take with respect to deficiencies we see in the systems. And I think the regulators working with FinCEN have come a long way in the last few years to really begin to gain consistency in the system and a better way of applying it.

Chairman SHELBY. That is good.

How is Treasury's use of the tools found in the PATRIOT Act and in Executive Orders viewed internationally today, 5 years after 9/11, and what difficulties has Treasury faced in getting international institutions to cooperate?

For example, last year at this time, I believe you spoke at the IMF and commented and commented that too many countries have blocked assets on non-Al Qaeda terrorist and terrorist groups, as required—too few countries. I am sorry. I will correct myself. Too few countries have blocked assets on non-Al Qaeda terrorist and terrorist groups as required by the United Nations resolution.

What is the record today? Where are we, Mr. Glaser?

Mr. GLASER. Excuse me, Mr. Chairman.

I think, as I said in my opening statement, I think we, in the U.S., and we, in the Treasury Department, have really been leading the international community and have been quite innovative in the way we have thought and think about the application of financial measures, either targeted financial sanctions or other authorities that we have in the PATRIOT Act, for example, Section 3.11—how we apply those. And I think it has been well received by the international community.

I think that a lot of countries are a bit behind us in the application of these types of financial tools. But I think that, for example, if you look at the United Nations and you look at the United Security Council, how the U.N. Security Council reacts to international security crisis, be it terrorism in SCR 1267 and 1373, be it WMD proliferation in 1540, the assassination of Hariri in 1636, North Korea in 16905.

Time after time after time, all of these U.N. Security Council resolutions have financial components to it. That is because I think we have been doing a good job of persuading people and persuading countries that this is an important component.

Now, I think that countries have a lot of work to do, and I think what I said at the IMF in the speech that you are referring to still stands. You know, countries have an obligation under U.N. SCR 1373 to block and freeze the assets of global terrorist organizations, all global terrorist organizations. I think that, particularly when you look at an organization like Hezbollah, there has not been enough common action in the international community to block those assets. That is something; again, we have worked very, very hard giving speeches at the IMF, but also going to these countries

and dealing with people directly and trying to persuade them that they have this international obligation. They have the tools.

Chairman SHELBY. How can this Committee help you in this regard? I know we cannot do everything, but we are very supportive in what you are doing.

Mr. GLASER. And we very much appreciate your support, Mr. Chairman, very genuinely. I think that holding hearings like this and shining light on these issues is what needs to be done.

The infrastructure is there, both here, in the international community, and in many countries. Some countries do not have what they need, but most of the big countries. What we need to do is continue to engage, continue to emphasize how important these are, continue to take action, and continue to lead the way, because I think we very much have been doing that.

Chairman SHELBY. But you have got some work to do, haven't you?

Mr. GLASER. We have a lot of work to do.

Chairman SHELBY. Mr. Werner, sharing information technology.

Two years ago, the Commissioner of the Small Business Division of the IRS responded to a question before this Committee regarding the relationship between FinCEN and the IRS in future application of the BSA Direct project. I know these are all technical things we are dealing with—tedious. Commissioner Brown commented at that time that the IRS is the biggest user of the data in the system and that he hopes to continue to be considered "a preferred customer of FinCEN." It is a new system.

Information technologies today are the key to the future abilities of all of your agencies to collect and process information related to possible money laundering and terror finance schemes. The failure of the BSA Direct program to meet its budget and schedule represents a serious setback in that regard, at least with respect to the way the program was described to this Committee.

With the increased reliance on the IRS systems that the BSA's direct demise will entail, is there any reason to believe that FinCEN's ability to execute its mission will be impaired? In other words, what lessons do you draw from the BSA Direct debacle?

Mr. WERNER. Thank you, Sir.

Chairman SHELBY. I know that is a lot of stuff.

Mr. WERNER. It is, but I understand what you are asking, Sir.

The BSA Direct data storage and retrieval component, which is what we had to terminate the contract on, was a disappointment to not be able to achieve that vision. Fortunately, our great partnership with the IRS did allow us to transition to their Web CBRS system. That system will take care of the immediate needs of the vast majority, probably close to 90 percent or more of our external BSA gateway users.

What it does not do is it is not a substitute for the overall concept that FinCEN had envisioned regarding a data warehouse and being able to do data cleansing and some other more advanced analytical technologies. And what we need to do now is to regroup at FinCEN, reengage on our requirement study and figure out exactly how to move forward from here. That may involve partnering with the IRS on that component or it may not, depending on what their capabilities and their own strategic initiatives involve.

What I can tell you, though, Sir, is that, again, trying to make lemonade out of lemons, it was a very instructive failure for FinCEN as an agency.

Chairman SHELBY. What have you learned?

Mr. WERNER. What we learned is that very smart, innovative, entrepreneurial people can not necessarily tackle a project of that scope and technical capacity and make it work just by the sheer force of their will.

What FinCEN needs and is now building is a project management office and a more rigorous strategy for analyzing information technology products and other products in terms of going forward in a much more—we had to grow up. We had gone from an office to an agency, and a growing agency. We need to put in place policies and procedures that reflect the complexity of our business. We are now in the process of doing that.

Chairman SHELBY. During the past 5 years, the FBI has considerably upgraded its law enforcement financial intelligence capacity. Treasury has built an Office of Intelligence and Analysis.

Given that fact, what role does FinCEN now play in the analysis of information for law enforcement, which was FinCEN's original mission?

Mr. WERNER. Yes, Sir.

What we are finding, actually, is that there is an even more advanced role for us to play because the kind of work that OIA and FBI and others are doing has allowed us to begin to remove ourselves from the mere data retrieval business and think about what value added we can really play in working with our customers.

The FBI is a great example because their IDW, now, is allowing them to make a lot of interesting associations with BSA data. I can give you an example. The other day they did a demonstration for me and what they showed me is that they went through suspicious activity reports that were coded terrorist suspicious activities and they matched them against their active investigation case file. What they found is a 20 percent match, which I was astounded at, because, as you know, Sir, terrorist financing is awfully difficult to detect. To see a transaction and understand that the terrorist financing encoded it that way, my expectation would be that you would get a lot fewer examples of true open investigations. And so, to have that kind of correlation really stunned us.

I looked at that and said, where FinCEN can now provide tremendous value is to pull those suspicious activity reports, match them to the institutions that are successfully filing them, examine their programs, and, if there are commonalities in those programs, and my guess is that there will be, we can then feed that back to the industry.

And that is the kind of dynamic communication the industry is begging for and that we have been looking to provide. So, this advancement in technology really is just opening new ways for us to take further advantage of BSA data.

Chairman SHELBY. Are you encountering any staff recruitment or retention problems, given that FinCEN is competing—you all compete out there—with other regulatory agencies, such as OCC, FDIC, and Federal Reserve, and so forth?

Mr. WERNER. That is a very interesting question, Sir, because we expect competition——

Chairman SHELBY. Will you be competing for quality people?

Mr. WERNER. Yes, Sir. Competing with the private sector is one thing. Generally, people make a philosophic decision to work for the public sector. But we do, in fact—we are experiencing recruiting problems because our regulatory peers, which are the Federal banking agencies, they are on a separate pay scale.

I think we see that reflected in applicant pools for our positions in the regulatory area.

Chairman SHELBY. Mr. Glaser.

In this October—we are talking about GAO, now—referring to the October 2005 report. In this October 2005 report on better strategic planning needed to coordinate U.S. efforts to deliver counterterrorism financing training and technical—it is a big mouthful, there.

The GAO said that bureaucratic battles between Federal agencies are hampering the government's efforts, at least in the area of cooperation and foreign assistance and training. You were reported as saying that interagency cooperation had been good, but admitted—as you have been candid with us—that the report pointed out that it could be better. It is an ongoing work, and that there was a strong commitment to make sure that the process is adjusted.

What has Treasury done, Sir, to date, to make these adjustments? In a related development, the Congressional Research Service noted that there was no common criteria among agencies for measuring success of governmentwide anti-terrorism efforts.

You want to comment on that?

Mr. GLASER. Sure. I would be happy to, Senator.

With respect to the GAO report, again, just to clarify on that report. That report focuses specifically on the provision of technical assistance related to terrorist financing, not on our efforts on terrorist financing broadly. And I think, as I said before, it was a fair report that did shine the light on some difficulties that we were having in the interagency community.

I think there has two things happening since then that has improved matters. Internally, within Treasury, what have we been doing? And I think that what we have been doing internally, within Treasury is bringing the process of delivering technical assistance more tightly into the policymaking realm.

We have an Office of Technical Assistance that has a new Deputy Assistant Secretary, Larry McDonald, who is fantastic. He just started at the end of 2005. We are coordinating, in TFI, much, much more closely with Larry and with his team to make sure that the decisions as to the provision of technical assistance on terrorist financing more accurately reflect Treasury and U.S. Government priorities.

I think more importantly than that is what the State Department has been doing, because the State Department certainly has the lead, overall, in the delivery of technical assistance. The provision of technical assistance is an arm of U.S. foreign policy. And what the State Department has done is really elevate the matter to the personal direction of Ambassador Crumpton. Ambassador Crumpton has revived an interagency group on technical assistance

related to terrorism broadly. I think that that is an important point.

Ambassador Crumpton's group does not just focus on terrorist financing but focuses broadly on all technical assistance related to terrorism, be it terrorist financing, be it customs, be it military assistance. Whatever assistance that might be necessary. It is all looked at comprehensively and strategically and looked at regionally, rather than just this exceptionalism that I think previously existed with respect to terrorist financing.

That has had a tremendous impact. I think that things are improving. I am not going to say that everything has been perfect. We are working through the issues that the GAO demonstrated, but I think that we can really very honestly say that there has been a very strong effort at the highest levels, both at Treasury and at State to look at these problems in the face and to do what we can to address them.

With respect to the second part of your question, on unified performance measures—it is always going to be hard to measure our performance in fighting terrorist financing. By nature, it is a surreptitious activity. If we knew where it was going on we would eliminate it.

I think there has been an effort really led by the NSC and by the NCTC to create global, broad goals and objectives within the U.S. Government and coordinate those and attach performance measures to those. I mean, we have been very much a part of that, and it is certainly our hope and expectation that that is going to provide more of a baseline for us to be able to measure the effectiveness of our actions. But that is always going to be a big challenge for us.

Chairman SHELBY. Thank you.

Senator Allard.

STATEMENT OF SENATOR WAYNE ALLARD

Senator ALLARD. Thank you, Mr. Chairman. I want to thank you for holding this hearing.

Currently, banks have some significant legal and reputational risks if they fail to report suspicious activity. Accordingly, they file a fair number of reports. And, as a result, I think the bottom line we have to ask is, do we need to improve on the quality of those reports filed, and maybe not too much on the quantity of filings, because, when we look at this, we see more than 13 million currency transaction reports filed each day. They have increased 45 percent last year to nearly 1 million, I guess.

Compliance costs for financial institutions are substantial. Have we looked at what we can do to streamline this process?

Mr. WERNER. Senator, I am the Director of FinCEN, so let me respond to your question.

We are always looking—we are constantly reassessing and assessing the regulatory system because we are trying to get that burden benefit balance right. Having said that, the reports that are filed with FinCEN are of extreme value to law enforcement, to the regulatory community, to the intelligence community. That does not mean that every individual form that is filed with us will lead to an investigation or prosecution but, in the aggregate, the data

that we are seeing come in to our system is extremely useful, not only in individual case work, but also in doing vulnerability assessments and doing threat assessments and feeding back to inform us on our regulatory scheme.

And what we are—with new developing technologies that FinCEN and other agencies are developing, we are only getting better at exploiting that data and making use of it. That is not to say that we do not have to engage in aggressive outreach with the industry. We do. Because there is a very innocent quality in terms of people's understanding of how to file forms and what they should be putting in the narratives as suspicious activity reports. So, we are engaging in aggressive outreach to try and improve that quality.

In addition, we want to make sure that people understand what their obligations are, because we really do not want people to be overfilling, either. Having said that, at this point, we are not seeing a lot of defensive filing. For the most part, the forms that we see filed are good forms and they are ones that should be filed. And even after enforcement actions, where we see a spike in activity, when we have gone back and analyzed those spikes, what we see is those are good filings. Institutions are going back and looking at their records and filing as a result of it.

While I take your point as an incredibly important one, which is that we need to continue to assess and reassess the system, I think that, at this point, that is something that we are doing.

Senator ALLARD. Well, I know that constituents in the State of Colorado have expressed concerns about, quote, defensive filings. I feel like the bank has felt like, well, we understand that this is a common sense thing, but we feel like, just to cover our tail, we have to go ahead and file these reports. I know you are denying that here, but my personal experience has indicated there are some people out there that feel that—both in the banking industry as well as consumers of banking services—feel that some of those reports are defensive in nature, and probably do not contribute an awful lot. It is pretty obvious, if you look at their record, that it is not tied to any terrorist activity.

Mr. WERNER. Sir, I am sure that there is defensive filing going on. I have no doubt of that. But I think in the aggregate, the data base that we see has a lot of very, very good, very important information, not just for terrorist financing but for other sorts of illicit finance, narcotics trafficking, money laundering, and other sorts of fraud.

When the FBI, through their IDW—and this is terrorist financing—matched the return of Bank Secrecy Act information to their queries, although, initially, the Bank Secrecy Act made up something like 15 percent of their database, they were finding that it was as high as a 50 percent return on queries were related to Bank Secrecy Act information.

So, we have no doubt that there is a high correlation between the filings we are getting and the illicit activity out there.

Senator ALLARD. Now, I assume that you are all participating in the PART Program, which is the Administrations—that is what the Administration calls the programs put in place as a result of our oversight that we pass here. It is Government Results and Account-

ability Act. I believe that is what we refer to it, here. It is where you actually set up goals and objectives and you measure your performance against those goals and objectives.

I am curious on these enforcement programs, what kinds of goals and objectives do you put out there? I hope they are not of the nature of, well, we got a greater appropriation than we did last year in our program, because that does not measure performance. I hope that somewhere in those goals and objectives that you are actually asking yourself, well, how many—this fact led to how many arrests? Did we increase the number of arrests—where we can actually see performance? How are you coming out on these performance measures?

Mr. WERNER. Well, we do not tie performance measures just into arrests because, as I said before, the Bank Secrecy Act—its value goes well beyond merely individual prosecutions. It also goes into vulnerability, systemic trends that we look at, threat assessments——

Senator ALLARD. So how do you put that down as measurable goals and objectives?

Mr. WERNER. What we have done is we have created a survey system where we go out to our customers, our law enforcement partners, and survey them on the value of the data to their investigations and their work. That includes not just the data itself, but also the analysis that we provide them. In that respect, we get a very high percentage of positive response to those queries.

Senator ALLARD. Do you survey banks, too?

Mr. WERNER. We do also survey banks. We do. For regulatory guidance and hotline response times and things like that.

Senator ALLARD. But on your performance measures, do you survey banks?

Mr. WERNER. Yes, we do. That is part of our survey.

Senator ALLARD. So you do not just do law enforcement?

Mr. WERNER. No.

Senator ALLARD. Which I think is important. I am not going to minimize that. I think that we have to do more to counteract terrorism, and I think the financial institutions—you know, on the Commission, the one area that we got an "A" on is on financial institutions, as far as the terrorists were concerned. We want to keep up those kinds of efforts. But on the other hand, I do hope we maintain a proper balance here, also.

And so, you know, I have received some concerns in this area, and that is the reason for the questions that I posed for you today, to make sure that you are actually taking a good evaluation of these programs and making sure that we are not putting unnecessary rules and regulations out there that do not contribute to measurable results.

Thank you, Mr. Chairman.

Chairman SHELBY. Thank you, Senator Allard.

I have a number of questions for the record, and we have some members that were in other Committees that could not be here. We will keep the record open for some questions relevant to what you do.

We appreciate your appearance today and we will continue to work with you and give you the tools to continue this fight. It is not going to go away.

Thank you. The hearing is adjourned.

[Whereupon, at 11:26 a.m., the hearing was adjourned.]

[Prepared statements supplied for the record follow:]

PREPARED STATEMENT OF DANIEL GLASER

DEPUTY ASSISTANT SECRETARY OF TERRORIST FINANCING AND FINANCIAL CRIMES,
DEPARTMENT OF THE TREASURY

SEPTEMBER 12, 2006

I. Introduction

Chairman Shelby, Ranking Member Sarbanes and distinguished members of the Committee, thank you for the opportunity to speak to you today about the Treasury Department's efforts and achievements in the financial war on terrorism, and to discuss the challenges that lay ahead. This Committee has played an important role in ensuring that we have the authorities to combat terrorist financing. As we take a moment to assess how far we have come since that pivotal September day in our nation's history, we recognize that there is still work to be done. The Treasury Department has been an integral player in the battle against terrorism and we will continue to use every tool at our disposal to stop the flow of illicit money to those who would seek to harm our citizens.

Over the last five years we have increased substantially our understanding of vulnerabilities in the international financial system, and how terrorist and other illicit financial networks exploit those vulnerabilities. At the same time, we have steadily enhanced our skill and sophistication in applying the financial tools that we have at our disposal to close those vulnerabilities, disrupt and dismantle illicit financial networks, and apply pressure on the states that provide terrorists support and comfort. We have begun to understand how—by communicating with the international private sector—we can make the international financial system a hostile environment for terrorist financiers and other illicit actors.

Indeed, over the last five years we have witnessed a revolution in the role that finance ministries can play in international security affairs. Counterterrorism and security policy has traditionally been the province of foreign affairs, defense, intelligence, and law enforcement officials—not Finance Ministers. But we have demonstrated why finance ministries worldwide should become integral components of national security communities.

The U.S. has led the way in this development through the establishment of the Treasury Department's Office of Terrorism and Financial Intelligence (TFI)—the first office of its type in the world. TFI's mission is to marshal the Treasury Department's policy, enforcement, regulatory, and intelligence functions to sever the lines of financial support to international terrorists, WMD proliferators, narcotics traffickers, and other threats to our national security. We seek to meet this responsibility by striving to achieve two overarching goals:

- Identifying and closing vulnerabilities in the U.S. and international financial systems; and
- Identifying, disrupting and dismantling the financial networks that support terrorists, organized criminals, WMD proliferators, and other threats to international security.

In my testimony today, I will: (i) Outline how we work to achieve these goals; (ii) articulate some of our successes; and (iii) explain the challenges that we continue to face.

II. Safeguarding the Financial System by Identifying and Closing Vulnerabilities

One of Treasury's core missions is to safeguard the domestic and international financial system from abuse by identifying and closing vulnerabilities that terrorist organizations, WMD proliferators, money launderers, drug kingpins, other international criminals and their support networks exploit. We work with our interagency partners, international counterparts and directly with the private sector to advance this fundamental interest by systematically pursuing the following strategic objectives:

a. identifying typologies of terrorist and illicit financing that present systemic threats to the domestic and international financial system;

b. strengthening and expanding international standards to address these vulnerabilities and to enhance transparency across the international financial system;

c. facilitating compliance with international standards through comprehensive international anti-money laundering/counter-terrorist financing (AML/CFT) assessments and technical assistance;

d. taking appropriate protective actions against those jurisdictions and financial institutions whose AML/CFT and enforcement deficiencies represent substantial threats to the domestic and international financial system; and

e. conducting private sector outreach to the international banking and other financial service industries, as well as to the charitable sector.

This comprehensive strategic approach, described in greater detail below, safeguards the financial system from terrorist and criminal abuse by effectively promoting transparency, particularly across those higher risk elements of the financial system. Such transparency in the financial system is essential in allowing financial institutions, law enforcement, regulatory and other authorities to identify sources and conduits of illicit finance, as well as those individuals and entities that comprise terrorist, WMD and criminal support networks.

Identifying such illicit behavior and terrorist and criminal support networks allows financial institutions and government authorities to adopt appropriate protective measures to prevent these nefarious elements from corroding the financial system. In turn, protective measures deny them access to the financial system, forcing terrorist organizations and criminal interests to adopt alternative financing mechanisms and support structures that present higher costs and greater risks. Finally, the transparency created by our systemic efforts to protect the financial system from abuse is an essential pre-condition for developing and applying targeted financial measures to attack and disrupt specific threats to our national security, foreign policy and criminal justice interests.

A. Identifying Typologies of Abuse and Vulnerabilities to the International Financial System

A critical strategic objective in our mission to safeguard the financial system is identifying systemic vulnerabilities that terrorists and other criminals can exploit to finance their operations and interests. We have collaborated with our partners across the interagency and international community on several projects to identify these vulnerabilities:

- Recently, Treasury worked closely with 16 federal bureaus and offices from across the law enforcement, regulatory, and policy communities to produce the U.S. Governments first-ever Money Laundering Threat Assessment. This working group pulled together arrest and forfeiture statistics, case studies, regulatory filings, private sector and government reports, and field observations. The report analyzes more than a dozen money laundering methods and serves as a first step in a government-wide process to craft strategic ways to counteract the vulnerabilities identified.
- Treasury collaborated with its partners at the Department of Homeland Security's Immigration and Customs Enforcement (ICE) to help produce a comprehensive report on trade-based money laundering, released by the Financial Action Task Force (FATF) in June 2006.
- Treasury is leading an international working group studying the vulnerabilities that new payment products such as stored-value cards and internet-based payment systems introduce to the international financial system. This study includes an initial assessment of the exploitation of these new payment products by criminal organizations.
- Treasury is now working with its partners across the USG to contribute towards the development of international typology studies on money laundering through the real estate industry and casino industries, and terrorist financing more broadly.

We will continue to pursue these and other initiatives to help us identify systemic threats to the international financial system and focus our efforts in developing appropriate policies to protect the financial system from terrorist and criminal abuse.

B. Strengthening and Expanding International AML/CFT Standards

Because of the growing international nature of the financial system, we must work continuously with other financial centers around the world to establish and maintain effective international standards to protect the international financial system from various sources and conduits of illicit financing. In coordination with the interagency community, Treasury primarily advances this strategic objective through the FATF, and also supports the progressive development of international standards against terrorist and illicit financing at the United Nations (UN).

The FATF sets the global standard for combating terrorist financing and money laundering and provides us with a unique opportunity to engage our international counterparts in this effort. Treasury—along with our partners at State, Justice,

Homeland Security, the Federal Reserve Board, and the Securities Exchange Commission—continues to assume an active leadership role in the FATF, which articulates standards in the form of recommendations, guidelines, and best practices. These standards aid countries in developing their own specific anti-money laundering and counter-terrorist financing laws and regulations that protect the international financial system from abuse.

Since before the terrorist attacks of September 11, 2001, we have consistently engaged the FATF to expand and strengthen these international standards to address the systemic vulnerabilities that terrorists and other criminals exploit, including through the development of Nine Special Recommendations on Terrorist Financing and the revision and strengthening of the FATF 40 Recommendations. Most recently, we have successfully engaged the FATF to adopt a new international standard to combat the illicit use of cash couriers, and we have enhanced the international standard for combating terrorist abuse of charities. We have also recently finalized a number of technical but critical aspects to the international standard governing the availability and integrity of originator information on cross-border wire transfers. Moving forward, we intend to discuss in the FATF how the existing AML/CFT international standards should be supplemented, amended or applied to address the vulnerabilities associated with trade-based money laundering.

At the UN, Treasury has supported interagency efforts led by the State Department to develop progressive international standards for combating terrorist financing and WMD proliferation. Most recently, these efforts have successfully led to the issuance of UN Security Council resolutions that:

- elaborate expansive criteria for issuing terrorist financing designations against individuals and entities associated with al Qaida or the Taliban (UNSCR 1617); and
- require member states to prevent the transfer of any financial resources in relation to North Korea's missile or WMD programs (UNSCR 1695).

These standard-setting efforts at the FATF and the UN create an international obligation and framework for countries to implement AML/CFT regimes that effectively protect the international financial system from various forms of illicit finance.

C. Facilitating Compliance with International AML/CFT Standards

To give full effect to these international standards, Treasury has worked continuously and closely with interagency partners and international counterparts to establish a comprehensive global system of AML/CFT assessments through the FATF, the various FATF-Style Regional Bodies (FSRBs), and the World Bank and International Monetary Fund. This system has facilitated compliance with the international AML/CFT standards by auditing the AML/CFT regimes of over 150 countries around the world to assess whether these international standards have been effectively implemented.

Most recently, the U.S. underwent such an assessment through the FATF's Mutual Evaluation Review (MER) process. All members of FATF periodically undergo a mutual evaluation and each jurisdiction is subject to the same methodology and set of standards. In all such assessments, the FATF identifies strengths and weaknesses in a jurisdiction's AML/CFT regime and follows up to ensure that significant deficiencies are addressed.

Through the FATF and FSRB mutual evalution process, Treasury has directly participated in the assessments of several strategically important countries in the campaign against terrorist financing, including Saudi Arabia, Pakistan, India and Switzerland. At the moment, a Treasury regional policy advisor is participating in the FATF mutual evaluation of Turkey, another strategically important country in our global counter-terrorist financing efforts.

In recent years, Treasury has worked continuously through a number of channels to globalize this assessment process by facilitating: (i) the development of new FSRBs that now cover all regions around the world, and (ii) a partnership between the FATF and the World Bank/IMF whereby AML/CFT assessments are now incorporated into every financial sector assessment conducted by these international financial institutions. These developments ensure the identification of systemic vulnerabilities created by jurisdictional deficiencies and allow for governmental authorities and the international financial community to take appropriate responsive actions.

One potentially appropriate governmental response to systemic vulnerabilities created by jurisdictional AML/CFT deficiencies is providing technical assistance to facilitate compliance with international standards. Treasury provides significant technical assistance to support the broader USG technical assistance mission in com-

bating terrorist financing and to facilitate the development of transparent and accountable financial systems in strategic countries of concern.

In summary, Treasury's ongoing efforts to globalize AML/CFT assessments, participate in strategically important assessments, and provide meaningful technical assistance collectively advance our core mission of closing down systemic vulnerabilities by promoting compliance with AML/CFT international standards.

D. Taking Protective Action against Systemic Vulnerabilities

Overview of Section 311

In those instances where jurisdictional or institutional deficiencies present ongoing systemic vulnerabilities that create substantial money laundering or terrorist financing threats to the international financial system, Treasury can take appropriate protective action under Section 311 of the USA PATRIOT Act. Section 311 authorizes Treasury to designate a foreign jurisdiction, foreign financial institution, type of account or class of transactions as a primary money laundering concern, thereby enabling Treasury to impose any one or combination of a range of special measures that U.S. financial institutions must take to protect against illicit financing risks associated with the designated target. These special measures range from enhanced due diligence, recordkeeping, and reporting requirements up to and including termination of any and all correspondent accounts or activities with the designated target.

We are grateful to Congress for granting us this powerful and flexible authority. Treasury has utilized Section 311 in a variety of ways to protect the U.S. financial system from money laundering and terrorist financing threats associated with three foreign jurisdictions and eight foreign financial institutions designated as primary money laundering concerns under Section 311. On each of these occasions, our Section 311 designation has had a significant effect in protecting not only the U.S. financial system, but also the international financial system, as international financial markets have taken independent protective financial actions in response to the systemic vulnerabilities associated with the designated target. In some instances, designation under Section 311 has even facilitated the development of rehabilitative measures that effectively addressed the underlying systemic vulnerability such that withdrawal of the 311 designation has been warranted.

Case Study: 311 Actions against Latvian Financial Institutions

Treasury's Section 311 designation of two Latvian financial institutions—Multibanka and VEF Banka—in April 2005 provides an excellent example of the effectiveness of this authority in eliminating systemic vulnerabilities in the financial system. Treasury's designations were grounded in a number of jurisdictional and institutional AML/CFT deficiencies and specific money laundering concerns that created substantial vulnerabilities for the U.S. and international financial systems. Concomitant with these designations, Treasury issued rulemaking notices that proposed prohibiting U.S. financial institutions from opening or maintaining correspondent accounts with the designated Latvian financial institutions.

In reaction, numerous U.S. financial institutions cut off all financial dealings with both Multibanka and VEF Banka and generally exercised greater caution in dealing with Latvian-based transactions, accounts and relationships. Moreover, the international financial community also subjected Latvian-based financial dealings to greater scrutiny in light of the jurisdictional and institutional deficiencies and concerns identified in the 311 actions.

Treasury's 311 designations also spurred various Latvian governmental and financial authorities to cooperate with a broad array of U.S. authorities. Treasury worked together with the State Department, law enforcement and federal banking regulatory authorities to develop a conference series of workshops to discuss AML/CFT concepts and to address a number of the AML/CFT deficiencies identified in the 311 designations. Owing to several significant jurisdictional and institutional remedial steps taken by the Latvian authorities and Multibanka, Treasury subsequently withdrew its finding of primary money laundering concern and its associated notice of propose rulemaking against Multibanka in July 2006. On the other hand, continued institutional deficiencies and ongoing money laundering concerns associated with VEF Banka led Treasury to issue a final rule prohibiting U.S. financial institutions from initiating or maintaining any correspondent relationship with that concern.

Both of these Section 311 designations against Latvian financial institutions succeeded in protecting the financial system from jurisdictional and institutional vulnerabilities, in part by facilitating appropriate remedial actions by the Latvian authorities and Multibanka, and in part by cutting off U.S. financial institutions from ongoing vulnerabilities associated with VEF Banka. These examples help dem-

onstrate the effectiveness of Section 311 in helping Treasury safeguard the financial system by closing down or taking protective action against ongoing systemic vulnerabilities.

E. Conducting Private Sector Outreach

Treasury has also advanced its core mission of safeguarding the financial system and vulnerable industries from abuse by launching comprehensive outreach campaigns with the private sector. Treasury's efforts in this regard are primarily focused on the international banking and financial service industries and the charitable sector.

Outreach to the International Banking Community

In accordance with its international private sector outreach strategy, Treasury has initiated private sector AML/CFT dialogues linking the U.S. banking sector together with those from the Middle East/North Africa (MENA) region and the Latin American region, with the support of relevant financial and regulatory authorities. The purpose of these dialogues is to:

(i) raise awareness of domestic and regional money laundering and terrorist financing risks, international AML/CFT standards and regional developments, and U.S. government policies and private sector measures to combat terrorist financing and money laundering;

(ii) assess the impact of AML/CFT international standards and U.S. law and regulation on AML/CFT development and implementation in the U.S. and foreign banking and financial service industries; and

(iii) strengthen development and implementation of effective AML/CFT measures, particularly in regions of strategic importance and jurisdictions that lack fully-functional AML/CFT regimes.

In collaboration with its interagency and regional partners, Treasury successfully facilitated the launch of the U.S.-MENA Private Sector Dialogue on AML/CFT with an initial AML/CFT Conference in Cairo in March 2006. Bankers and financial and regulatory authorities from the U.S. and the region discussed a range of challenges associated with the development and implementation of effective AML/CFT jurisdictional and institutional measures. We are now collaborating with our partners in this effort to finalize the agenda for a follow-on conference at the Federal Reserve Bank of New York in December 2006.

Treasury has initiated a similar dialogue with the Latin American banking community, hosting a roundtable discussion of U.S. and regional interests at Treasury in June 2006 to help frame this initiative. We are collaborating with these regional interests to plan an initial AML/CFT conference in the region in early 2007.

This direct private sector outreach to the international financial community complements our other work to address vulnerabilities in the international financial system by providing a mechanism to explain our money laundering and terrorist financing concerns, assess and facilitate AML/CFT progress and implementation, and receive feedback on the effectiveness of our efforts from key regional participants in the international financial system.

Outreach to the Charitable Sector

Outreach to the charitable sector represents a fundamental objective for Treasury in its broader campaign to combat terrorist financing. Treasury's ongoing engagement with the charitable community strives to *protect charities* from terrorist abuse and *empower the sector* to adopt and implement effective safeguards against terrorist exploitation. I will describe Treasury's protective efforts—advanced largely through designation of those charities that support terrorist organizations and activities—in a few moments.

Treasury's efforts to empower the charitable sector require a sustained interagency outreach campaign to communicate and advance the following fundamental points:

- The U.S. government and the charitable community share common fundamental interests in (i) promoting humanitarian relief and charitable works, and (ii) protecting charitable giving from terrorist abuse;
- Terrorist abuse includes direct support of terrorist activity and broader terrorist exploitation of charitable funds and services to radicalize vulnerable populations and cultivate support for terrorist organizations;
- Terrorist abuse is ongoing, pervasive and particularly difficult in conflict zones where terrorist groups operate and needy populations require humanitarian support;

- Combating terrorist abuse of the charitable sector requires a comprehensive approach, including oversight, outreach, enforcement, and international actions designed to: (i) empower the sector to protect against terrorist abuse, and (ii) identify and disrupt terrorist abuse of the sector;
- Actions to empower the sector include: (i) providing guidance for the sector to consider in developing and applying measures to safeguard operations from terrorist abuse, and (ii) providing information about the nature of the ongoing terrorist exploitation threat to inform the sector in developing and applying appropriate safeguards; and finally
- Actions to disrupt terrorist abuse of the sector include law enforcement investigations and prosecution, as well as financial and economic sanctions such as designations—these tools are mutually reinforcing but distinct from one another.

Moving forward, Treasury will continue to underscore these fundamental points and provide additional guidance to the charitable community about appropriate protective measures against terrorist abuse. Treasury is currently finalizing the revised version of its Anti-Terrorist Financing Guidelines: Best Practices for U.S.-Based Charities, originally issued in November 2002 and revised and reissued for public comment in December 2005. Treasury will also continue to provide additional information on the risks and typologies of terrorist abuse, such as those discussed in Treasury's paper on the risks associated with terrorist exploitation of post-earthquake relief efforts in Pakistan, available together with other materials on the Treasury website.

III. Disrupt and Dismantle

In addition to identifying and closing vulnerabilities in the financial system, Treasury is working to aggressively disrupt and dismantle the networks that support and facilitate some of the gravest threats the U.S. faces.

The first step in disrupting and dismantling illicit financial networks is identifying those networks. For that reason, the intelligence component of our efforts is particularly important. Recognizing that importance, in close collaboration with Congress we have become the first finance ministry in the world with an internal intelligence analysis office. The Office of Intelligence and Analysis within the Treasury Department brings the knowledge of the intelligence community to bear on the evolving threat of illicit finance. Having an intelligence analysis office at the Treasury is a tremendous innovation. Financial intelligence is uniquely reliable; it allows us to track threats, as well as to deter and disrupt them.

We are learning that the targeted financial measures we have developed since 9/11 to combat terrorist support networks can and should be used to disrupt and dismantle the networks that support other threats. We have shown that these types of financial measures can be quite effective, in part because they unleash market forces by highlighting risks and encouraging prudent and responsible financial institutions to make the right decisions about the business in which they are engaged. As we have seen in the terrorism context, they also give us a concrete way in which to target directly those individuals and entities we know are bad actors and to strike at the heart of their operations.

Today, I would like to highlight Treasury's use of these targeted financial measures to address threats posed by:

a. Terrorists and their support networks;

b. WMD proliferators and their supporters; and

c. State sponsors of terrorism.

Each day, we are working to use financial measures to actively complement broader U.S. strategies to address these threats. We are also focusing on seeking similar actions from our international partners, working collaboratively with other countries and international organizations to develop the multilateral authorities and capabilities that are needed to support the financial actions we are taking. We have seen that these efforts are beginning to reap benefits in the form of growing international recognition of the effectiveness of financial measures. Not only do multiple international organizations such as the Financial Action Task Force, the United Nations, and others recognize that financial measures have an important role to play in the maintenance of global security, multiple UN Security Council resolutions make reference to financial measures in the context of a variety of specific threats.

A. Combating Terrorism with Financial Authorities

Attacking Terrorists Through the Use of Targeted Financial Sanctions

Since September 11, 2001, we have made significant progress in creating and deploying financial tools to identify, disrupt and dismantle the financial networks that facilitate and support terrorism. Through the adoption of UNSCR 1267 and 1373, the U.S. has facilitated the establishment of an effective international framework with obligations to ensure that the international financial system is a hostile working environment for those who support terrorist networks.

Treasury continues to work to refine and focus U.S. implementation of those obligations, predominantly through the application of targeted financial sanctions and our primary financial tool for combating terrorists and their support networks: Executive Order 13224. OFAC Director Szubin will testify to in greater detail how this powerful authority freezes the assets of terrorists and terrorist support entities and isolates them from the U.S. financial and commercial systems. This authority also allows Treasury to expose terrorists' true sources of funding, crippling their ability to raise and move money under the guise of legitimate activities, such as charitable fundraising or the provision of financial services.

To date, the U.S. has designated a total of 460 individuals and entities pursuant to E.O. 13224, of which 375 were named by Treasury. Director Szubin will describe some of these designations in greater detail in his testimony. Through mentioning several key actions, he serves to highlight the breadth of terrorist entities that we have been able to expose and disrupt:

- **Financial Institutions.** Treasury last week designated **Bayt al-Mal** and **Yousser Company,** which are financial institutions that functioned as Hizballah's unofficial treasury in Lebanon.
- **Charities.** Treasury has designated in whole or in part more than 40 charities worldwide as supporters of terrorism, including the designation of the **Islamic Resistance Support Organization (IRSO),** a key Hizballah fundraising organization, two weeks ago. In August, Treasury designated the Philippine and Indonesian branches of the Saudi-based **International Islamic Relief Organization (IIRO)** for facilitating fundraising for al Qaida and affiliated terrorist groups.
- **Financiers and Fundraisers.** Financiers and fundraisers have been significant targets of designation, disrupting their ability to tap into their personal financial reserves and network of donors. Recently designated financiers include al Qaida donor **Abd al Hamid Sulaiman Al-Mujil,** who has been called the "million dollar man" for supporting Islamic militant groups, and **Bilal Mansur Al-Hiyari**, who provided financial support to the Zarqawi Network in support of its brutal attacks in Iraq against the Iraqi people, U.S. troops and coalition partners.

Treasury's implementation of targeted financial sanctions against these types of support network individuals and entities achieves multiple objectives, including:

- Deterring entities who might otherwise be willing to finance terrorist activities;
- Exposing "money trails" that may generate leads to previously unknown terrorist cells and financiers;
- Dismantling terrorist support networks by encouraging members of the support network to disassociate themselves from individuals or entities that are the targets of the sanctions;
- Terminating terrorist cash flows by shutting down the pipelines used to move terrorist funds or other assets;
- Forcing terrorists to use more costly and higher risk means of financing their activities, which makes them more susceptible to detection and disruption; and
- Fostering international cooperation and compliance with obligations under relevant UNSCRs, including UNSCR 1267, 1373, and 1617.

Encouraging Multilateral Action

A significant part of Treasury's mission is devoted to U.S. government efforts to secure international support and implementation of targeted financial sanctions actions like those I have described. In the five years since Sept. 11, we have learned all too well that the effectiveness of these authorities is significantly enhanced when other countries support U.S. efforts by freezing terrorist assets in their own jurisdictions, and prohibiting their nationals from dealing with terrorists. In coordination

with the Department of State, Treasury facilitates such action through a variety of activities, including by maintaining a dialogue with other countries regarding the financial actions that are needed to disrupt specific terrorist cells or networks. However, we are also working to strengthen other countries' capacity and ability to implement targeted financial sanctions.

Through the U.S. government's efforts with the EU, the Financial Action Task Force, the G7 and others, we have succeeded in assisting other countries to develop national sanctions authorities similar to our own and to improve cooperation in implementing asset freezes. In many cases, countries have joined us in imposing sanctions on U.S.-designated individuals and entities, either independently or through action at the United Nations. We have seen an increase in the number of countries approaching the UN Security Council to seek the designation of terrorist supporters. This global designation program, overseen by the UN's 1267 Committee, is a powerful tool for global action against supporters of al Qaida. It envisages 191 UN Member States acting as one to isolate al Qaida's supporters, both physically and financially. In 2005, 18 Member States submitted names for the Committee's consideration, many for the first time, and we will continue to support this process and encourage others to do so as well.

B. Using Financial Authorities to Combat WMD proliferation

Attacking WMD Proliferators Through the Use of Targeted Financial Sanctions

Related to our effort to combat terrorism is the effort to disrupt WMD proliferation, to prevent the possibility that nuclear, chemical or biological weapons could fall into the hands of terrorists. In fact, the financial tools we are using to combat terrorist support networks have proven to be effective in disrupting WMD proliferation as well. The international community also has recognized the need to combat WMD proliferation through financial measures, as reflected in UNSCR 1540, which calls on all states to develop and implement authorities to combat proliferation, including by denying proliferators and their supports access to the financial system. More recently, the UN Security Council adopted resolution 1695—passed in response to North Korea's launching of seven ballistic missiles in violation of the September 2005 Joint Statement of the Six-Party Talks, as well as North Korea's 1999 agreement to a moratorium on testing long-range missiles—requiring all member states to prevent the transfer of financial resources associated with North Korean proliferation and missile programs.

We are implementing UNSCR 1540 and UNSCR 1695 obligations through Executive Order 13382, issued by the President in June 2005. E.O. 13382 adds powerful tools similar to those we have in the counter-terrorism realm—a broad-based transactions prohibition and an asset freeze—to the array of options available to the U.S. government to combat WMD trafficking. As part of issuing Executive Order 13382, the President identified and targeted eight entities in North Korea, Iran, and Syria, thereby prohibiting U.S. persons from engaging in transactions with them and requiring any assets of those entities within the control of U.S. persons to be frozen. The President also authorized the Secretary of State and the Secretary of the Treasury to designate additional proliferators of WMD and their supporters under the new authorities provided by the Order.

In addition to the eight entities named in the annex of E.O. 13382, the Treasury Department has designated 19 entities and one individual as WMD proliferators. These actions described in greater detail in Director Szubin's testimony, have exposed some of the front companies, suppliers, financial institutions and individuals that facilitate their WMD proliferation, including:

- **Sanam Industrial Group and Ya Mahdi Industries Group**, both subordinates to Iran's **Aerospace Industries Organization (AIO)**, which manages and coordinates Iran's missile program and oversees all of Iran's missile industries.
- Chinese companies **Beijing Alite Technologies Company, Ltd. (ALCO), LIMMT Economic and Trade Company, Ltd., China Great Wall Industry Corporation (CGWIC)**, and **China National Precision Machinery Import/Export Corporation (CPMIEC)**, as well as a **U.S. office of CGWIC** located in California. These companies supplied Iran's military and Iranian proliferators with missile-related and dual-use components.
- Swiss company **Kohas AG**, which acted as a technology broker in Europe for the North Korean military and procured goods with weapons-related applications, and its president, Swiss national **Jakob Steiger.**

By prohibiting U.S. persons from engaging in transactions with these front companies and individuals, we can effectively deny proliferators access to the U.S. fi-

nancial and commercial systems, cutting them off from the benefits of our economy and trade. Our actions also expose their links to proliferation activity, and put unwitting facilitators on notice to cease their dealings with them. Ultimately, we believe that these targeted actions will remove the profit incentive from this dangerous trade and degrade proliferators' ability to conduct business worldwide.

Creating Global Action to Disrupt Financial Underpinnings of Proliferation Networks

Although the U.S. has taken initial steps to implement UNSCR 1540 and UNSCR 1695, many countries have not. Treasury, in conjunction with the State Department and other agencies, has begun outreach initiatives on a variety of fronts to encourage other countries to fulfill these international obligations by developing and utilizing authorities similar to E.O. 13382 in their own jurisdictions. Alternatively, we are urging countries to consider how they may be able to use existing authorities to freeze WMD proliferators' assets and prohibit their nationals from having dealings with them.

- **Proliferation Security Initiative**. Treasury is working to encourage the more than 70 countries that participate in the Proliferation Security Initiative (PSI) to use financial measures to combat proliferation support networks. This initiative, which was established by the President in May 2003, aims to stop shipments of weapons of mass destruction, their delivery systems, and related materials worldwide. I personally attended the PSI's High Level Proliferation Meeting in Warsaw, Poland in late June and was encouraged by the strong response to the U.S.-led discussion of ways in which countries could address the financial underpinnings of WMD proliferation. We plan to continue to support dialogue on this issue within the PSI's Operational Experts Group, which meets several times annually to discuss practical aspects of combating WMD trafficking.
- **Global Initiative**. We will also support activities associated with the Global Initiative to Combat Nuclear Terrorism, announced by President Bush and President Putin in July. This initiative goes to the heart of the threat that is most concerning—the possibility that nuclear weapons could fall into the hands of terrorists—and opens up new possibilities for the effective use of financial authorities.

C. State Sponsors of Terrorism.

In the post–9/11 era, the world faces two unique, but overlapping, problems. We face the threat of the global *jihadists*, who survive in states but are not always directly supported by them. We also face the threat of state sponsors of terrorism dedicated to acquiring weapons of mass destruction. With respect to states, it is a particular challenge to limit or, preferably, halt altogether their ability to use the international financial system to support their threatening behavior. They hide behind a veil of legitimacy, disguising their activities, such as weapons sales or procurement, through the use of front companies and intermediaries. In some cases, they intentionally obscure the nature of their financial activities to avoid suspicion and evade detection. The strategies we have employed to combat the threats posed by North Korea, Iran and Syria are good examples of the ways in which financial authorities are effective in dealing with state sponsors of terrorism.

Iran

As we continue to deal with the challenge presented by Iran's pursuit of a nuclear weapons program, we must also confront its support for terrorism. We have already begun to take steps to do so.

First, while Iranian financial institutions are prohibited from directly accessing the U.S. financial system, they are permitted to do so indirectly through a third country bank for payment to another third country bank. Last week, we took actions to completely cut off one of the largest Iranian state-owned banks, Bank Saderat, from the U.S. financial system. This bank, which has approximately 3400 branch offices worldwide, is used by the Government of Iran to transfer money to terrorist organizations such as Hizballah, as well as Hamas, the Popular Front for the Liberation of Palestine-General Command and Palestinian Islamic Jihad. For example, since 2001, a Hizballah-controlled organization received $50 million directly from Iran through Saderat. Hizballah uses Saderat to send money to other terrorist organizations as well. Hizballah has used Bank Saderat to transfer funds, sometimes in the millions of dollars, to support the activities of other terrorist organization such as Hamas in Gaza. We will no longer allow a bank like Saderat to do business in the American financial system, even indirectly.

Moreover, we have begun to engage with the international financial community to discuss the risks of doing business with Iran. In fact, Treasury Under Secretary Stuart Levey is engaged in precisely such consultations in Europe this week. We are already seeing private institutions—particularly those in the financial community—responding to Iran's provocative behavior and reassessing their relationships with Iran. Earlier this year, the Swiss bank UBS cut off all dealings with Iran. HSBC and Credit Suisse have also limited their exposure to Iranian business. According to the banks, these were business decisions, pure and simple—handling Iran's accounts was no longer good business. As further evidence of the change in tide, a number of foreign banks are refusing to issue new letters of credit to Iranian businesses. And earlier this year, the OECD raised the risk rating of Iran, reflecting this shift in perceptions and sending a message to those institutions that have not yet reconsidered their stance.

North Korea

Treasury has undertaken two broad initiatives to counter illicit North Korean activity. First, we have applied targeted financial sanctions to a number of North Korean proliferation firms under the WMD proliferation Executive Order, E.O. 13382. As I've discussed, a designation under this E.O. cuts the target off from access to the U.S. financial and commercial systems and puts the international community on notice about a particular threat.

Second, we took a regulatory action to protect our financial system against Banco Delta Asia (BDA), a Macau-based bank that was handling North Korea's dirty business without any pretense of due diligence or control. BDA was a willing partner, actively helping North Korean agents conduct surreptitious, multimillion dollar cash deposits and withdrawals without questioning the basis of these transactions. Indeed, BDA officials had negotiated a lower standard of due diligence with their North Korean clients. As I previously discussed, using our Section 311 authorities, Treasury designated Banco Delta Asia as a primary money laundering concern. This action has had a profound effect, not only in protecting the U.S. financial system from abuse, but also in notifying financial institutions and jurisdictions globally of an illicit finance risk.

As a result of these actions and public revelations about North Korea's conduct, responsible foreign jurisdictions and institutions have taken steps to ensure that North Korean entities engaged in illicit conduct are not receiving financial services. Press reports indicate that some two dozen financial institutions across the globe have voluntarily cut back or terminated their business with North Korea, notably including institutions in China, Japan, Vietnam, Mongolia, and Singapore. The result of these voluntary actions is that it is becoming very difficult for the Kim Jong-Il regime to benefit from its criminal conduct. UN Security Council Resolution 1695 has accelerated the trend. It requires all countries to prevent the transfer of financial resources in relation to North Korea's WMD and missile programs.

Indeed, the line between North Korea's licit and illicit money is nearly invisible. Financial institutions around the world should think carefully about the risks of doing North Korea-related business.

Syria

As in North Korea, we have taken a combination of steps to address Syria's problematic behavior and the threats posed by Syria. First, under Executive Orders 13399 and 13338, Treasury is applying targeted financial sanctions that, among other things, freeze the assets of individuals and entities that contribute to Syria's support of international terrorism or were involved in the assassination of the former Lebanese Prime Minister Rafik Hariri. In addition, Syria's Scientific Studies and Research Center (SSRC) is subject to an asset freeze under the WMD proliferation sanctions program, having been named by the President in the annex of Executive Order 13382 establishing the program in June 2005. SSRC is the Syrian government agency responsible for developing and producing non-conventional weapons and the missiles to deliver them. While it has a civilian research function, SSRC's activities focus substantively on the acquisition of biological and chemical weapons.

Second, we took action under Section 311 to protect the U.S. financial system against the Commercial Bank of Syria (CBS), which has been used by criminals and terrorists to facilitate or promote money laundering and terrorist financing, including the laundering of proceeds from the illicit sale of Iraqi oil and the channeling of funds to terrorists and terrorist financiers. In March 2006, Treasury issued a final rule, pursuant to Section 311, designating CBS as a primary money laundering concern and requiring U.S. financial institutions to close correspondent relationships with CBS. Consequently, prominent international financial institutions have begun to reassess their relationships with Syria and a number of Syrian entities.

IV. Conclusion

I am hopeful that my testimony today has provided a broad view of how Treasury's efforts are safeguarding the financial system and helping to advance the overarching efforts of our government to combat terrorism and various other threats. As we review the developments at Treasury since 9/11, it is clear that we have come a long way in reshaping Treasury's role to focus on closing down vulnerabilities to the financial system and applying financial measures to disrupt and dismantle the networks that support terrorists, WMD proliferators and state sponsors of terrorism.

It is also clear that we have considerable challenges ahead of us. We must continue to work with our interagency partners and the private sector to ensure that we are collecting, sharing and applying useful financial information to combat terrorism and other threats. We must also work with our interagency partners and the private sector to advance the effectiveness and efficiency of our financial actions, including our systemic regulatory efforts and our targeted and economic financial measures, in preventing terrorist activity and in disrupting these threats. We must also continue to work with our international counterparts to develop and share meaningful financial information and to achieve broader multilateral capability and support for our financial actions. And we must adjust the development and application of our financial tools as terrorists and other threats adapt their financing methods and as we continue to learn how to improve our efforts. With the comprehensive strategic approach that I have outlined here today, we will move forward to attack these challenges.

Finally, I am grateful for the support that the Congress has provided to us as we have refined our mission under the development of TFI at Treasury. I am honored to be a part of such an important mission at Treasury and am particularly grateful for the support and leadership that our mission continues to receive from across the interagency community and from within Treasury, particularly from Undersecretary Stuart Levey, Assistant Secretary Pat O'Brien, FinCEN Director Werner and OFAC Director Szubin, and others whom I work with every day. Such unwavering support and leadership will ensure that we continue to advance our mission as we tackle the challenges that lie ahead.

I would now be happy to answer any questions that you may have.

PREPARED STATEMENT OF ADAM J. SZUBIN

DIRECTOR OF THE OFFICE OF FOREIGN ASSETS CONTROL, DEPARTMENT OF THE TREASURY

SEPTEMBER 12, 2006

Chairman Shelby, Ranking Member Sarbanes and Members of the Committee, thank you for this opportunity to discuss the role that the Office of Foreign Assets Control (OFAC) has been playing to combat terrorism in the five years since September 11.

It is, in a way, fitting that this hearing marks my first public appearance as the Director of OFAC. Combating terrorist financing has been a principal focus of mine almost since that fateful day five years ago. At the time, I was practicing law in the Justice Department's Federal Programs Branch and I looked to discover how I could contribute to our Government's efforts to combat terrorism. It was an OFAC action that provided my entry into the counter-terrorism arena. Shortly after the September 11 attacks, OFAC froze the assets of three Islamic charities in the United States that had been funneling money to al Qaida and Hamas. In combination with law enforcement action by the FBI, OFAC's actions effectively shut down what had been among the more significant conduits of terrorist financing in the United States. When the charities filed lawsuits challenging the government's actions, I joined a team of lawyers representing OFAC and the Treasury Department, as we successfully argued in various court actions why OFAC's actions had been legal and appropriate.

In the years since, I have continued working on terrorist financing and related issues, first as Counsel to the Deputy Attorney General on terrorism financing issues, then as Senior Advisor to Under Secretary Stuart Levey, who oversees the Office of Terrorism and Financial Intelligence (TFI), of which OFAC is a part.

Over the last five years, this Committee has demonstrated its absolute commitment to combating terrorist financing, and ensuring that the Government has all of the tools necessary to do this work aggressively and appropriately. I am therefore particularly pleased to be here today to introduce myself to the members of this committee and thank you for your leadership and support.

OFAC in 2006

My testimony will focus on OFAC's work to combat terrorist organizations and state sponsors of terrorism. I would, however, first like to outline briefly the wide range of national security issues that OFAC confronts today. OFAC is charged with administering and enforcing the U.S. Government's economic and trade sanctions. These sanctions span approximately 25 regimes and countries, and also target international narcotics traffickers, proliferators of weapons of mass destruction, and terrorist support networks.

Crafting these sanctions programs requires meticulous legal and policy analysis to ensure that our sanctions are effective, balanced, and clear. And, before they can be implemented, our targeted programs require persistent and creative investigative work to unravel the hidden financial trails of security threats, be they terrorist or WMD networks or drug kingpins. In recent years, TFI's Office of Intelligence and Analysis has assumed responsibility for researching and investigating the terrorist networks that form the basis for OFAC's actions in this arena, and has done exceptionally fine work. Once our sanctions are in place, however, much of OFAC's work is only beginning. We do extensive outreach to the private financial sector, at home and abroad, to answer questions and ensure that it understands the implications of our sanctions across a range of complex industries. We review and process tens of thousands of license and interpretive guidance requests a year, filed by individuals, firms, and multinational corporations, each of which requires careful consideration, and some of which entail sophisticated transactional analysis. We also investigate possible violations of our sanctions and, in the appropriate case, assess civil penalties or refer the violator for criminal prosecution. All of these efforts are supported by a talented resource management team, which makes continual adjustments to meet shifting priorities. OFAC performs this front-to-end work across all of its 30 sanctions programs, from the Balkans to Zimbabwe. The fact that it has been able to fulfill this mission so ably with a staff of only 125 FTE gives a sense of how dedicated and professional this staff is.

To provide a snapshot of our operations, in just the past three months, OFAC has exposed and targeted the nerve centers of Mexico's notorious Arellano Felix Organization, one of Colombia's most elusive cartels, four Chinese companies facilitating WMD-related activities, two Syrian military leaders, a set of major Hizballah financial entities, and has also cut off from the U.S. financial system an Iranian bank that was supporting Middle East terrorist groups. OFAC has also worked closely with the Departments of State and Justice to help establish and identify targets for three new sanctions programs, including Sudan's Darfur Region, Cote d'Ivoire and Belarus. In nearly every national security issue of the day, OFAC is making a contribution.

On a daily basis, OFAC works hand-in-hand with the other organizations testifying today, the Office of Terrorist Finance and Financial Crime, the Financial Crime Enforcement Network (FinCEN), and the Internal Revenue Service, as well as the Office of Intelligence and Analysis, which is not present. Under the leadership of Under Secretary Stuart Levey's Office of Terrorism and Financial Intelligence, these offices offer a range of powerful financial authorities and influence that can be harnessed to deter, disrupt, or disable threats to our national and economic security.

We also work closely with other federal departments and agencies to ensure that our programs are implemented and enforced effectively. In addition, we engage in regular outreach with the private sector enterprises affected by our programs, ranging from the financial and services sectors to manufacturing and agricultural industries. The cooperation we receive from U.S. corporations in complying with sanctions is generally exceptional.

Against this background, I will focus on OFAC's role in combating terrorism in the five years since the deadly attacks of 9/11.

September 11th Leads to New Sanctions Authorities

Following the horrific events of September 11th, the President issued Executive Order 13224, authorizing the Secretaries of the Treasury and State to wield the President's broad financial authorities against terrorist organizations and their support networks. The Executive Order has proven to be a powerful and flexible tool—it allows us to designate and block the assets of individuals and entities controlled by or acting on behalf of named terrorist organizations, freezing any of the target's assets that are held by U.S. persons and preventing U.S. persons from having any future dealings with them. Violations of the Executive Order are subject to civil and criminal penalties. To date, the U.S. has designated approximately 460 individuals and entities pursuant to E.O. 13224, of which 375 were named by Treasury.

Congress strengthened and reinforced these authorities with the passage of the USA PATRIOT Act in October 2001. The Act clarified OFAC's authority to block the assets of suspect entities in "aid of an investigation," which is an important tool when there is concern about asset flight or when our intelligence leads us to suspect that a dangerous funds transfer is imminent. In addition, the PATRIOT Act made clear that OFAC could use classified information in its designations without risking having to turn this information over to a designated terrorist supporter at a later date. These provisions have enhanced our ability to take swift and meaningful action, while leaving intact a proper balance between effectiveness and fairness.

In cases in which our designation targets are associated with either al Qaida or the Taliban, as has been the case more than two-thirds of the time, we can also propose these names to the United Nations 1267 Sanctions Committee for inclusion on its designation list. When a target is designated by the U.N. Committee, all U.N. member states worldwide are obligated to freeze the target's assets. Thanks to the able work of the State Department, we have made effective use of this international tool, both in using it ourselves to broaden the impact of our own designations and in encouraging other countries to submit their own targets.

The Impact of "Unilateral" Actions

One question frequently posed to OFAC is, how meaningful are OFAC's actions when the U.S. acts by itself to designate a foreign target—whether a terrorist supporter, a narcotics trafficker, or a supporter of WMD proliferation—and that target doesn't hold assets in the United States? Or, to put it more simply, are unilateral actions effective?

As it turns out, even when we initially act alone, we can have a dramatic impact. There are two main reasons for this. First, the United States is the world's leading banking and financial center; to paraphrase an old saying, "all financial roads lead to New York." When a designated party in Afghanistan tries to send money to Southeast Asia, that transfer will often pass through a United States bank, if only for an instant. The result is typically that these funds are frozen and we are notified by a call to our hotline or the filing of a blocking report. In addition, it is important to remember that U.S. persons and U.S. branches situated abroad are subject to U.S. law, and must comply with OFAC's regulations as if they were in the United States.

Our second "force multiplier" is that international financial institutions frequently implement our sanctions voluntarily, even when they are under no legal obligation from their host countries to do so. We have seen this time and again, in countries from Kuwait to Latvia. These financial institutions may do so because they don't want to be hosting the business of terrorist organizations, even if it is legally permissible. They may cooperate because of reputational risk. Or, perhaps they do so because of fears of litigation or U.S. action. Whatever the cause, the "OFAC list," as it is known, is on the computer screens of bank compliance officers the world over. As a result, our "unilateral" actions are anything but and can have a decisive impact against terrorist supporters, narcotraffickers, and WMD proliferators.

Using Targeted Sanctions Against Terrorist Financing Networks

The Treasury Department was applying its financial authorities against terrorist organizations long before 2001. OFAC first implemented sanctions against Middle East terrorist groups in January 1995, and then expanded its scope to target Usama bin Laden and al Qaida in 1998. In implementing these programs, OFAC drew on its experience in directing targeted sanctions against narcotraffickers and their financial networks, and its experience—dating back to the 1940s—in administering sanctions against various countries.

As a result, while September 11th prompted a surge in OFAC's counter-terrorism program, the legal framework, institutional knowledge, and connections to the financial community were already in place to allow for the swift and effective use of economic sanctions. The President issued a new Executive Order to address the threat on September 23, 2001, and OFAC moved to block the assets of several al Qaida support organizations before that year's end. OFAC's exceptional institutional capacity and experience in administering sanctions has allowed it to become a model and advisor for other governments in the post-9/11 world.

As I previously noted, in the five years since, OFAC has designated 375 individuals and entities as supporters of terrorism, blocking their assets and—more importantly—cutting them off from the U.S., and frequently the international, financial systems. In close coordination with colleagues in the Treasury Department, and at the Departments of State and Justice, we have exposed the financial networks of terror groups including al Qaida, Hizballah, Hamas, Jemmah Isalmiyya, and the GSPC, and designated financiers and companies in Southeast Asia, the Persian

Gulf, the Horn of Africa, South America's TriBorder Area, Europe, and the United States.

When we have acted against terrorist supporters in the United States, we have coordinated especially closely with the Federal Bureau of Investigation and other U.S. law enforcement agencies through the Joint Terrorist Task Forces. Indeed, some of our most effective actions have been joint operations, taken in concert with law enforcement. In February 2004, federal agents executed a search warrant on Al Haramain, pursuant to a joint investigation by IRS–CI, the FBI, and DHS/ICE. Simultaneously, Treasury's OFAC blocked the accounts of the organization pending investigation, freezing the organization's assets in place and ensuring that no money would flow through this group during further investigation. A similar coordinated Treasury/law enforcement action was taken in October 2004 against the Islamic African Relief Agency (IARA), and its U.S. alias, the Islamic American Relief Agency. Treasury designated this global network as well as five of its senior officials as Specially Designated Global Terrorists pursuant to E.O. 13224. On the same day, the FBI raided IARA's headquarters in Columbia, Missouri as part of a separate criminal investigation.

Time does not allow for a full review of OFAC's terrorist designations and successes in detail, but I would like to highlight some of our most recent actions.

Last month, we designated two overseas branches of the International Islamic Relief Organization (IIRO), which is headquartered in Saudi Arabia, as well as Abd al Hamid Sulaiman Al-Mujil, the head of IIRO's branch in the Eastern Province of Saudi Arabia. These branch offices, while holding themselves out as purely charitable organizations, were bankrolling the al Qaida network in Southeast Asia. In July, we designated Muhammad Ahmed 'Abd Al-Razziq, a Canadian and Sudanese national who provided administrative and logistical support for al Qaida.

We have also taken a string of recent actions to disrupt and undermine Hizballah's financial network. Of course, the U.S. has long recognized Hizballah as a deadly terrorist organization but the recent fighting in Lebanon provided a stark reminder of how dangerous and well-supplied this terrorist organization is.

Two weeks ago, we designated the Islamic Resistance Support Organization (IRSO), a so-called "charity" operated by Hizballah. IRSO offered donors the option of earmarking their donations to equip Hizballah fighters or to purchase rockets. Just last week, OFAC designated Bayt al-Mal and the associated Yousser Company, which together functioned as Hizballah's unofficial treasury, holding and investing its assets and serving as intermediaries between Hizballah and the mainstream banks. At the same time, we designated Husayn al-Shami, a senior Hizballah leader and financial facilitator. These actions, driven by the intelligence work of TFI's Office of Intelligence and Analysis, and coordinated closely with our interagency partners, exposed and attacked some of Hizballah's most prominent financial entities. The world financial community is now on notice as to their true character.

Iran as a State Sponsor of Terrorism

Of course, one cannot hope to apply effective financial pressure against a group like Hizballah so long as it maintains massive inflows of cash from a state sponsor of terrorism, in this case the Iranian Government. OFAC administers a range of sanctions against Iran, the world's leading government sponsor of terrorism, aimed at limiting the regime's financial reach and pressuring it to cease its hostile and destabilizing activities.

In a small exception to this general sanctions program, we have allowed Iranian banks to access the U.S. financial system indirectly, through third-country intermediaries. This past Friday, we took regulatory action to cut off Iran's Bank Saderat from even indirect access to the U.S. financial system. We took this action because Bank Saderat has been a significant facilitator of Hizballah's financial activities and has served as a conduit between the Government of Iran and a range of terrorist groups, including Hizballah, Hamas, the Popular Front for the Liberation of Palestine-General Command (PFLP–GC), and the Palestinian Islamic Jihad (PIJ). As Under Secretary Levey said in announcing this action on Friday, "we will no longer allow a bank like Saderat to do business in the American financial system, even indirectly."

Weapons of Mass Destruction

Recent events involving the nuclear programs of both North Korea and Iran make clear the very serious and real challenges that we and the whole international community face. Recognizing that we must use all of our national authorities to prevent a weapon of mass destruction from falling into the wrong hands, the President issued Executive Order 13382 in June 2005, authorizing the Treasury and State Departments to designate and freeze the assets of proliferation entities and those that

facilitate their activities. This authority is a powerful one, as the suppliers, financiers, transporters and other facilitators of WMD networks tend to have commercial presences and accounts around the world that make them vulnerable to exactly this kind of financial action.

In issuing the Executive Order, the President identified eight entities in North Korea, Iran, and Syria, making them immediately subject to the prohibitions set forth in the Order. OFAC's WMD investigation team provided the evidence for these designations, and has continued to track and expose proliferation networks around the world. In the past year, OFAC has designated 19 proliferation entities and one individual under this order. Notable targets have included:

- Sanam Industrial Group and Ya Mahdi Industries Group, both subordinates to Iran's Aerospace Industries Organization (AIO), which manages and coordinates Iran's missile program and oversees all of Iran's missile industries. The Sanam Industrial Group has purchased millions of dollars worth of equipment on behalf of AIO from entities associated with missile proliferation. Ya Mahdi Industries Group also has been involved in international purchases of missile-related technology and goods on behalf of AIO.
- Chinese companies Beijing Alite Technologies Company, Ltd. (ALCO), LIMMT Economic and Trade Company, Ltd., China Great Wall Industry Corporation (CGWIC), and China National Precision Machinery Import/Export Corporation (CPMIEC), as well as a U.S. office of CGWIC located in California. These companies supplied Iran's military and Iranian proliferators with missile-related and dual-use components.
- Swiss company Kohas AG, which acted as a technology broker in Europe for the North Korean military and procured goods with weapons-related applications, and its president, Swiss national Jakob Steiger. Both Kohas and Steiger have been involved in activities of proliferation concern on behalf of North Korea since the late 1980s.

Our actions have cut these entities off from the U.S. financial system and alerted international banks and companies to avoid these designated firms. We have also sent a loud message to any companies that might be considering engaging in proliferation activities that this line of business now comes with severe risks.

Conclusion

Together with my colleagues at this table and throughout the government, we will continue to employ all of our resources and authorities to keep our country safe. We greatly appreciate the continuing interest and oversight of this committee. Thank you for your support.

PREPARED STATEMENT OF ROBERT W. WERNER

DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK,

SEPTEMBER 12, 2006

Chairman Shelby, Senator Sarbanes, and distinguished members of the Committee, I appreciate the opportunity to appear before you today to discuss the Financial Crimes Enforcement Network's (FinCEN) ongoing initiatives and efforts to combat money laundering and terrorist financing in the post 9/11 world. This hearing is especially appropriate following yesterday's fifth anniversary of the vicious terrorist attacks against this country. As the Director of FinCEN, which is the agency responsible for administering the Bank Secrecy Act (BSA)—the United States' primary anti-money laundering/counter-terrorist financing regulatory regime, I welcome the opportunity to work with the Members of this Committee in our united fight to safeguard the U.S. financial system against financial crime. I also greatly appreciate all the support and guidance this Committee has provided over the past five years.

I am also pleased to be testifying with my colleagues from other components of Treasury. Each of these offices plays an important role in the global fight against money laundering and terrorist financing, and our collaboration on these issues has greatly improved the effectiveness of our efforts.

As you know, FinCEN's mission is to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity. FinCEN works to achieve its mission through a broad range of interrelated activities, including:

- Administering the Bank Secrecy Act;

- Supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of financial intelligence; and
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

To accomplish these activities, FinCEN utilizes a team comprised of approximately 300 dedicated federal employees, including analysts, regulatory specialists, international specialists, technology experts, administrators, managers, and Federal agents who fall within one of the following areas of expertise at FinCEN:

- **Analysis and Law Enforcement Support**—FinCEN provides federal, state, and local law enforcement and regulatory authorities with different methods of direct access to reports financial institutions file pursuant to the BSA. FinCEN also combines BSA data with all-source information to produce analytic products supporting the needs of law enforcement, intelligence, regulatory, and other financial intelligence unit customers. Products range in complexity from traditional subject-related research performed by contract analysts to more advanced analytic work including geographic assessments of money laundering threats.
- **Global Support**—FinCEN is one of more than 100 recognized national financial intelligence units around the globe that collectively constitute the Egmont Group. FinCEN plays a lead role in fostering international efforts to combat money laundering and terrorist financing among these financial intelligence units, focusing our efforts on intensifying international cooperation and collaboration, and promoting international best practices to maximize information sharing.
- **Regulatory Policy and Programs**—FinCEN issues regulations, regulatory rulings, and interpretive guidance; assists state and federal regulatory agencies in targeting and consistently applying BSA compliance standards in their examination of financial institutions; and takes enforcement action against financial institutions that demonstrate systemic non-compliance. These activities span the breadth of the financial services industry, including—but not limited to—banks and other depository institutions; money services businesses; securities broker-dealers; futures commission merchants and introducing brokers in securities; dealers in precious metals, stones, or jewels; insurance companies; and casinos.

Tying It All Together

FinCEN's goal is to increase the transparency of the U.S. financial system so that money laundering, terrorist financing, and other economic crime can be deterred, detected, investigated, prosecuted—and, ultimately, prevented. Our ability to tie together and integrate our regulatory, international, and law enforcement efforts assists us to achieve consistency across our regulatory regime.

In addition, the BSA data received through Currency Transaction Reports, Suspicious Activity Reports, and other forms have proved to be highly valuable to our law enforcement customers, who use the information on a daily basis as they work to investigate, uncover, and disrupt the vast networks of money launderers, terrorist financiers and other criminals.

Additionally, we strive to use the BSA regulatory regime as an avenue for building partnership between the government and private sector, which is critical in order to achieve the goals of the system. Specifically, we do this in two major ways:

- First, requiring financial institutions subject to the BSA to develop risk-based anti-money laundering programs tailored to their businesses, and provide guidance in this regard. Such programs include the development and implementation of policies, procedures, and internal controls needed to address money laundering, terrorist financing, and other risks posed by that financial institution's products, geographic locations served, and customer base; and,
- Secondly, requiring financial institutions to maintain records and report certain information that is important to the detection, deterrence and investigation of financial crime.

We have learned that in order for this system to work, the government must provide guidance and feedback to the industry in ways that support their understanding of potential vulnerabilities, effective ways to address those vulnerabilities and the benefits derived from information reported by them. The risk-based nature of the regulatory scheme also recognizes that financial institutions are in the best position to design anti-money laundering/counter-terrorist financing programs that address the specific risks that they face. In other words, the success of this regime

depends upon the government and financial institutions acting in true partnership—each committed to the goal of taking reasonable steps to ensure that the financial system is protected from criminals and terrorists to the greatest extent possible through the development of appropriate programs and the sharing and dissemination of information.

Ensuring that we strike the right balance between the cost and benefit of this regulatory regime is, in my view, one of FinCEN's central responsibilities. Accordingly, it is vital that we continue to examine how we can more effectively tailor this regime to minimize the costs borne by financial institutions while at the same time ensuring that the law enforcement, intelligence, and regulatory communities receive the information they need.

Recent Accomplishments

Over the past year, we made great strides toward enhancing BSA compliance. For example, we signed a memorandum of understanding (MOU) with the Internal Revenue Service (IRS) to routinely exchange information about BSA examination activities, including the identification of IRS-examined financial institutions with significant BSA compliance deficiencies. We also have similar agreements with the five federal banking agencies and have negotiated 42 memoranda of understanding—or information sharing agreements—with state and territorial supervisory agencies that examine for their own rules on BSA/anti-money laundering compliance. In addition, we collaborated with the federal banking agencies and the Office of Foreign Assets Control to develop and publish an interagency Bank Secrecy Act/Anti-Money Laundering Examination Manual that is designed to ensure the consistent application of the BSA. Further, we extended BSA anti-money laundering program requirements to dealers in precious metals, precious stones, or jewels and certain insurance companies; finalized proposed regulations regarding due diligence requirements in connection with foreign correspondent and private banking accounts; required mutual funds and certain insurance companies to report suspicious activity; and have issued important guidance to the money services businesses industry.

FinCEN is also placing a stronger emphasis on producing more advanced analytic products rather than engaging in basic database queries. For example, analysis of BSA filing patterns enables us to conduct geographic threat assessments that assist law enforcement agencies to allocate limited resources. By identifying increases—or decreases—in filing activities, law enforcement can determine where vulnerabilities may exist and how to adjust their staffing levels accordingly. This proactive data analysis of BSA filings also supports our regulatory rulemaking process. For instance, our regulatory policy specialists are able to use the valuable data provided by financial institutions to identify where additional regulation may be needed and to identify evolving trends in illicit finance.

As the United States' financial intelligence unit (FIU), we collaborate with other FIUs worldwide to exchange information in support of international and terrorist financing cases. To that end, FinCEN developed the Egmont Secure Web to provide a secure system to exchange sensitive information with our foreign counterpart FIUs. FinCEN is currently modernizing this system to enhance its security and increase communication capabilities. FinCEN also plays a significant role in assisting other countries in developing their FIUs by providing technical assistance ranging from analytical training as well as IT and regulatory support. We also sponsor new FIUs for membership in the Egmont Group. In 2005, FinCEN hosted the 13th Plenary of the Egmont Group, which was attended by nearly 300 delegates from more than 90 FIUs from countries and jurisdictions around the world. At the Plenary, seven new FIUs were granted membership, bringing the total to 101. We will continue to work to make this network of FIUs more effective by encouraging information sharing and joint projects.

Lastly, FinCEN continued to strengthen both the policies and technology relating to the information-sharing program authorized under Section 314 of the USA PATRIOT Act. We developed and deployed a secure, web-based system for transmitting information requests from federal law enforcement agencies to financial institutions, and for transmitting the institutions' responses to those requests. Previously, information requests were transmitted via a slower and less secure system of e-mail and faxes.

Cross-Border Wire Feasibility Study

Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004 (S. 2845, Pub. L. No. 108–458, Dec. 17, 2004) directs the Secretary of the Treasury to prescribe regulations to require the reporting to FinCEN of certain cross-border electronic transmittals of funds to help detect and prevent the proceeds of financial crimes and terrorist financing from flowing across America's borders. The Act re-

quires the Secretary to issue these regulations by December of 2007, if he can certify that the technical capability to receive, store, analyze, and disseminate the information is in place prior to any such regulations taking effect. Finally, the Act also requires that, in preparation for implementing the regulation and data collection system, the Treasury Department study the feasibility of such a program and report its conclusions to Congress.

For the purposes of this study, FinCEN has engaged members of the financial services industry, the federal financial regulatory agencies, and federal law enforcement agencies through the Bank Secrecy Act Advisory Group,[1] which includes representatives of the U.S. financial services industry, law enforcement, and federal and state financial regulatory agencies. We have also engaged separately with our partners in the law enforcement community, through meetings with their representatives and through the distribution of surveys to those agencies, in order to assess what value might be derived from such reporting in the context of their missions. And we have conducted similar meetings with our regulatory partners.

Canada and Australia already require the reporting of cross-border wire transfers to their Financial Intelligence Units (FINTRAC and AUSTRAC, respectively). In that regard, both FINTRAC and AUSTRAC have provided us with extensive assistance through demonstrations of their respective reporting systems and sharing their views of best practices and lessons learned from the design and implementation of their regimes.

Through these efforts, FinCEN has identified the potential value in collecting cross-border electronic wire transfer information and potential avenues for combining that data with other BSA data. FinCEN has also identified a number of policy-related concerns implicated by the proposed requirement, which arose from feedback FinCEN has received from numerous financial industry representatives and the five federal banking agencies. Chief among these concerns is how to protect the privacy of individuals about whom we collect information. Another significant concern are the costs U.S. financial institutions may incur in complying with such a reporting requirement. Last, there is some concern about the potential impact of the proposed reporting requirement on the day-to-day operations of electronic funds transfer systems in the United States. Our feasibility study will outline these issues and propose an approach for resolving them.

BSA Direct

We have also taken steps to address significant issues that have arisen over the past year. One such matter involved certain aspects of our BSA Direct project. BSA Direct is an overall umbrella project with several components, including: retrieval and sharing, electronic filing, and secure access. The electronic filing and secure access components of BSA Direct have been operational for a number of years. The retrieval and sharing development began conceptually in September of 2003, with a contract awarded on June 30, 2004. The retrieval and sharing (R&S) component of BSA Direct was, in part, aimed at improving authorized users' access and ability to analyze the BSA data. It was designed to apply data warehousing technology to structure the data in a single, integrated, secure web-based environment, and provide sophisticated business intelligence and other analytical tools in a user-friendly web portal. Under this design, law enforcement and regulatory agencies would gain easier, faster data access and enhanced ability to query and analyze the BSA data—improvements that were expected to lead to increased use of the BSA data and enhancements of its utility.

On March 15, 2006, I notified Congress of my intent to issue a temporary 90-day "stop-work" order on this project. This action was necessary due to the project's inability to meet performance milestones. An assessment team, comprised of management, analysts, technology specialists, and independent consultants, was created shortly after the issuance of the stop-work order to assess and refine core requirements for BSA information retrieval, dissemination, sharing, and analysis; to determine whether this component of BSA Direct could be salvaged and/or leveraged by other alternatives; and to define the best path to ensure business continuity.

On July 10, 2006, the assessment team reported its findings and concluded that BSA Direct R&S was a partially built system that integrated a number of best-in-class products that did not, in its present state, function well together. As a result,

[1] Congress established the Bank Secrecy Act Advisory Group (the "BSAAG") in 1992 to enable the financial services industry and law enforcement to advise the Secretary of the Treasury on ways to enhance the usefulness of Bank Secrecy Act reports. Since 1994, the Advisory Group has served as a forum for industry, regulators, and law enforcement to communicate about how law enforcement uses Suspicious Activity Reports, Currency Transaction Reports, and other Bank Secrecy Act reports and how FinCEN can improve the reporting requirements to enhance their utility while minimizing the burden on financial institutions.

the system could not be deployed to any of FinCEN's users in the short term. Moreover, FinCEN, the contractor, and our external consultants could not definitively predict how close the system was to meeting the envisioned requirements or the time, resources, and risks involved in completing the system.

Based on these findings, the assessment team recommended that FinCEN terminate the existing contract, assess immediate needs, and plan for new capabilities. Based on the underlying information and analysis, I supported this recommendation and, therefore, on July 13, 2006, I terminated the BSA Direct R&S contract.

As we move forward, FinCEN will initiate a re-planning effort for BSA Direct R&S, to address strategic, technical, and resource planning issues, as well as stakeholder analysis. In addition, we will continue our efforts with the Internal Revenue Service to implement WebCBRS as an immediate means of meeting internal and customer needs for BSA data query and analysis tools.

Money Services Businesses

Another significant issue that FinCEN has faced and continues to face relates to the money services business industry. There has been mounting concern among FinCEN and others at the Department of the Treasury, various financial regulators, and the money services business industry regarding the ability of money services businesses to establish and maintain banking services. Many banks have expressed an uncertainty with respect to the appropriate steps they should take under the BSA to manage potential money laundering and terrorist financing risks associated with this industry. At the same time, the money services business industry has expressed concern that misperceptions of risk have unfairly led to labeling them as "unbankable."

Individual decisions to terminate account relationships, when compounded across the U.S. banking system, have the potential to result in a serious restriction in available banking services to an entire market segment. The money services business industry provides valuable financial services, especially to individuals who may not have ready access to the formal banking sector.

Consequently, it is important that we maintain the ability of money services businesses that comply with BSA requirements and related state laws to do business through the formal financial system, subject to appropriate anti-money laundering controls. Equally important is ensuring that the money services business industry maintain the same level of transparency, including the implementation of a full range of anti-money laundering controls, as do other financial institutions. The risk of money services business account relationships being terminated on a widespread basis is that many of these businesses could go "underground." This potential loss of transparency would, in our view, significantly damage our collective efforts to protect the U.S. financial system from financial crime—including terrorist financing. Clearly, resolving this issue is critical to safeguarding the financial system.

In March of 2005, the Non-Bank Financial Institutions and the Examination subcommittees of the Bank Secrecy Act Advisory Group jointly hosted a fact-finding meeting to solicit information from banks as well as money services businesses on issues surrounding the provision of banking services to the money services business industry. Subsequently, in April of 2005, FinCEN and the federal banking agencies issued interagency guidance to the banking industry on the provision of banking services to domestic money services businesses. FinCEN issued a companion advisory to money services businesses on what they should expect when obtaining and maintaining banking services.

Currently, based upon what we learned at the March 2005 meeting, and in subsequent discussions with other federal and state regulators, law enforcement, and the industry, we have developed and are implementing a three-point plan for addressing these issues:

1. *Guidance*—that outlines with greater specificity BSA compliance expectations when banks maintain accounts for money services businesses.
2. *Education*—that provides banks and bank examiners enhanced awareness of the operation of the variety of products and services offered by money services businesses and the range of risks that each may pose.
3. *Regulation*—that strengthens the existing federal regulatory and examination regime for money services businesses, including coordinating with state regulators to better ensure consistency and leveraging of examination resources.

With respect to the issues surrounding the provision of banking services to money services businesses, we are considering additional actions, guidance, and outreach necessary to address this issue. For example, in March of 2006, we published an advance notice of proposed rulemaking to seek additional information from the

banking and money services business industries on this issue. The comment period, which closed in July, provided us a number of insights that we will consider as we move forward on this issue.

In conclusion, Mr. Chairman, we are grateful for your leadership and that of the other Members of this Committee on these issues, and we stand ready to assist in your continuing efforts to ensure the safety and soundness of our financial system. Thank you for the opportunity to appear before you today. I look forward to any questions you have regarding my testimony.

PREPARED STATEMENT OF EILEEN C. MAYER

DIRECTOR, FRAUD/BANK SECRECY ACT OF SMALL BUSINESS/SELF EMPLOYMENT DIVISION, INTERNAL REVENUE SERVICE

SEPTEMBER 12, 2006

Good morning Chairman Shelby, Ranking Member Sarbanes, and the members of the Senate Committee on Banking, Housing, and Urban Affairs. My name is Eileen C. Mayer and I am the Director of Fraud/Bank Secrecy Act (BSA) within the Small Business/Self Employed (SB/SE) division of the Internal Revenue Service (IRS). My office is assigned the responsibility to fulfill the IRS' obligations under the Bank Secrecy Act as well as coordinating the establishment of Service-wide fraud strategies, policies, and procedures. My office also provides fraud referral coordination for all operating divisions of the IRS.

IRS' role in administering the BSA is derived from statutory authority given to the Secretary of the Treasury to administer the provisions of the Act. He in turn delegated that authority to the Director of the Financial Crimes Enforcement Network (FinCEN). FinCEN retained some authorities but delegated others. Specifically, the IRS was delegated the authority to examine, for BSA compliance, all financial institutions not currently examined by a Federal functional regulator. These entities include money services businesses (MSBs), such as check cashers, issuers of traveler's checks, and money transmitters, casinos, certain credit unions that are not otherwise regulated by the Federal Government, dealers in jewelry and precious metals and insurance companies.

Emphasis on Customer Service

Under the leadership of Commissioner Everson, the IRS has taken a balanced approach to tax compliance, one that emphasizes service as well as enforcement. Many MSBs are small businesses and in some cases sole proprietorships. As a result, they may not fully understand their responsibilities under the BSA.

An important part of fulfilling our responsibilities under the BSA is to work closely with our office of Communications, Liaison and Disclosure (CLD) to identify those areas where education and outreach efforts can be most productive. We also have BSA outreach specialists within Stakeholder Liaison (SL), located in the six top high risk money laundering and related financial crime areas: Miami, New York, Chicago, Houston, San Francisco, and Los Angeles.

Stakeholder Liaison has expended a great deal of its resources during FY 06 in reaching out to MSBs on two fronts: one through local/regional/national outreach events and the other through direct contacts with MSB entities. To date, our BSA Stakeholder Liaisons have spoken at 41 events hosted by various MSB organizations and associations on such topics as MSB registration and BSA compliance program requirements. In addition to key-note speaker requests, they have also appeared on radio talk shows, phone forums and taped industry educational programs.

In July 2006, our BSA outreach specialists began contacting MSBs that either have failed to renew their registration or who may be unaware of their registration obligation. The entities are being sent a FinCEN-approved letter and fact sheet, along with an MSB registration form (FinCEN 107). These contact letters will be followed by a personal phone call by a BSA Stakeholder Liaison in order to determine the correct status of the business and to answer any questions they may have about the registration process. The combination of outreach and direct interaction with MSBs is establishing a strong bond with the MSB community that will only grow stronger over time.

In addition, we are revising our BSA Internal Revenue Manual and once it is finalized we will make it available to all MSBs – including via the internet. We plan to convert the manual to a more user-friendly format similar to the manual created by the Federal Financial Institutions Examination Council.

Coordination with Other Groups

In our efforts to assure compliance with the provisions of the BSA, we have been pleased to partner with the other agencies represented at the hearing today. While each of the groups has distinct responsibilities relative to the BSA, we all must work cooperatively to be most effective in monitoring and preventing questionable transactions.

For example, we are working with the Office of Foreign Assets Control (OFAC) to leverage our resources. OFAC has an information sheet for MSBs on its web site. In order to reach MSBs about the OFAC requirements, we are printing 10,000 of these information sheets, and will include them in the letter we send to MSBs that informs them that they may be subject to regulatory requirements under the BSA. Our examiners will also give the sheet to any MSB that they examine.

We are working with Treasury and OFAC on a delegation that would allow us to ask OFAC-compliance-related questions during our BSA examinations of MSBs. In addition, to increase the awareness of our examiners about the OFAC requirements, OFAC provided a speaker for our Continuing Professional Education (CPE) session this summer. The audience included all BSA managers and examiners.

We are also working closely with the states. As evidence of that cooperation, Commissioner Everson was pleased to announce in late April that we had reached agreements with 33 states and Puerto Rico to begin sharing BSA information. The agreements will allow the IRS and the participating states to leverage their resources to ensure that MSBs are complying with their federal and state responsibilities to register with the government, to create and maintain anti-money laundering programs, and to report cash transactions and suspicious activities. This would have not been possible without the support and assistance of FinCEN.

And, we, of course, have a very close working relationship with FinCEN. We have a memorandum of understanding in place which provides for exchanges of information to help FinCEN fulfill its role as administrator of the BSA and to assist us in conducting examinations of MSBs to assess BSA compliance. IRS and FinCEN work closely on such things as setting examination priorities, reviewing the BSA Internal Revenue Manual, and training. As I will discuss in more detail later, we also refer all potential BSA civil penalty cases to FinCEN for appropriate action.

IRS also is a member of the Money Laundering Threat Assessment working group, along with FinCEN. The focus of this group is to identify money laundering threats throughout the United States through investigations conducted by all law enforcement agencies.

IRS Enforcement

In recent years, the IRS has strengthened the focus on enforcement, while maintaining appropriate service to taxpayers. Detecting and investigating money laundering activity is an important part of tax compliance for the IRS. In addition, the failure to file forms required by the BSA and criminal violations of the BSA, including the structuring of deposits to avoid currency transaction reporting requirements, often have a direct link to tax evasion and money laundering. In some cases, because the schemes are sophisticated and because we may not be able to obtain evidence from some foreign countries, it is almost impossible to conduct traditional tax investigations. In these circumstances, money-laundering violations frequently are the only possible means to detect tax evaders.

Money laundering not only is used by domestic and international criminal enterprises to conceal the illegal, untaxed proceeds of narcotics trafficking, arms trafficking, extortion, public corruption, terrorist financing, and other criminal activities; it is also an essential element of many tax evasion schemes. With the globalization of the world economy and financial systems, many tax evaders exploit domestic and international funds transfer methods to hide untaxed income. These schemes often involve the same methods to hide money from illegal sources and to hide unreported income. Both activities generally use nominees, wire transfers, multiple bank accounts, and international "tax havens" to avoid detection.

Money laundering is the financial side of virtually all crime for profit. To enjoy the fruits of their crime, criminals must find a way to insert the illicit proceeds of that activity into the stream of legitimate commerce in order to provide the resources necessary for criminal organizations to conduct their ongoing affairs.

IRS' Role in BSA Compliance

As part of its core tax administration mission, the IRS addresses both the civil and criminal aspects of money laundering. On the civil side, the Department of the Treasury, through FinCEN, has delegated to the IRS responsibility for ensuring compliance with the BSA for all non-bank financial institutions (NBFIs) not other-

wise subject to examination by another federal functional regulator, including MSBs.

Under this FinCEN delegation, the IRS is responsible for three elements of compliance:—(i) the identification of MSBs, (ii) educational outreach to all NBFIs, and (iii) the examination of those entities for compliance.

Currently, there are nearly 27,000 MSBs registered and posted on the FinCEN website. However because the true universe of potential MSBs is unknown, we utilize several methods to identify unregistered MSBs. One method is to utilize information from the states that identifies businesses that are registered at the state level but not with FinCEN. We also review our Currency Banking and Retrieval System (CBRS) data base to discover suspicious activity reports (SARs) or currency transaction reports (CTRs) that emanate from or are filed on entities that should be registered. We also get leads from other Federal agencies such as Immigration and Customs Enforcement. Finally, we receive anecdotal reports on entities that are not registered but who are doing check cashing or other financial activities that would subject them to registration requirements

In FY 2006, we started a special initiative to identify businesses that should be registered but are not. We built 2000 real cases that were used to train our newest examiners. We have been pleased with the results and plan to continue this type of initiative in the future.

Our outreach program is designed to reach both registered and unregistered MSBs. We focus special attention on those industries that FinCEN has referred to us. For example, currently we are working with convenience store owners and gasoline retailers, many of whom are MSBs and may not even realize it. We work closely with the trade associations that represent specific MSBs, making sure they understand the requirements that their members face. We also make ourselves available for seminars at association events and as exhibitors at their trade shows. We also look at industries where we suspect that there may be high incidences of non-registration and work closely with them to make sure they understand the registration requirements.

From a criminal perspective, IRS' Criminal Investigation (CI) Division is responsible for the criminal enforcement of the BSA and money laundering statutes related to tax crimes. CI uses the BSA and money laundering statutes to detect, investigate, and prosecute criminal conduct related to tax administration, such as abusive schemes, offshore tax evasion, and corporate fraud. CI also investigates criminal violations of the BSA, including the structuring of deposits to avoid currency transaction reporting requirements, which frequently have a direct link to both tax evasion and money laundering.

The IRS CI Division has increased its emphasis on BSA responsibilities significantly, with particular focus on improving the effectiveness and efficiency of SAR Review Teams. CI now hosts approximately 80 SAR Review Teams located throughout its 30 field offices. These teams are made up of federal, state and local law enforcement officials and work closely with Assistant United States Attorneys. The expansion in the number of teams significantly enhances analysis of SARs because each team can focus on the geographical area with which it is most familiar. Increased use of technology, primarily data-mining tools, is assisting teams in efficiently analyzing the ever-increasing number of SARs being filed.

MSB Compliance

The BSA imposes several requirements on money services businesses. These include:

- The development and implementation of an adequate Anti-Money Laundering (AML) compliance program. An effective program is one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities. Such a plan must include the following elements: (a) a system of internal controls to assure compliance; (b) the designation of an individual responsible for coordinating and monitoring day-to-day compliance; (c) the provision of training for appropriate personnel; and (d) the provision for independent review to monitor and maintain an adequate program.
- A requirement that MSBs file a report of each deposit, withdrawal, exchange of currency or other payment or transfer which involves a transaction of currency of more than $10,000; and,
- A requirement that "suspicious transactions" be reported. The BSA and its implementing regulations have defined what might be classified as a suspicious transaction. They include such things as transactions that involve funds gained from illegal activities or that are designed to evade reporting

or recordkeeping requirements under the BSA, or transactions in which the particular customer would normally not engage.

IRS Examinations

It is important to point out that all of the IRS BSA examiners and their managers devote 100 percent of their examination time to examinations of BSA-related cases. This contrasts with our efforts in 2004 and before when BSA work was a collateral duty of revenue agents who were engaged in traditional income tax audits.

We currently have 353 BSA examiners on board. We had hoped to have 385 by the end of FY 2006, but we will not make that goal despite our best efforts. We will be recruiting actively on a number of fronts in FY 2007 to increase our workforce to the maximum level, and to keep it there.

As the BSA program has grown, we have changed some of the focus of our exams. Today, we examine both the corporate headquarters of MSBs and their agents which, according to the BSA, are MSBs in their own right. In addition, unlike the federal banking and securities regulators, the IRS is not obligated to undertake examinations on any particular cycle. And due to the size of the MSB population, that would be prohibitive. As a result, our examination plan is largely determined on a risk basis and by the relative size of the institutions for which we are responsible. Large MSBs are examined as a matter of course, with the IRS performing a centralized examination of the MSBs corporate headquarters. Smaller MSBs are targeted for an audit if they have been identified as high risk, including at risk for terrorist financing, as determined by leads from other federal or state agencies and the entity's SAR filing history. Once we determine what entity to examine, as explained below, the extent of our exam is based on an analysis of the risks posed in that particular institution.

We are also now utilizing a centralized case selection process. The Treasury Inspector General for Tax Administration (TIGTA) has previously scrutinized our work selection process, observing that current processes create a significant risk of undetected non-compliance and inconsistent program delivery. As a result, we are developing a systematic, risk-based inventory selection process. This process is based on a scoring system that uses data from the CBRS to identify the best candidates for examination. We are currently field testing that scoring system.

Once we identify a particular MSB for examination, our first step is to request from the entity a copy of its anti-money laundering compliance program and a copy of the independent audit of the compliance program. The examiner will then prepare a risk-based assessment that essentially determines the scope of the rest of the examination.

During the course of the exam, the examiner will identify the entity's AML risks, evaluate policies, procedures, and internal controls and assess whether breakdowns in the AML compliance program place the institution at risk for money laundering or terrorist financing. We will then always perform selective transactional testing.

Upon completion of the examination, one of four outcomes will occur. First, if no violations are found, we will issue what we call Letter 4029, which gives the entity documentation that a review has occurred and that no violations were identified. This is important because we are well aware that many MSBs are facing increasing difficulty in finding banks willing to do business with them. These banks, both large and small, seem to believe that opening new or maintaining existing accounts for money services businesses will be too costly, pose a potential threat to their reputation, or expose them to greater regulatory scrutiny.

This is regrettable. The money services business industry provides valuable financial services, especially to individuals who may not have ready access to the formal banking sector. It is long-standing Treasury policy that a transparent, well-regulated money services business sector is vital to the health of the world's economy. It is important that money services businesses that comply with the requirements of the Bank Secrecy Act and applicable state laws remain within the formal financial sector, subject to appropriate anti-money laundering controls.

It is equally important to ensure that the money services business industry maintains the same level of transparency, including the implementation of a full range of anti-money laundering controls required by law, as do other financial institutions. If account relationships are terminated on a wide-spread basis, we believe many of these businesses could go "underground." This potential loss of transparency would significantly damage our collective efforts to protect the U.S. financial system from money laundering and other financial crimes – including terrorist financing.

The second possible outcome of an examination would be the issuance of a Letter 1112 (L–1112). The L–1112 would be issued if violations are found, but they are technical, minor, infrequent, isolated, and non-substantive. This letter will detail the violations and ask that the entity commit to correct the apparent violations. It

also provides the business with the opportunity to disagree with the findings and to provide us within 30 days an explanation of any disagreement.

It is important to realize that the issuance of an L–1112 involves no fines or other penalties on the MSB. It merely says that we have found these violations and that by signing the letter, the business agrees to correct the deficiencies that were noted.

The third potential outcome of an examination is an instance where a significant BSA violation or deficiency is identified. In this instance, the case is referred to FinCEN for consideration of civil penalties. Examples in this category are violations that are flagrant, demonstrated bad faith, or were committed with disregard for the law or the consequences to the institution. Other factors in considering whether to refer a matter to FinCEN include: (a) the frequency of violations; (b) whether the violation is intentionally concealed; (c) whether the business fails to cooperate in correcting the violation; and (d) the history of prior violations and/or poor compliance. Thus, field examiners are given a clear list of criteria to consider in determining whether to refer a case to FinCEN.

Once a case is referred to FinCEN, the IRS is no longer involved. FinCEN makes the determination of what, if any, civil penalty is appropriate.

Finally, if the examiner believes that there may be a willful criminal violation involved, the case would immediately be referred to IRS-Criminal Investigation when the relevant facts have been developed. CI will evaluate the case and determine whether it reaches the level of criminal behavior and meets certain minimum case selection criteria. From a legal perspective, one of the most difficult issues facing CI in deciding if a case is worthy of a criminal investigation is documenting sufficient evidence of affirmative acts to establish willfulness. Willfulness can be difficult to prove and when dealing with the Bank Secrecy Act violations, it often requires documenting a subject's knowledge of their obligations under the BSA.

From a practical perspective, case selection is another key factor in determining whether a case will be successfully prosecuted. Our CI division has vast experience in determining the prosecution potential of cases selected for investigation, evidenced by a 96.3% acceptance rate at the Department of Justice and a 92.2% acceptance rate at the United States Attorneys Offices for Fiscal Year 2005.

If CI makes the determination that they will not refer the case to the Department of Justice for review, it comes back to us and we decide whether to then refer it to FinCEN for consideration of possible civil penalties.

If an MSB believes that an examiner has made a mistake in his or her assessment of potential violations, there is recourse. As noted above, if the MSB is issued an L–1112 letter, it has 30 days in which to respond, explaining why the examiner is wrong. The MSB can also elevate the issue to the BSA Territory Manager or contact FinCEN through their hot line number, posted on their website.

To give you an idea of the universe of MSB cases we audit, in FY 2005, we examined 3,680 MSBs. We issued L–1112 violation letters to 1,337 of these. We referred 21 cases for criminal investigation and referred 7 cases to FinCEN.

As of August 25, of this fiscal year, we had already examined 5,481 MSBs and issued violation letters to 3,585 entities. We have also issued 1,744 Letters 4029, indicating clean examinations. We have referred 14 cases to CI and 17 cases to FinCEN.

Our draft BSA workplan for FY 2007 includes the examination of 6,756 MSBs. This is in addition to casinos, credit unions, insurance companies and jewelers. The FY 2007 plan represents an 8 percent increase over FY 2006 and a 83 percent increase from the FY 2005 workplan. The FY 2007 plan is premised on the assumption that we accomplish our aggressive hiring initiative.

New Industries

One of the questions raised by the Committee's staff prior to this hearing was how we are addressing the new FinCEN regulations of jewelers and insurance companies. In terms of jewelers, FinCEN has advised us that these regulations are not final. Until they are, we have been told by FinCEN not to conduct exams. In the meantime, the Service has developed an implementation strategy which encompasses examinations, monitoring, and training. We have met with representatives from the industry to discuss what they plan to do to implement the regulations and to also discuss their concerns.

For the insurance industry, in conjunction with the BSA examinations, we are assisting insurance companies, as necessary, through our partnership with FinCEN, in understanding their obligations under the BSA. We have developed a strategy and implementation plan for insurance companies that encompass examinations, monitoring and training. The training curriculum is in the development stage. We have added a Technical Advisor/Program Analyst Position, within the BSA policy operation, with specific responsibility for insurance companies. Examiners will be

trained in the first quarter of FY 07 and the examinations are scheduled to start right after the training.

FinCEN has provided the Service a listing, by name, of each insurance company that may come under Service jurisdiction. In addition, based upon criteria that we have established, we have identified the initial insurance companies for BSA examination.

After establishing a baseline measure on industry compliance, we will conduct an analytical review of examination results, and evaluate the efficacy and efficiency of these examinations in conjunction with an industry risk. Based on this review, adjustments to the examination plan can be anticipated in FY2008.

BSA Direct and Web-CBRS

The IRS is now making information required by the Bank Secrecy Act and the USA PATRIOT Act available to FinCEN and other Federal and organizations through an application called Web-CBRS (Web-Currency Banking and Retrieval System).

The IRS began developing a web application for the CBRS approximately five years ago. Its intent was to take advantage of efficiencies from relational data base software and secure Web interfaces. Web-CBRS is critical to our efforts in Fraud/BSA to bring about compliance with both the BSA and the USA PATRIOT Act. We have a skilled and experienced information technology (IT) application development staff in Detroit. They have demonstrated that, with clear requirements, they can bring large projects to completion on schedule.

The implementation of Web-CBRS is on or ahead of schedule. On September 30, 2006, the IRS intends to take the old integrated database management system offline. At this point, Web-CBRS will be the only first-hand source of Bank Secrecy Act and USA PATRIOT Act information available.

This is critical in that FinCEN announced on July 13, 2006 that they had permanently halted the BSA Direct Retrieval and Sharing Component Project (BSA Direct).

When problems with FinCEN's BSA Direct application began to surface in May 2006, FinCEN's IT staff approached the IRS' Modernization and Information Technology Systems (MITS) Application Development organization to discuss the feasibility of providing Web-CBRS to their users in the event that BSA Direct was not operational as planned.

As it became evident that BSA Direct would not be delivered on schedule, FinCEN and the IRS signed an Interagency Service Agreement (ISA) to share data, and began to take the steps necessary to make Web-CBRS available to FinCEN and its customers. These steps included adding the FinCEN Gateway requirements to Web-CBRS, conducting acceptance testing of the FinCEN requirements, training key FinCEN users (FinCEN trainers) on Web-CBRS, and adding FinCEN users to Web-CBRS. FinCEN transferred $300,000 to the IRS to complete these actions. The IRS provided $450,000 in additional development funds to make sure that other work, primarily the revision of BSA forms, did not slip because of the unexpected need to replace BSA Direct. The IRS has also devoted an additional $1,000,000 to cover the cost of processing a significantly higher volume of paper returns.

In addition, as part of the final review of BSA Direct, we met with FinCEN in June, 2006 to review the capabilities of Web-CBRS as compared to those proposed for BSA Direct. We agreed at this meeting that we would work with FinCEN to modify the Web-CBRS data base to meet reasonable additional needs that they may have.

We are committed to cooperate with FinCEN to improve both the usefulness and the quality of the BSA data that is available through Web-CBRS. Our joint working group, Tiger Team, has identified many small systemic changes to processing requirements and BSA forms that will make the data clearer, more consistent, and more useful to law enforcement.

Conclusion

As I stated earlier in this testimony, the fight against money laundering and terrorist financing are top priorities for the Internal Revenue Service. We are prepared to increase our commitment to the BSA Program, and we will continue to coordinate our efforts closely with FinCEN and the other groups represented here this morning.

We will also not forget the importance of assisting MSBs whenever possible in understanding and complying with their responsibilities under the BSA. As Commissioner Everson has said often, service plus enforcement equals compliance.

Mr. Chairman, I thank you for this opportunity to appear before you this morning and will be happy to respond to any questions that you or other members of the Committee may have.