TERRORIST FINANCING SINCE 9/11: ASSESSING AN EVOLVING AL-QAEDA AND STATE SPONSORS OF TERRORISM

HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MAY 18, 2012

Serial No. 112–93

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

78–153 PDF WASHINGTON : 2013

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
PETER T. KING, New York *(Ex Officio)*

BRIAN HIGGINS, New York
LORETTA SANCHEZ, California
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ZACHARY HARRIS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Director*

CONTENTS

TERRORIST FINANCING SINCE 9/11: ASSESSING AN EVOLVING AL-QAEDA AND STATE SPONSORS OF TERRORISM

Friday, May 18, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE,
Washington, DC.

The subcommittee met, pursuant to call, at 11:17 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Long, and Higgins.

Mr. MEEHAN. The Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence will come to order.

The subcommittee is meeting today to hear testimony regarding the evolution of al-Qaeda and state sponsors of terrorism in regards to terrorism financing since September 11. I now recognize myself for an opening statement.

I would like to welcome everyone to today's hearing of the Subcommittee on Counterterrorism and Intelligence examining the United States Government's approach to combating terrorist financing more than a decade after the September 11 attacks. I look forward to hearing from today's expert witnesses—and I mean expert—on the unique role of terrorist financing and what it plays in the war on terrorism and on the evolving trends in this field.

The September 11 hijackers used United States and foreign financial institutions to hold, move, and retrieve their money. They deposited money into United States accounts via wire transfer and deposits of travellers checks and cash that was brought from overseas. They kept funds in foreign accounts, which they accessed through ATMs and credit card transactions here in the homeland. According to the September 11 Commission, the plot cost al-Qaeda somewhere in the rage of $400,000 to $500,000, of which approximately $300,000 passed through the hijacker's bank accounts here in the United States.

After the attacks, the United States publicly declared that the fight against al-Qaeda financing was as critical as the fight against al-Qaeda itself. The charge of the United States intelligence and law enforcement communities was clear: If we choke off the terrorists' money, we limit their ability to conduct mass casualty attacks.

Within months of the attacks, the Department of Defense, the FBI, the CIA, and, perhaps most importantly, the Department of Treasury launched a swift and unprecedented crackdown on do-

mestic and international terrorist financing. I am very pleased, in fact, some of the very people who are responsible for that are sitting on our expert panel today.

Since then, the Treasury's Office of Terrorism and Financial Intelligence has played a critical intelligence and enforcement role against terrorist financing through its dual aims of safeguarding the United States financial system against illicit use and combating rogue nation's terrorist facilitators, money launderers, drug kingpins, and other National security threats.

The Department of Treasury and the intelligence community's successes against al-Qaeda financing and fundraising is without question. In 2005, the 9/11 Commission issued a report card that evaluated progress the Government had made in implementing that group's recommendations. It gave the Government an A–. Not too many A–'s at this day or any day in Government, but it gave it an A– in combating terrorist financing, the best mark on the scorecard.

But despite our successes, and this is important, we can't become complacent. Because al-Qaeda and its affiliates continue to expand their geographic reach worldwide. State sponsors of terrorism like Iran and Syria are highly sophisticated, and they continue to take advantage of the United States and international financial systems in order to skirt international sanctions.

The United States military and counterterrorism efforts have largely decimated core al-Qaeda leadership in Afghanistan and Pakistan, and the group is under significant financial strain and is struggling to secure steady financing to plan and execute attacks against the United States homeland and Western interests.

The terrorist enemies we now face are more diverse, diffuse, and decentralized than ever. Al-Qaeda and their affiliates have concluded that, to bring America down, they will attack with, "smaller but more frequent operations," what some may refer to as the strategy of a thousand cuts. The aim is to bleed the enemy, meaning us, to death.

In June 2011, the Obama administration released a National Strategy for Counterterrorism, where the evolution of terrorist financing was documented: AQAP receiving charitable donations in Yemen, FARC, and the Taliban drug trafficking, Hezbollah's drug and criminal activities, AQAM's link to drug trafficking an kidnapping, and the role of Boko Haram and al-Shabaab in kidnapping for ransom and extortion.

Hezbollah facilitators were particularly savvy in skirting U.S. restrictions on terrorist financing and have been charged in a number of high-profile criminal schemes. As a former United States Attorney in Philadelphia, I initiated investigations into Hezbollah's fund-raising activities that included attempts to transport stolen laptop computers, passports, and Sony PlayStation systems. A separate intricate Hezbollah scheme illustrates the interconnectedness of these networks where a Lebanese bank laundered money from Colombian drug cartels and mixed it with proceeds from used car sales that were bought in the United States and then sold in Africa. The cash was then moved back into Lebanon and poured into Hezbollah's coffers. Clearly, these groups are highly innovative and motivated, and we must be up to the challenge.

Terrorist groups and state sponsors of terrorism turning to criminal activities to set up additional networks to acquire logistical support and to raise financial resources is another evolving trend which could point to future activities of terrorist financing.

Given this shifting trend and the relatively low amounts of money required to undertake an attack, the United States Government may need to recalibrate some of its tactics and examine how the intelligence and law enforcement communities and I believe also the financial entities—the private financial entities will adapt their strategies in order to address remaining vulnerabilities in combating terrorist financing.

I thank the witnesses for the time to be with us today, and I look forward to hearing from this distinguished panel.

[The statement of Mr. Meehan follows:]

STATEMENT OF CHAIRMAN PATRICK MEEHAN

MAY 18, 2012

WELCOME

I'd like to welcome everyone to today's hearing of the Subcommittee on Counterterrorism and Intelligence examining the U.S. Government's approach to combating terrorist financing more than a decade after the 9/11 attacks.

I look forward to hearing from today's expert witnesses on the unique role terrorist financing plays in the war on terrorism and on the evolving trends in this field.

POST-SEPTEMBER 11 ACTIONS

The September 11 hijackers used U.S. and foreign financial institutions to hold, move, and retrieve their money. They deposited money into U.S. accounts via wire transfers and deposits of cash or travelers checks brought from overseas. They kept funds in foreign accounts, which they accessed through ATMs and credit card transactions here in the homeland. According to the 9/11 Commission, the plot cost al-Qaeda somewhere in the range of $400,000–$500,000, of which approximately $300,000 passed through the hijackers' bank accounts in the United States.

After the attacks, the United States publicly declared that the fight against al-Qaeda financing was as critical as the fight against al-Qaeda itself. The charge of the U.S. intelligence and law enforcement communities was clear: If we choke off the terrorists' money, we limit their ability to conduct mass casualty attacks.

Within months of the attacks, the Department of Defense, the FBI, the CIA, and perhaps most importantly the Department of the Treasury, launched a swift and unprecedented crackdown on domestic and international terrorist financing.

Since then, Treasury's Office of Terrorism and Financial Intelligence has played a critical intelligence and enforcement role against terrorist financing through its dual aims of safeguarding the U.S. financial system against illicit use and combating rogue nations, terrorist facilitators, money launderers, drug kingpins, and other National security threats.

TODAY'S HEARING

The Department of the Treasury and the intelligence community's successes against al-Qaeda financing and fundraising is without question. In 2005, the 9/11 Commission issued a "report card" that evaluated progress the Government had made in implementing the group's recommendations. It gave the Government an "A–" in combating terrorist financing—the best mark on the report card.

Despite our successes, we must not become complacent. Al-Qaeda and its affiliates continue to expand their geographic reach worldwide. State sponsors of terrorism like Iran and Syria are highly sophisticated and continue to take advantage of the U.S. and international financial systems in order to skirt international sanctions.

NEW TERRORIST TOOLS USED IN THE FIGHT

Since U.S. military and counterterrorism efforts have largely decimated core al-Qaeda leadership in Afghanistan and Pakistan, the group is under significant finan-

cial strain and is struggling to secure steady financing to plan and execute attacks against the U.S. homeland and Western interests.

The terrorist enemies we now face are more diverse, diffuse, and decentralized than ever. Al-Qaeda and their affiliates have concluded that to bring America down they will attack us with "smaller, but more frequent operations in what some may refer to as the strategy of a thousand cuts. The aim is to bleed the enemy to death."

This was the aim with the AQAP cargo bomb plot of October 2010, where the group boasted that the overhead cost for the attack was only $4,200 and would provoke the U.S. and Western countries to respond with "billions of dollars in new security measures."

In June 2011, the Obama administration released a National Strategy for Counterterrorism, where the evolution of terrorist financing were document: AQAP receiving charitable donations in Yemen; FARC and Taliban drug trafficking, Hezbollah's drug and criminal activities, AQIM's links to drug trafficking and kidnapping, and the role of Boko Haram and al-Shabaab in kidnapping for ransom and extortion.

Hezbollah facilitators are particularly savvy in skirting U.S. restrictions on terrorist financing and have been charged in a number of high-profile criminal schemes. As a former U.S. Attorney in Philadelphia, I initiated investigations into Hezbollah's fundraising activities that included attempts to transport stolen laptop computers, passports, and Sony PlayStation systems. A separate intricate Hezbollah scheme illustrates the interconnectedness of these networks, where a Lebanese bank laundered money from Colombian drug cartels and mixed it with proceeds from used cars bought in the United States and then sold in Africa where the cash was moved back to Lebanon and poured into Hezbollah's coffers. Clearly these groups are highly innovative and motivated and we must be up to the challenge.

Terrorist groups and state sponsors of terrorism turning to criminal activities to set up additional networks, to acquire logistical support, and to raise financial resources is another evolving trend which could point to the future of terrorist financing.

Given this shifting trend, and the relatively low amounts of money required to undertake an attack, the U.S. Government may need to recalibrate some of its tactics and examine how the intelligence and law enforcement communities will adapt their strategies in order to address remaining vulnerabilities in combating terror financing.

CONCLUSION

I thank the witnesses for taking the time to be with us today and I look forward to hearing from this distinguished panel.

Mr. MEEHAN. The Chairman now recognizes the distinguished Ranking Member of the Subcommittee on Counterterrorism, the gentleman from New York, Mr. Higgins, for any statement he may have.

Mr. HIGGINS. Thank you, Mr. Chairman.

Just briefly, in reference to your opening statement, we have learned in prior hearings that Hezbollah, which is a terrorist organization, a Shia Muslim group committed to violent jihad, acts as a proxy for Venezuela, for Syria, and for Iran. They have a presence in the 20-country region of Latin America. Additionally, they have a presence in 15 American cities, including four major cities in Canada. We have also been told that we are not to be too concerned about this, that their activities are limited to fund-raising. Well, I see the fund-raising activities by a terrorist group as an act of terrorism, at least, at least in a preliminary way.

So those are some of the concerns that I have. But, in the interest of time, I will submit my opening statement for the record, so that we can get to the expert witnesses. Thank you for being here.

Thank you, Mr. Chairman. I yield back.

Mr. MEEHAN. Thank you.

Other Members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today, on this important topic.

Dr. Jonathan Schanzer is the vice president of research at the Foundation for Defense of Democracies. He worked as a terrorism finance analyst at the United States Department of Treasury, where he played an integral role in the designation of numerous terrorist financiers.

Dr. Schanzer has also worked for several other United States-based think tanks, including the Washington Institute for Near East Policy and Jewish Policy Center and the Middle East Forum. He studied Middle East history in four countries and most recently received his Ph.D. from King's College in London where he wrote his dissertation on the U.S. Congress and its efforts to combat terrorism in the 20th Century.

Mr. John Cassara enjoyed a 26-year career in the Federal Government intelligence and law enforcement community as an expert in anti-money laundering and terrorist financing. He worked at the Department of Treasury's Financial Crimes Enforcement Network, and this was the first institution set up to take on the issue of terrorist financing, and at the United States Financial Intelligence Unit. He was detailed to work in the Office of Terrorism Finance and Financial Intelligence at the Department of Treasury and the Department of State's Bureau of International Narcotics and Law Enforcement Affairs and Anti-Money Laundering Section. That had to be quite a business card.

During his law enforcement investigative career, Mr. Cassara conducted a large number of money laundering, fraud, intellectual property rights, smuggling, and diversion of weapon and high technology investigations. Just the scope of that demonstrates the numerous schemes that are possible. These investigations took place in Africa, the Middle East, and Europe for a variety of Federal agencies, including directing the first truly international money laundering task force and serving as an undercover arms dealer.

Mr. Dennis Lormel is the president and CEO of DML Associates, a full-service investigative consultancy. Mr. Lormel retired from the Federal Bureau of Investigation in 2003 after 30 years of Government service and almost 28 as a special agent in the FBI.

In December, 2000, he was appointed the chief of the FBI's Financial Crimes Program. Following the terrorist attacks of September, 2001, Mr. Lormel established and directed the FBI's Terrorist Financing Initiative, which evolved into the Terrorist Financing Operations Section within the Counterterrorism Division. Since leaving law enforcement, he has provided risk advisory consulting services and has served as an advisor to the Congressional Anti-Terrorist Financing Task Force.

The Honorable Sue Eckert is a senior fellow at the Thomas J. Watson Institute at Brown University, where her research is concentrated on making United Nations sanctions more effective through targeting and combating the financing of terrorism.

Prior to joining Brown University, Ms. Eckert was employed at the Institute of International Economics; and from 1993 until 1997, Ms. Eckert was appointed by President Clinton and confirmed by the Senate as the assistant secretary of commerce for export administration. Previously, she served on the professional staff of the

House of Representatives Committee on Foreign Affairs. In addition, she has worked with business groups and served on numerous working groups and committees addressing security and technology issues.

I am very grateful for this panel. You bring in expertise on an issue which I think is dramatically under-appreciated by most Americans, and few realize the importance of this as we conduct investigations and do our best to protect not just this Nation but Western interests from around the world from terrorist activity and threats.

A critical element is the ability to understand how they are funded, how they are supported, how they operate, and we have seen a remarkably changing capacity for them to do it. You have been there at the front end of this. We really need your insights to understand how things have evolved and what we ought to be looking for to continue to do the best job that we can to be on top of the ability to control their ability to carry out acts of terrorism against us.

So, at this point, I appreciate your being here. We are going to be called again to votes at 11:50, but we want to get the benefit of your testimony. We are going to do as much as we can to probe on questions as soon as we complete that. So I ask you to do your best to focus on the essence of your testimony and see if we can stay within the 5-minute period.

So the Chairman now recognizes Dr. Schanzer to testify.

STATEMENT OF JONATHAN SCHANZER, VICE PRESIDENT OF RESEARCH, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. SCHANZER. Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee, on behalf of the Foundation for Defense of Democracies I thank you for the opportunity to testify.

I base my testimony today on my experience as an analyst at the U.S. Treasury's Office of Intelligence and Analysis, where I worked from 2004 to 2007 and was directly involved in designating several terrorist financiers.

Mr. Chairman, after the September 11 attacks, the U.S. Treasury immediately went to work uncovering terrorist funds. On September 23, President George W. Bush issued an Executive Order designating terrorist entities that threatened America. That list quickly grew and became a powerful tool for capturing terrorist money.

The 9/11 Commission report at least in 2004 gave Treasury high marks for its efforts, but in denying terrorists the use of the formal banking sector, we have driven terror financing underground, and we are now victims of our own success. Terrorists have adapted in part by hatching cheaper plots. It cost al-Qaeda of the Arabian Peninsula, AQAP, just $4,200 to place two bombs on cargo planes in October, 2010. The group bragged openly of this, underscoring that it is nearly impossible now to stop such low-cost operations.

Other terrorist groups rely heavily on bulk cash smuggling to evade detection with couriers delivering suitcases full of cash to terrorist masterminds. Still others engage in trade-based money launderings, where they plow illicit cash into legitimate businesses to further finance terrorist activities.

Broadly speaking, terrorist financiers are increasingly shifting to criminal activity. Earlier this year, U.S. authorities indicted a vast Hezbollah network of money laundering, cocaine deals, and more, exposing 30 U.S.-based car dealerships that helped the group move cash. Similarly, Senator Dianne Feinstein recently noted how the Taliban relies heavily on profits from the heroin trade to finance its operations.

If this trend continues, it is reasonable to assume that criminal investigations will play an increasingly prominent role in U.S. efforts to counter terror finance. For its part, Treasury must continue to issue designations, even if fewer of them lead to actually capturing cash. The naming and shaming of terrorist financiers lets them know that they are being watched, and that helps to stem the flow of cash that can finance attacks on the homeland or against allies abroad.

Designations can also expose key nodes of terrorist groups. That has been critical in exposing al-Qaeda's relationship with Iran. In July 2011, Treasury designated al-Qaeda leader Yasin al-Suri and five others who moved money and recruits to Pakistan, the Gulf, and Iraq. Treasury declared that al-Suri's network operates as part of a "secret deal" between al-Qaeda and the Iranian Government.

In January 2009, Treasury designated four other al-Qaeda operatives in Iran. All of them, including Osama bin Laden's son, Sa'ad bin Laden, served on al-Qaeda's executive council.

Of course, none of this comes as a surprise. The 9/11 Commission in 2004 expressed concern over the Iran-al-Qaeda operational relationship, noting that it requires "further investigation by the U.S. Government." Treasury is doing just that, and it shares its findings through the designation process.

Remarkably, Treasury's robust counterterrorism program is the only one of its kind in the world. None of America's allies come close to our investment in human and financial resources to combat terror finance. This can be blamed on a combination of tight budgets and a lack of political will.

Though the international Financial Action Task Force, or FATF, recently beefed up its standard, it is insufficient. FATF allows members to self or mutually evaluate, operates according to recommendations, and enables states like Saudi Arabia and Qatar to give themselves high marks regardless of the realities. The system is full of holes, and terrorists predictably gravitate to the areas of weakest authority.

Looking ahead, Treasury's policy shop, the Office of Terrorism Finance and Financial Crimes, TFFC, needs to prompt both allies and adversaries to do more to combat terror finance. But, for the short term, the most glaring challenge is the threat of a nuclear Iran. On this front, Treasury has had a real impact. Tehran now faces tougher sanctions than ever before, and the regime is cash-strapped. Though Teheran continues to push forward with its nuclear program, the regime reportedly finds it increasingly difficult to bankroll terrorist proxies, Hamas, and Hezbollah to the extent that it had in the past. Admittedly, we may now be past the point where economics can prevent a nuclear Iran, but Treasury's efforts have nevertheless been instructive. They demonstrate that, if prop-

erly applied, sanctions can truly diminish a state sponsor's ability to finance terror.

Mr. Chairman, there are many other challenges on the terrorism financing front that I did not have time to address today. If I have missed anything you wish to discuss, I am happy to answer your questions; and on behalf of the Foundation for Defensive Democracies, I thank you for inviting me today.

[The statement of Mr. Schanzer follows:]

PREPARED STATEMENT OF JONATHAN SCHANZER

MAY 18, 2012

Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee, on behalf of the Foundation for Defense of Democracies, thank you for the opportunity to testify.

I base my testimony today on my experience as an analyst at the U.S. Treasury Office of Intelligence and Analysis, where I worked from 2004 to 2007, and was directly involved in designating several terrorist financiers.

Mr. Chairman, after the September 11 attacks, the U.S. Treasury immediately went to work uncovering terrorist funds. On September 23, President George W. Bush issued an Executive Order designating terrorist entities that threatened America.[1] That list grew quickly and became a powerful tool for capturing terrorist money.

The 9/11 Commission report, released in 2004, gave Treasury high marks for its efforts.[2] But in denying terrorists the use of the formal banking sector, we have driven terror finance underground, and we are now victims of our own success.

Terrorists have adapted, in part, by hatching cheaper plots. It cost al-Qaeda of the Arabian Peninsula just $4,200 to place two bombs on cargo planes in October 2010. The group bragged openly of this, underscoring that it is nearly impossible to stop such low-cost operations.[3]

Other terrorist groups rely heavily on bulk cash smuggling to evade detection, with couriers delivering suitcases full of cash to terrorist masterminds.[4] Still others engage in trade-based money laundering, where they plow illicit cash into legitimate businesses to further finance terrorist activities.[5]

Broadly speaking, terrorist financiers are increasingly shifting to criminal activity. Earlier this year, U.S. authorities indicted a vast Hezbollah network for money laundering, cocaine deals, and more—exposing 30 U.S.-based car dealerships that helped the group move cash.[6] Similarly, Senator Dianne Feinstein recently noted how the Taliban relies heavily on profits from the heroin trade to finance its operations.[7]

If this trend continues, it's reasonable to assume that criminal investigations will play an increasingly prominent role in U.S. efforts to counter terror finance.

For its part, Treasury must continue to issue designations, even if fewer of them lead to capturing terrorist cash. The naming and shaming of terrorist financiers lets them know they're being watched. And that helps us stem the flow of cash that can finance attacks on the homeland or against allies abroad.

Designations also expose key nodes of terrorist groups. This has been critical in exposing al-Qaeda's relationship with Iran.

In July 2011, Treasury designated al-Qaeda leader Yasin al-Suri and five others who moved money and recruits to Pakistan, the Gulf, and Iraq. Treasury declared

---

[1] "Executive Order on Terrorist Financing," September 23, 2001, *http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/print/20010924-1.html.*

[2] *http://govinfo.library.unt.edu/911/report/index.htm.*

[3] See the November 2010 issue of AQAP's *Inspire* magazine: *http://info.publicintelligence.net/InspireNovember2010.pdf.*

[4] John Diamond, "Terror Funding Shifts To Cash," *USA Today,* June 18, 2006, *http://www.usatoday.com/news/washington/2006-06-18-terror-cash_x.htm.*

[5] Avi Jorisch, *Tainted Money: Are We Losing the War on Money Laundering and Terrorism Financing?* (VA: Red Cell Publishing, 2009), pp. 95–104.

[6] *United States of America* vs. *Lebanese Canadian Bank, et al. http://www.justice.gov/dea/pubs/pressrel/pr121511_filed-complaint.pdf.*

[7] "GOP lawmaker concerned over strength of Taliban," *Los Angeles Times,* May 4, 2012. *http://latimesblogs.latimes.com/world_now/2012/05/washington-us-intelligence-afghanistan-taliban-stronger-president-obama.html.*

that al-Suri's network operates as part of a "secret deal" between al-Qaeda and the Iranian government.[8]

In January 2009, Treasury designated four other al-Qaeda operatives in Iran. All of them, including Osama bin Laden's son, Sa'ad bin Laden, served on al-Qaeda's executive council.[9]

Of course, none of this comes as a surprise. The 9/11 Commission in 2004 expressed concern over the Iran-al-Qaeda operational relationship, noting that it required "further investigation by the U.S. government." Treasury is doing just that, and it shares its findings through the designation process.

Remarkably, Treasury's robust counter-terrorist program is the only one of its kind in the world. None of America's allies come close to our investment in human and financial resources to combat terror finance. This can be blamed on a combination of tight budgets and a lack of political will.

Though the international Financial Action Task Force (FATF) recently beefed up its standards,[10] it is insufficient. FATF allows member states to self-evaluate, and operates according to "recommendations,"[11] enabling states like Saudi Arabia and Qatar to give themselves high marks, regardless of the realities. The system is full of holes, and terrorists predictably gravitate to the areas of weakest authority.

Looking ahead, Treasury's policy shop—the Office of Terrorism Finance and Financial Crimes[12]—needs to prompt both allies and adversaries to do more to combat terror finance. But for the short term, the most glaring challenge is the threat of a nuclear Iranian.

On this front, Treasury has had a real impact. Tehran now faces tougher sanctions than ever before, and the regime is cash-strapped. Though Tehran continues to push forward with its nuclear program, the regime reportedly finds it increasingly difficult to bankroll terrorist proxies Hamas and Hezbollah to the extent it had in the past.

Admittedly, we may now be past the point where economics can prevent a nuclear Iran. But Treasury's efforts have nevertheless been instructive. They demonstrate that, if applied properly, sanctions can truly diminish a state sponsor's ability to finance terror.

Mr. Chairman, there are many other challenges on the terrorism financing front that I did not have time to address today. If I have missed anything you wish to discuss, I am happy to answer your questions.

On behalf of the Foundation for Defense of Democracies, I thank you again for inviting me here today.

Mr. MEEHAN. Thank you, Doctor. Very grateful for your testimony.

The Chairman now recognizes Mr. Cassara to testify.

STATEMENT OF JOHN A. CASSARA, PRIVATE CITIZEN

Mr. CASSARA. Chairman Meehan, Ranking Member Higgins, and Members of the subcommittee. Thank you for the opportunity to testify today. It is an honor for me to be here. While there are no simple solutions to all of the challenges identified by this subcommittee, I believe there are three realistic and cost-effective steps we should take.

Mr. Chairman, I believe you used the term "recalibrate tactics." I think that is a very, very good way of putting it. I have broadly categorized my proposed recalibrations, if you will, as transparency, technology, and draining the swamp. The three are inter-

---

[8] "Treasury Targets Key Al-Qa'ida Funding and Support Network Using Iran as a Critical Transit Point," July 28, 2011, Page Content *http://www.treasury.gov/press-center/press-releases/Pages/tg1261.aspx*.

[9] "Treasury Targets Al Qaida Operatives in Iran," January 16, 2009. *http://www.treasury.gov/press-center/press-releases/Pages/hp1360.aspx*.

[10] Amit Kumar, "The Revised FATF Standards: A Shot in the Arm for Countering the Financing of Terrorism Efforts," April 16, 2012, Center for National Policy, *http://cnponline.org/ht/display/ViewBloggerThread/i/37450/pid/35636*.

[11] See the FATF mandate here: *http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf*.

[12] See: *http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorist-Financing-and-Financial-Crimes.aspx*.

twined and complementary. I elaborate upon them in my written statement. Because of time constraints, I will just briefly summarize them.

Let's begin with transparency. Shortly after the September 11 terrorist attacks, I had a very interesting conversation with a Pakistani businessman involved in the gray markets and the underworld of crime. He told me something I will never forget. He said: Mr. John, don't you understand that criminals and terrorists are moving money and transferring value right under your noses? But the West doesn't see it. Your enemies are laughing at you. His words infuriated me because I knew he was right. I worked overseas for years with frequent travels to the Arabian Peninsula, Africa, South Asia. I became intrigued with the opaque, indigenous, but very effective ways of transferring money and value so different from our own. For example, the Pakistani businessman was referring to various forms of what we would loosely call trade-based money laundering. It involves the transfer of value via commodities and trade goods.

In addition to simple but effective customs fraud, trade-based value transfer is often used to provide counter-valuation, or a way of balancing the books in many global underground financial systems, including some that are used to finance terror. Without going into detail, some of these trade-based value schemes are found in hawala networks, most other regional forms of alternative remittance systems, the Afghan transit trade, suspect international Lebanese Hezbollah networks, trading syndicates, and non-bank lawless regimes in the Horn of Africa.

Now, in theory, spotting anomalies in trade data and overlapping these anomalies with financial data transportation data, travel data, would allow us to kind of peer into these underground networks by in effect going in through the back door.

When a buyer and seller are working together, the price of a good or a service can be whatever they want it to be. There is no invoice police. Now, this is a very simple example. This pen, it is a nice pen. Let's say it cost roughly $50. Buyer and seller, via, say, false invoicing could overvalue this to say it is worth $100. Simply, similarly, they could undervalue it to show it is worth say $10, or say even $1. Now, why is this important? Well, to move money out of a country, participants import goods at overvalued prices or export goods at undervalued prices. To move money into a country, the participants import goods at undervalued prices, or export goods at overvalued prices. For the most part, all of this avoids countries' financial transparency reporting requirements. We are not picking this up. This vulnerability is what Osama bin Laden himself once himself called cracks in the Western financial system.

I once had a conversation with an Iranian freight forwarder in Dubai and I was talking about this type of money laundering, trade manipulation, over- and under-invoicing. He says to me: Mr. John, money laundering, but that is what we do. Precisely, it is the way of life out there. It is the way they do business.

Now, in order to help combat this type of trade-based money laundering the Department of Homeland Security's Immigrations and Customs Enforcement, or ICE, established the world's first trade transparency unit, or TTU. There are approximately eight

additional TTUs in the Western hemisphere and more planned. Congress can help promote transparency by ensuring the U.S. TTU has sufficient resources to systematically examine trade fraud in the United States for reasons of both National security and to enhance our revenue. Our TTU should be encouraged to further expand the TTU network overseas, particularly in areas where adversaries operate, and we should also promote trade transparency overseas by building it into the U.S. trade agenda.

Let me briefly switch now and talk about technology. Over the last few years, there have been tremendous advances in the amount of data collected and available for analysis. Just a few examples include financial, trade, and transport data. Communications and social networking are growing exponentially. Industry calls these record sets of information big data. Concurrently, there have been major advances in data warehousing, data mining, and advanced analytics. I am not a technical person; however, I am excited about some of the new tools and resources that have been recently developed to exploit big data and help the modern criminal investigator. Yet those tools are not in our investigators' hands, not at the Federal, State, or local level. I am convinced the only way we are going to realistically stay abreast of some of these challenges we face in financial crimes and terror finance is to use technology as a force multiplier.

Now, if we are talking about financial data, we have to talk about Treasury's Financial Crimes Enforcement Network, FinCEN. FinCEN is mandated to collect, analyze, and disseminate financial intelligence. FinCEN is the gatekeeper and should be the U.S. Government's premier financial crimes resource. However, as I documented in my first book, "Hide and Seek: Intelligence, Law Enforcement, and the Stalled War on Terrorist Finance," FinCEN has never lived up to its early promise and potential. The expertise and managerial will simply do not exist to fully exploit the data and——

Mr. MEEHAN. I am going to have to, because we are going to get called. It is all worth developing in our follow-up questions. Let me ask if I can: Is there a quick point you want to make in summary?

Mr. CASSARA. No, I refer the committee to my statement, and my statement elaborates on these points.

[The statement of Mr. Cassara follows:]

PREPARED STATEMENT OF JOHN A. CASSARA

MAY 18, 2012

Chairman Meehan, Ranking Member Sanchez, and Members of the Subcommittee on Counterterrorism and Intelligence, thank you for the opportunity to testify today. It is an honor for me to be here.

In 2005, I retired after a 26-year career as a case officer for the Central Intelligence Agency and as a special agent for the U.S. Department of Treasury. I believe I am the only individual to have ever been both a covert case officer and a Treasury special agent.

Much of my career with Treasury was involved with combating international money laundering and terror finance. I currently work as a contractor and consultant for a number of U.S. departments, agencies, and business enterprises, although the views that I express here are only my views and not necessarily representative of these organizations. I have been fortunate to continue my domestic and international travels primarily providing training and technical assistance in financial

crimes enforcement. I have written three books on terror finance and numerous articles. I have direct experience with many of the issues being discussed here today.

A few days after the most successful terrorist attack in U.S. history, President George W. Bush stated, "Money is the lifeblood of terrorist operations. Today we are asking the world to stop payment." We are meeting here this morning in part to ask whether that request has been fulfilled and, if not, what more can and should be done.

The short answer is both "yes" and "no." Completely eradicating terror finance is impossible. There is no magic bullet. Yet after 10 years of concerted effort, it is now harder, costlier, and riskier for terrorists to raise and transfer funds, both in the United States and around the world. That's the good news. Unfortunately, there is no doubt that our financial countermeasures have not been as smart or efficient as they could be and that we will continue to face new challenges in the coming years.

The learning curve has been steep. For example, in the years immediately after September 11, most policymakers within the Treasury Department were convinced that "financial intelligence" or Bank Secrecy Act (BSA) data was the key to following the terrorist money trail. They had misplaced faith in the approximately in (2012 numbers) 17 million pieces of financial data that are filed annually with Treasury, including approximately 1 million Suspicious Activity Reports (SARs). This is in addition to the countless millions of additional pieces of financial information filed around the world. This data comes from a wide variety of sources, including banks, money service businesses, and individuals.

"Financial intelligence," also known as "BSA data," or "financial transparency reporting requirements" was initiated during the early years of the "War on Drugs" when enormous amounts of illicit proceeds from the international narcotics trade regularly sloshed around Western financial institutions. So it is important to understand the financial reports were not originally designed to combat terror finance where small amounts of both illicit and licit monies are commonly used. It shouldn't really be a surprise that out of the tens of millions of pieces of financial intelligence filed annually in the United States and around the world not one piece of financial intelligence was filed on any of the 19 September 11 hijackers. And even if there had been, the United States did not have the programs and management structures in place that would have detected the suspicious financial activity. I say this with confidence because I worked at Treasury's Financial Crimes Enforcement Network (FinCEN) at the time. I demonstrated the failings in my first book, *Hide & Seek: Intelligence, Law Enforcement and the Stalled War on Terror Finance* (Potomac Books, 2006). The same dearth of financial intelligence has subsequently held true for major terrorist attacks from Bali to Baghdad.

Although the last 10 years have demonstrated that financial intelligence here and abroad is not the panacea for counter-terrorist finance, much of the financial data does contain excellent information and some has proved vital in "connecting the dots." The data is invaluable in money laundering and other investigations. That being said, it is not being effectively exploited.

Over the past 10 years, our adversaries' operational and financial tactics have evolved. We are faced with immense challenges. The situation is made worse by the comparatively small amounts of funding involved with terror finance. For example, it is estimated that September 11 cost al-Qaeda approximately $300,000–$500,000. Even this relatively small amount towers over the recent attempt to hide explosives in a printer cartridge aboard an air cargo flight to the United States. Al-Qaeda in the Arabian Peninsula boasted in its on-line magazine that, "It is such a good bargain for us to spread fear amongst the enemy and keep him on his toes in exchange for a few months work and a few thousand dollars."

While there are no simple solutions to all of the challenges identified by this subcommittee, I believe there are some straightforward and cost-effective steps we should take. I have broadly categorized them as technology, transparency, and draining the swamp. The three are intertwined and complimentary.

TECHNOLOGY

Over the last few years, there have been tremendous advances in the amount of data collected and available for analysis. Just a few examples include financial, trade, transport, and travel data. Communications and social networking are growing exponentially. Industry calls these record sets of information, "big data." I will not discuss the collection of classified data.

Concurrently, there have been major advances in data mining and advanced analytical capabilities that can help organizations derive the "intelligence" from this vast amount of data. Data warehousing and retrieval are enhanced by cutting-edge technologies that search, mine, analyze, link, and detect anomalies, suspicious be-

haviors, and related or interconnected activities and people. Fraud frameworks can be deployed to help concerned Government agencies and departments detect suspicious activity using scoring engines that can both rate, with high degrees of statistical accuracy, behaviors that warrant further investigation while generating alerts when something of importance changes. Predictive analytics use elements involved in a successful case or investigation and overlays these elements on other data sets to detect previously unknown behaviors or activities, enhancing and expanding an investigator's knowledge, efforts, productivities while more effectively deploying resources. Social network analytics helps investigators detect and prevent criminal activity by going beyond individual transactions to analyze all related activities in various mediums and networks uncovering previously unknown relationships. Visual analytics is a high-performance, in-memory solution for exploring massive amounts of data very quickly. It enables users to spot patterns, identify opportunities for further analysis, and convey visual results via web reports or the iPad. Moreover, it is now possible to engineer "red flag indicators" in financial reports—both within the Government and in commercial enterprises that file the information—that will identify likely suspect methodologies such a hawala or trade-based money laundering.

Unfortunately, while the Federal Government is beginning to incorporate these advanced analytical capabilities, it lags far behind in its deployment of commercially available and viable technologies. As a subset, the Federal financial investigative resources trail even further behind. FinCEN is mandated to collect, house, analyze, and disseminate financial intelligence. FinCEN should be the U.S. Government's premier financial crimes resource. However, FinCEN has never lived up to its early promise and potential. One important problem with FinCEN is that although it has attempted to implement a number of data mining activities over the years, they have not been successful. Recently, progress has been made developing and employing new analytical tools. However, the FinCEN analysts are only able to use perhaps 10 percent of their new analytical capacity. The expertise and managerial will simply do not exist to fully exploit many of the tools now finally at their disposal.

Within the next few years, it is estimated that approximately 500–700 million additional pieces of financial information in the form of wire transfer data will be routed annually to FinCEN. If FinCEN is not able to successfully analyze the current 1 million BSA filings it receives annually it is highly doubtful that it will succeed with this new tasking. Yet law enforcement and intelligence professionals should have access to the data and be able to interpret it. Technology will be the force multiplier and the only realistic solution to effectively exploit current and new streams of financial data.

In order to move forward, we must move to get around the FinCEN impediment. I propose that we "downstream" both financial information and analytics platforms directly to end-users in the law enforcement community. For example, the financial data and an accompanying user-friendly analytics platform could be made directly accessible to various task forces, U.S. attorney offices, regional Suspicious Activity Report (SAR) review teams, appropriate Federal, State, and local law enforcement departments and agencies. Since FinCEN is mandated by the Department of Treasury to administer the Bank Secrecy Act (BSA) and accompanying data, FinCEN could license and control the release of the data and the analytics platform.

Moreover, in my discussions with members of the U.S. intelligence and defense communities, frustration is often expressed that they do not have direct access to appropriate and targeted financial databases that intersect with their international areas of responsibility. Instead of looking for ways to increase the dissemination of necessary data, legal advisors within Treasury work to impede the release of information. While I certainly understand and endorse privacy and other concerns, the technology exists today to engineer safeguards into the dissemination of the data to prevent abuse. I urge that our colleagues be given increased access to this vital information in order to help safeguard our security.

TRANSPARENCY

Shortly after the September 11 terrorist attacks, I had a conversation with a Pakistani businessman involved with the underworld of crime. He was involved in the gray markets of South Asia and the Middle East. He said, "Mr. John, don't you know that the criminals and the terrorists are moving money and transferring value right under your noses? But the West doesn't see it. Your enemies are laughing at you."

His words infuriated me because I knew he was right. I worked overseas for years with frequent travels to the Arabian peninsula, Africa, and South Asia. For the most part, U.S. officials could not understand or identify the opaque, indigenous, but

very effective ways of transferring money and value so different from our own. For example, the above Pakistani businessman was referring to various forms of what we loosely call "trade-based money laundering." It involves the transfer of "value" via commodities and trade goods. In addition to customs fraud, trade-based value transfer is often used to provide "counter-valuation" or a way of balancing the books in many global underground financial systems—including some that have been used to finance terror.

In theory, by promoting trade transparency and using technology to spot anomalies in trade data (and overlapping those flagged anomalies with financial, travel, transportation, law enforcement, and other databases) we may be able to use trade as a "back door" to enter into previously hidden underground financial networks.

Trade-based money laundering scams take a wide variety of forms. For example, it could be simple barter or a commodity-for-commodity exchange. In certain parts of Afghanistan and Pakistan, for example, the going rate for a kilo of heroin is a color television set. Drug warlords exchange one commodity they control (opium) for others that they desire (luxury and sports utility vehicles). In the United States and Mexico, weapons go south and drugs come north. However, generally speaking, money laundering and value transfer through simple invoice fraud and manipulation are most common. The key element here is the misrepresentation of the trade good to transfer value between importer and exporter. The quantity, quality, and description of the trade goods can be manipulated. The shipment of the actual goods and the accompanying documentation provide cover for "payment" or the transfer of money. The manipulation occurs either through over- or under-valuation, depending on the objective to be achieved. To move money out of a country, participants import goods at overvalued prices or export goods at undervalued prices. To move money into a country participants, import goods at undervalued prices or export goods at overvalued prices. For the most part, all of this avoids countries' financial intelligence reporting requirements.

Trade-based value transfer is found in every country around the world. I believe it is the "new frontier" in international money laundering and counter-terrorist finance countermeasures. Without going into detail, trade-based value transfer is found in hawala networks, most other regional "alternative remittance systems," the misuse of the Afghan Transit Trade, Iran/Dubai commercial connections, suspect international Lebanese/Hezbollah trading syndicates, non-banked lawless regimes such as Somalia, etc.

I have written extensively about trade-based money laundering. I invented the concept of trade-transparency units (TTUs), which is now part of the U.S. Government National Anti-Money Laundering Strategy. I am delighted that the Department of Homeland Security's Immigration and Customs Enforcement (ICE) has adopted this concept by establishing the world's first TTU. There are approximately eight additional TTUs in the Western Hemisphere and more TTUs are planned.

In addition to being an innovative countermeasure to trade-based money laundering and value transfer, systematically cracking down on trade-fraud is a revenue enhancer for participating governments. Frankly, it is for this reason that many countries outside of the United States have expressed interest in the concept. In essence, these governments understand that they are not collecting the appropriate amount of duties on the goods because the values on the invoices are mis-stated. Finding new revenue, without actually having to raise tax rates, is an economic imperative.

TTUs are already proving to be valuable resources for our government and international partners. For example, in 2008 the United States and Mexico partnered in the creation of a TTU in Mexico City. Such efforts should be promoted and expanded. Congress can help by ensuring that the TTUs have sufficient resources to systematically examine trade fraud in the United States for reasons of both National security and to enhance our revenue. We should also promote trade transparency overseas by building it into the U.S. trade agenda.

DRAIN THE SWAMP

Since the end of the Cold War, there has been a dramatic decline in the number of countries that support and finance targeted acts of terrorism in order to achieve their national objectives. Today, Iran is the major "state sponsor" of terrorism. In the early days of al-Qaeda, the terrorist group received much of its financial resources from Osama bin Laden's personal family wealth, along with contributions from wealthy Saudi and other donors. Today, al-Qaeda and other jihadist groups have been forced to disperse and receive little centralized direction or funding. This is the good news.

With the decline of the above historical model—that is, groups with centralized command and control receiving most of their money from "state sponsors," evil regimes, and wealthy donors—terrorists and their supporters must increasingly rely on self-finance. In many cases, a symbiosis is developing between organized crime and terrorist organizations, and this sort of link has been observed around the world. As I detail in a book I co-authored with former Treasury official Avi Jorisch, *On the Trail of Terror Finance: What Law Enforcement and Intelligence Officers Need to Know* (Red Cell Publishing 2010) we have observed individual terrorists and terrorist groups involvement with narcotics trafficking, intellectual property rights violations or trafficking in counterfeit goods, cigarette smuggling, robberies, credit card scams, fraud, trafficking in stolen cars, kidnapping for ransom, extortion, and other serious crimes. Unfortunately, self-finance in this way is much harder to detect, track, and disrupt.

Given the above, "draining the swamp" or cracking down at home and abroad on local and transnational financial crime might eventually become one of the most effective strategies to combat terrorism. Even the U.S. military and international peacekeeping forces operating in lawless states have come to recognize that their adversaries, many with terrorist links, increasingly engage in traditional crime to help finance their activities.

For this strategy to succeed, law enforcement, intelligence, and military organizations must learn to look beyond the immediate circumstances of a given local crime. Whether they are confronted with narcotics trafficking, organized robbery, human trafficking or other activities, street cops, criminal investigators, and analysts alike must learn to ask whether these seemingly isolated acts have more sinister ties. Officials, both in the United States and overseas, must learn to "ask the next question" during the course of routine investigations: Where is the money going?

Yet most law enforcement officers get caught up in the quick statistic. That is how they are recognized and rewarded. They are not interested, often times not allowed, and do not have the networks to determine if the local crime they uncovered has broader implications.

In my travels around the United States and overseas, I have observed first-hand how little law enforcement groups actually know about following the money. It is particularly shocking because outside of crimes of passion, criminals and criminal organizations engage in criminal activity because of greed; i.e., money. For example, Karachi, Pakistan's largest city and economic hub, is heavily infiltrated by militants and terrorists making money through criminal activities such as cigarette smuggling, selling counterfeit goods, bank robbery, street robbery, kidnapping for ransom, and other heinous crimes. Mr. Sharfuddin Memon, a director of a Karachi citizens' crime watch group, described the motivations behind this activity: "The world thinks this is about religion, but that's a mistake. It's about money and power. Faith has nothing to do with it."

I urge Congress to support effective training programs that educate law enforcement and intelligence officers on the importance of "asking the next question" and following the money trail. I also believe we should make much more concerted efforts—using various means—to work with international public media and other communications networks and brand terrorists for what they are: International thugs. They should not be allowed to glorify themselves. The last 10 years have demonstrated that criminals are using jihad as a concept to legitimize their activities. By using publicity, transparency, and draining the swamp we will delegitimize them.

As I said at the outset, our enemies are adept at exploiting the weaknesses in the U.S. financial reporting system. Osama bin Laden once called these "cracks in the Western financial system." Their financial behavior has evolved. I also mentioned new financial threats on the horizon. Some of these include pre-paid gift and stored value cards; service-based laundering; mobile payments commonly referred to as "m-payments" or the use of cell phones to store, receive, and transmit money; digital currencies; virtual currencies in the on-line virtual world, etc. Unfortunately, time does not permit a full review. However, many of these and other financial threats and countermeasures that may merit scrutiny by this subcommittee were articulated over 5 years ago in the 2007 *National Money Laundering Strategy* written by the Departments of Treasury, Justice, and Homeland Security. The document was a blueprint for further action in the areas of financial crimes and threat finance. Unfortunately, in many areas, little or nothing has been done. I urge the subcommittee to review the document and ask hard questions about progress to date.

"Without money there is no terrorism." While this is a simplistic formula, our adversaries know that they need money to survive and fund their operations. They are proving adept and creative at finding new ways to access this lifeblood. I have pro-

found respect for our intelligence and enforcement communities. The challenges they face in following illicit financial trails are immense.

I appreciate the opportunity to appear before you today and I'm happy to elaborate on my experiences and to answer any questions you may have.

Mr. MEEHAN. Anybody who is watching these hearings should appreciate the tremendous amount of work that went into the written testimony, which is far more expansive, and I think lays out for those who are studying this issue.

Mr. Lormel, let me turn to you for 5 minutes before we—and Ms. Eckert. Thank you.

STATEMENT OF DENNIS M. LORMEL, PRESIDENT AND CEO, DML ASSOCIATES, LLC

Mr. LORMEL. Thank you, sir. I appreciate——

Mr. MEEHAN. May want to push your button.

Mr. LORMEL. Sorry. I appreciate the fact you are having this hearing and I admire your desire to continue this. It is very heartening to see that the committee wants to address this topic. It is very important.

I was in a unique position on 9/11. I was in a position of leadership in the FBI where I got to follow the money, and I saw firsthand in the 3 years that I was there how well we used proactive techniques. One of the things that you are interested in are investigative techniques and tactics. How we succeed is being proactive. How we succeed is to look at financial information and how we can take financial intelligence and use it from a strategic, tactical, and historic standpoint, and use that in furtherance of investigative initiatives. We did it then. The Government is doing it today, and they do it pretty well, but we can do things better than what we do, and I hope that the committee can come away with that sense in going back and looking and assessing the Government on some of these issues.

In any event, let me start with the Government and the private sector in terms of perspectives. Perspective is very important, and the Government and private sector have some good partnerships, but we can partner better. One of the things we have to look at is the Bank Secrecy Act and the important of bank secrecy information and how we can use that in furtherance of investigative developments and initiatives. Quite frankly, when you look at the Bank Secrecy Act you are looking at identifying suspicious activities in terms of who, what, when, where, how. When it comes to the private sector they are interested in the how. The Government is interested in the why. So we have to blend those two and bring them together better than we do. Terrorists, and you said it in your statement, Mr. Higgins said it, and I have heard it here with the other panelists, of how challenged we are in terms of moneys being used differently and smaller denominations of moneys being used. So the Government is more challenged in terms of identifying terrorist financing. That goes to the fact that again, going back to the financial sector, it is possible to identify terrorist financing, but it is not probable. The lesser amounts that are used, the more challenging it gets, and it plays then to the importance of the partnerships between the public and private sector, and again, bringing the why and how together to be able to accomplish these things.

I testified on October 3, 2001, and I was asked specifically to testify about what the biggest vulnerabilities in the financial sector were. I said the biggest vulnerabilities were wire transfers, correspondent banking, and money services businesses. Today, I kind of look at this a little differently. I say that the problems we have are basically two-fold. You have criminal problems, crime problems, and you have got problems in terms of facilitation tools. The crime problems are fraud and money laundering, and money laundering in the greater context of all types of activities that require money being laundered back through the financial industry. Then the facilitation tools would be things like wire transfers, correspondent banking, money service businesses. If you—I am sorry, not money-service businesses, illegal money remitters.

The Iranian sanctions, for instance, if you look at wire transfers, correspondent banking, shell companies, those are things that they take advantage of. Illegal money remitters, to me, is the biggest problem we have in the financial sector. The banks don't recognize who their clients are, customers are that have illegal money remittance operations. Then electronic mechanisms. That is the wave of the future. We have tremendous capabilities. We are getting away from cash. The more we get away from cash and the more like cash these mechanisms become, the more vulnerable we are to money laundering. I think if you look at Africa as a flashpoint, that is a good case in point of how terrorists are using these mechanisms to be able to launder money.

I think there are some very good partnerships, again, and one in particular, is JPMorgan Chase and the Department of Homeland Security investigations. They have partnered to strategically collect information and, through targeted transaction monitoring, have really done a tremendous job in dealing with human smuggling. We can do the same thing in terrorist finance, but it takes a more concerted effort. So those are things that we need to look at.

In my written statement, I put in it some recommendations, Chairman, about certain things that we need to do.

[The statement of Mr. Lormel follows:]

PREPARED STATEMENT OF DENNIS M. LORMEL

MAY 18, 2012

Good morning Chairman Meehan and distinguished Members of the committee. Thank you for inviting me to testify at this hearing. Terrorist financing is a subject that is extremely important to me. This topic does not receive the attention it deserves. I greatly appreciate the fact that you are taking the time to delve into this subject.

There are few events in a lifetime that evoke deep-seated emotion and vivid recollection. The terrorist attacks against the United States by al-Qaeda on September 11, 2001 (9/11), are clearly one of those historic moments that remain frozen in our minds. I poignantly remember my personal reaction then and how it affects me now. September 11 changed my life, as it did for so many of us. As the agent in charge of the FBI's Financial Crimes Program at that time, I was in a unique situation where I was afforded an opportunity to respond in a manner few other people could. I was in a position to "follow the money." I witnessed, first-hand, investigative successes which disrupted or deterred funding intended to support terrorist activities. I am an ardent believer that terrorist financing is a critical component of the war against terrorism.

By way of background, immediately after 9/11, I was responsible for the formation and oversight of the FBI-led, multi-agency, Financial Review Group, which evolved into a formal Section within the FBI's Counterterrorism Section, known as the Ter-

rorist Financing Operations Section (TFOS). Since retiring from the FBI, I have provided consulting services regarding fraud, money laundering, and terrorist financing. Many of my clients are in the financial services sector.

My Government investigative and private sector consulting experience has provided me a rare opportunity to understand two very distinct perspectives. For over 30 years, I had a law enforcement perspective. In that capacity, my perspective was Government- and investigative-driven. For the last 9 years, in my current position as a consultant, my perspective has shifted to one that is industry- and compliance-driven. This provides me with a unique understanding of the responsibilities, sensitivities, challenges, and frustrations experienced by the Government and financial sectors in dealing with anti-money laundering (AML) and terrorist financing considerations. There is a notable difference in perspectives. This is one of the many challenges we face in dealing with terrorist financing and other criminal problems.

Identifying suspicious activity in financial institutions, especially involving terrorist financing, is extremely challenging. This is where understanding perspective is critically important. When it comes to identifying and reporting suspicious activity, you must consider the "who, what, where, when, why, and how." Law enforcement typically focuses on the "why" as the most important element while financial institutions are most concerned about the "how." This is one of the areas where collaboration between law enforcement and financial institutions is not as consistent as it could be. Law enforcement frequently shares "war stories" about investigative successes with industry. However, they do not often provide specific information about "how" financial institutions were used by the bad guys. The Internal Revenue Service is one agency that does provide this type of information to financial institutions at industry training forums.

In order to succeed, individual terrorists, such as lone wolves, and terrorist groups must have access to money. They require funding in order to operate and succeed. Invariably, their funding sources will flow through financial institutions. To function, terrorists must have continuous access to money. Regardless of how nominal or extensive, the funding flow is operationally critical. Terrorists, like criminals, raise, move, store, and spend money in furtherance of their illicit activity. This is why Bank Secrecy Act (BSA) reporting requirements are essential to our National Security. This fact becomes more compelling in view of the actuality that finance is one of the two most significant vulnerabilities to terrorist and criminal organizations.

Terrorist financing is not adequately understood and extremely difficult to identify, especially when funding flows are more nominal. This is where Government, through the interagency community engaged in terrorist financing, must interact more efficiently with the financial services sector to identify terrorist financing. It is possible for financial institutions to identify terrorist financing, but it is highly improbable. We must take continual actions that increase the probability factor, thereby increasing the possibility of identifying funding flows. The challenge confronting the Government and banking community is to improve the effectiveness of the process. This is where the Government needs to be more effective and efficient in the "how" of assisting financial institutions in identifying suspicious activity. Government should develop better feedback mechanisms to financial institutions about "how" terrorists use financial institutions and provide them with typologies that financial institutions could use for transactional monitoring.

The interagency community that has jurisdiction and responsibility for terrorist financing should be commended for their contributions. Terrorist financing is one area where the Government excelled following 9/11 and where they continue to perform admirably.

Terrorist financing is every bit as challenging today as it was in the immediate aftermath of 9/11. Law enforcement, regulators, and intelligence agencies here, in the United States (U.S.), and abroad, have achieved noteworthy and meaningful accomplishments. New proactive and progressive methodologies have been developed and implemented in furtherance of such efforts. When the Government succeeds in implementing and executing proactive methodologies, the ability of terrorists to carry out operations is diminished. However, lingering concerns and the resiliency of terrorists to adapt to change, coupled with the ease of exploitation of systemic vulnerabilities in the financial sector, will perpetuate the challenge of addressing the issues presented by terrorist financing.

Despite the gains we've made, the financial services sector is as inherently vulnerable today as it was on 9/11. On October 3, 2001, as a senior executive in the FBI, I testified before the House Financial Services Committee. One of the issues I addressed was vulnerabilities or high-risk areas in the financial services sector. I testified that wire transfers, correspondent banking, fraud, and money services busi-

nesses were the biggest areas of vulnerability to the financial services industry at that time.

Today, I have refined the vulnerabilities in two categories: Crime problems and facilitation tools. The most significant crime problems we currently face in the financial services industry are fraud and money laundering. Fraud was magnified during the recent financial crisis and continues to represent a significant threat to our economy. Money laundering encompasses all other criminal activity where the proceeds of crime are laundered through financial institutions. The key facilitation tools used in furtherance of fraud and money laundering are: Wire transfers, correspondent banking, illegal money remitters, shell companies, and electronic mechanisms.

Illegal money remitters represent one of the most significant problems confronting banks. This has been an on-going challenge. Many banks cannot identify customers who operate illegal money remittance operations. On the surface, they appear to be a legitimate business. However, if like the Carnival Ice Cream Shop in Brooklyn, New York, they actually functioned as illegal money remitters funneling money to high-risk countries. Consequently, terrorist and criminal groups have used illegal money remitters in furtherance of their illicit activities. There are a number of cases we can point to that illustrate this problem to include the Time Square bombing case.

Sanctions against Iran have caused Iranian entities to regularly use shell companies to hide beneficial ownership, as well as rely on correspondent banking and wire transfers to illegally move funds. The Lloyds Bank "stripping" case is a prime example of how correspondent banking was used by Iran as a facilitation tool. In this matter, Lloyds stripped SWIFT messaging information to hide Iranian bank identification in order to avoid U.S. banking monitoring detection. The Alavi Foundation case was an example of how Iran used shell companies to hide beneficial ownership in a New York City office building. Both cases involved the use of wire transfers.

The use of electronic payment mechanisms is an area of growing concern regarding how terrorists move money due to the anonymity and instant settlement it affords. Electronic payment mechanisms are becoming more prolific and vulnerable to misuse by criminals and terrorists. Africa is a venue of concern for the growing use of electronic mechanisms.

The Government has made consistent incremental progress in addressing terrorist financing. Individual agencies and entities responsible for terrorist financing have matured and evolved. They have individually and collectively developed investigative methodologies to effectively deal with the constant and emerging challenges. Although on an agency-by-agency level, we can point to enhanced capabilities, the true measure of Government success is the ability of the interagency community to work as a unified team, and to parlay their collective investigative capabilities into a joint Government-wide terrorist financing strategy. In the aftermath of 9/11, I was part of such a working group that was led by David Aufhauser, then the General Counsel at the Treasury Department. Mr. Aufhauser was a true leader who marshaled the interagency collaborative initiative. He was an unsung hero and visionary. I recommend that the committee periodically assess the status of the interagency terrorist financing working group to ensure that it is effectively coordinating the broader interagency initiatives.

The face of terrorism since 9/11 has been altered significantly. The last few years have seen tremendous change and instability in the Middle East. Core al-Qaeda has been decimated and affiliate groups have evolved into greater threats. Our homeland has experienced a growing concern involving lone wolf terrorists and other home-grown threats. These developing factors have modified terrorist financial typologies.

The evolving terrorist landscape has led to less costly terrorist plots. As noted earlier, the more nominal amounts have been more challenging to identify. This is due to the fact they are generally more undetectable. For example, many lone wolf terrorists such as Farooque Ahmed, who plotted to detonate a bomb on the Washington, DC metro system, relied on money from their legitimate jobs to pay for their illicit activity.

The Government must continuously identify and assess emerging trends and develop case typologies they can share with financial institutions. In so doing, the financial services sector can implement transaction monitoring strategies to identify patterns of activity consistent with the case typologies of criminals and terrorists. The Government has not done this as consistently as they could have.

In general, law enforcement and the Financial Crimes Enforcement Network (FinCEN) have done a good job in sharing information with the financial services sector. However, they have not done as much as they think they have or they could. I do not make this comment lightly. When I was in the FBI, I thought I had maxi-

mized liaison relationships. It was not until after my retirement from law enforcement and my consulting work with the financial services sector that I realized I could have done more. It was a matter of perspective. If only I knew then, what I know now, I would have been dangerous. Law enforcement and FinCEN should do a better job of listening and providing feedback to financial institutions in the form of "how" terrorists and criminal organizations use the financial system in furtherance of their illicit activities.

What is important, especially in dealing with more minimal dollar amounts, is identifying case typologies and using them to develop targeted transaction monitoring strategies. This leads to the need for more consistent collaboration between law enforcement and the financial services sector. The model for this type of public- and private-sector collaboration was set in recent years by JPMorgan Chase under the leadership of compliance executive William Langford and senior investigator Phil DeLuca. Working in conjunction with the ICE Department of Homeland Security Investigations (HSI), JPMorgan Chase was able to identify financial patterns for human smugglers and traffickers. This was because HSI provided specific typologies to JPMorgan Chase setting forth the "how." This enabled JPMorgan Chase to identify patterns of transactional activity and develop targeted transactional monitoring. In so doing, JPMorgan Chase was able to provide HSI with financial intelligence information which led to successful criminal investigations. This initiative was greatly supported by an informal task force involving DHI and the financial services sector that was led by John Byrne and the Association of Anti Money Laundering Specialists (ACAMS). Because of the successful impact of this public-private partnership, ACAMS provided a special award to JPMorgan Chase and HSI, which was presented at the recent Money Laundering.com annual anti-money laundering conference. This is a great example of how law enforcement, in this case HSI, provided the "how" to a financial institution, JPMorgan Chase, and how the bank used the information to identify patterns of illicit activity. I recommend that the committee look at this collaboration as a model of the type of cooperative initiative that could be used to fight terrorist financing.

This type of initiative could be effectively used to identify terrorist financing. There are a number of scenarios that could be identified and targeted in a similar fashion. An example would be the case of a lone wolf terrorist who leaves the United States and travels to Pakistan to attend a terrorist training camp. During the time that this individual attends the training camp, it is unlikely he or she would incur any financial activity, virtually falling off the financial grid. The combination of travel to Pakistan, a high-risk country for terrorism, and a gap in financial activity, could be identified by targeted financial monitoring in a financial institution.

One of the perceived impediments to banks in regard to targeted transactional monitoring is the challenge of satisfying the regulators. Regulators are not generally forward thinkers. They deal with black-and-white issues and are more prone to a check-the-box mentality that tends to stymie progressive and innovative thinking. In fairness to regulators, their mandate is not to think outside the box but to ensure that regulatory requirements are met by financial institutions. This is a daunting task. There is often a perplexing triangle involving financial institutions, law enforcement, and the regulators. BSA reporting requirements were established to benefit law enforcement. Unfortunately, financial institutions are generally more concerned with placating their regulators than providing the "why" to law enforcement. Financial institutions, law enforcement, and regulators need to come to a better consensus about the balance of law enforcement and regulatory considerations. This is an area that this committee or the House Financial Services Committee should look into.

Certain countries pose a challenge to deal with in terms of their capacity or political will to establish terrorist financing regimes. Other countries, most notably Iran, pose a significant threat and are indifferent to complying with international standards as they flaunt their nuclear and/or other ambitions. The first step to deal with these situations is to coordinate a strong interagency response at the domestic level. This calls for relying on a combination of diplomatic, regulatory, intelligence, military, and law enforcement responses. By orchestrating a choreographed response strategy, pressure could be leveraged against these countries. The second step is to coordinate international responses and strategies with the Financial Action Task Force (FATF), the United Nations and other international bodies.

There is a growing and troubling nexus between transnational criminal organizations, drug cartels, and terrorist organizations. Each has their own objective and is willing to deal with the others to further their own interests. The Lebanese Canadian Bank investigation manifests this emerging problem. It illustrated the alliance between Hezbollah, a terrorist organization, the Joumaa drug trafficking and money laundering organization in Lebanon, and the Los Zetas Mexican drug cartel. This

troubling alliance relied on drug trafficking and trade-based money laundering, among other activities to facilitate the illicit activities of three dangerous transnational groups. The interagency community should closely assess the collaborative operations of these organizations and develop strategies to deal with other similar associations.

As noted earlier, it is possible to identify terrorist financing but highly improbable. This is one area where collaboration and partnership between the public and private sector are essential. In 2009, I wrote an article addressing how to increase the probability through such collaboration. For the most part, the same points I articulated then are applicable today. Accordingly, there are six steps the Government and financial services industry should take to collectively and unilaterally increase the probability of identifying terrorist financing. They are:

1. The Government and financial sector must recognize the importance of terrorist financing-specific training. This is a dimension that is lacking on both sides, although more on the part of financial institutions. Without specific training, the ability to understand and disrupt terrorist financing is more difficult to achieve.
2. The Government must develop a means to legally provide security clearances to select personnel in financial institutions in order to share limited intelligence information that could be scrubbed against bank monitoring systems to identify account or transactional information associated with terrorists. The FBI has been discussing this challenging issue since 9/11, in concert with select industry compliance leaders and experts.
3. A consistent and comprehensive feedback mechanism from law enforcement must be developed that demonstrates the importance of BSA reporting, especially the significance of Suspicious Activity Reports (SARs). FinCEN's SAR Activity Review is a good mechanism that provides insightful information. In addition, specific feedback from law enforcement to financial institutions concerning the value and benefit of BSA data, including SAR filings, would have a dramatic impact on the morale of individuals responsible for SAR reporting.
4. There must be an assessment by the Government of all SARs related to or identifiable with terrorism cases. Such a review would identify specific red flags that could be used as a training mechanism and more importantly, could be factored into identifying typologies that could be used for the monitoring/surveillance capabilities of financial institutions. In addition, a determination could be made as to why the financial institution filed a SAR. In many instances, the SAR was filed for violations other than terrorist financing. Understanding what triggered the SAR filing; in tandem with how the SAR ultimately was linked to terrorist interests would be insightful.
5. In addition to assessing SARs, the Government and industry should collectively identify and assess as many case studies, of terrorist financing-related investigations, as can be identified and legally publicly accessed. The case studies should be compared to determine what types of commonalities and patterns of activity exist. In addition, common red flags should be easily discernible. This type of case study assessment, coupled with the SAR analysis, would provide more meaningful information to consider in identifying terrorist financing characteristics, especially in cases involving more nominal financial flows. This would enable financial institutions to more effectively use surveillance and monitor techniques to identify questionable transactional information.
6. A combination of BSA data, particularly SARs, combined with empirical and anecdotal information would enable the Government and financial sector to collectively and unilaterally conduct trend analyses. This would be a significant factor in identifying emerging trends. On a Government level, this would contribute to implementing investigative and enforcement strategies. On the institutional level, this would enable the financial sector to implement strategies to mitigate risk.

Although the landscape has changed, and methodologies have evolved since 9/11, terrorist financing remains the same. In essence, terrorists must have access to funds when they need them in order to operate. It is incumbent that Government agencies cooperate, coordinate, and communicate on both an interagency level and with the private sector in order to deny terrorists from moving and accessing funds and thereby diminishing their ability to operate.

I would again like to thank the committee for affording me the opportunity to participate in this forum. I would be happy to answer any questions or to elaborate on my statement.

Mr. MEEHAN. Let me say one thing. Unfortunately, there is just 6 minutes left in the vote that I must go vote on right now. I am

struggling with how best to do this. I think they are going to give me a minute to sprint, so what I am going to do is ask Ms. Eckert to do her testimony, and then I am going to have to reconvene with the rest of the committee.

Let me go to Ms. Eckert's testimony and then I will give you a closing comment and we will try to work from there, but I want to make sure you get your opportunity to hit the essence, Ms. Eckert. So the Chairman now recognizes Ms. Eckert.

STATEMENT OF SUE E. ECKERT, SENIOR FELLOW, WATSON INSTITUTE FOR INTERNATIONAL STUDIES, BROWN UNIVERSITY

Ms. ECKERT. Mr. Chairman, thank you very much for the opportunity to be here, and I want to commend you and the committee for focusing on this vitally important issue. I don't think enough attention has been paid to it. Ten years with experience in countering the financing of terrorism, I think it is a very opportune time to focus on it.

I have a number of recommendations. So I am not going to review what has been done with regard to al-Qaeda. There are specific initiatives that I am part of that we are looking at, the effectiveness of sanctions, for example, against Iran and North Korea, other sponsors of terrorism. My comments in the testimony and today are primarily focused on al-Qaeda.

I won't focus right now in terms of some of the unintended consequences of the regime countering financing of terrorism, but I think it is important to pay attention to some of those because they have the potential to weaken what is a critically important initiative both globally and Nationally.

So what I would do is just very briefly offer a couple of points that I think that we need to take account of as we look at strengthening the CFT measures.

First is, I think it is important to understand that we need enhanced information analysis. There is still a great deal we don't know. New electronic payment methods through cell phones and stored value cards, digital currencies that some of my colleagues have been talking about are very important to focus on. We need to understand differences in terms of not only the terrorist organizations, but how they move, raise, and store funds. We need to develop metrics. In the past, the only metrics that we have had are the number of designations and the amount frozen. Those are clearly inadequate to—and they can be misleading. We haven't seen a steady progress with regard to that, but that doesn't mean that our terrorist financing initiatives are not working.

Finally, I think one of the—for information, we need to analyze the information that we have and evaluate it. The private sector provides ample amount of information, but it goes into a process, as one of my colleagues has said, and it is not really utilized and not really analyzed except when it gets to the law enforcement side.

So I think that there is an awful lot that can be done within the current system to be able to discern patterns that could assist financial institutions in identifying terrorist financing.

The second major area is collaboration and information sharing with the private sector. The central role in this is the private sector. Governments don't freeze assets; the private sectors do. There are a number of ways. We have all talked about the need for greater collaboration, but I think that the partnerships so far has been a pretty much one-way flow of information.

I think there is more that can be done. Security clearances for certain individuals in financial institutions; the British have done it to great effect. What we need to do is to understand that initiatives to enhance information will make our law enforcement intelligence efforts smarter and more effective.

Inadequate capacity in other countries. We cannot do this alone. The United Nations has played a very important role, Egmont and a number of the FATF have played important roles in establishing this global regime, but more needs to be done to provide assistance to other countries to be able to put in place the necessary legal, administrative, and enforcement mechanisms to carry out this prohibition in the financing of terrorism.

Further, I think that it is time, 10 years later, really for a critical assessment of effectiveness. In this regard there has been, you know, a lot focused on some of the positive things, but not necessarily the cost or limitations of the current approach and whether or not we are focusing on where the challenges are going and how the terrorists are raising moneys now. It is still focused primarily on the formal financial sector, and I think that we really need to take a good hard look at what we are doing now. As you said, I had to strike in my testimony the number of times I said recalibrate, so I am pleased that we are thinking in the same vein.

But in short, there has been an impressive global effort to regulate transport or movement of funds through formal sector financial institutions, but al-Qaeda and other groups have adapted and they continue to have access to funds. In order to be effective we have to reassess and recalibrate policies and create a genuine partnership with the private sector.

Thank you, sir.

[The statement of Ms. Eckert follows:]

PREPARED STATEMENT OF SUE E. ECKERT

MAY 18, 2012

Chairman Meehan, Ranking Member Higgins, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you to discuss the critical issue of terrorist financing. As the disrupted airline bombings plot out of Yemen last week indicates, terrorist threats to the United States persist notwithstanding the death of Osama bin Laden and decline of the hierarchical organization of al-Qaeda.

My comments are based on my previous experience as assistant secretary of commerce responsible for regulating dual-use goods and technology, as well as more recent academic initiatives to strengthen the instrument of U.N. sanctions. Currently, my colleague at the Graduate Institute in Geneva, Thomas Biersteker, and I are leading the Targeted Sanctions Consortium, an international group of scholars and practitioners conducting a comprehensive and comparative analysis of the impacts and effectiveness of U.N. sanctions, including those targeted on al-Qaeda and affiliated groups, as well as sanctions against Iran and DPRK. I've also worked with the United Nations Counterterrorism Implementation Task Force to explore the identification of indicators that might be useful to financial institutions in detecting potential terrorism financing activity. In this regard, I've had the opportunity to interact with the private sector, National regulators, and international counterterrorism

policymakers involved in the global effort to combat the financing of al-Qaeda and affiliated groups. The views expressed however, are my own, and not necessarily endorsed by any entity or colleagues with whom I am affiliated.

Due to time constraints, this abbreviated statement focuses on terrorism financing related primarily to al-Qaeda (AQ) and lays out some considerations for ways forward. I am happy, however, to provide an expanded statement based upon our book, *Countering the Financing of Terrorism,* and more recent initiatives assessing the effectiveness of U.N. sanctions.

EVOLVING THREAT AND MEANS OF FINANCING

Al-Qaeda today is profoundly transformed from the group that engineered the attacks on 11 September 2001. The once-hierarchical organization evolved into a confederation of allied entities, and subsequently into a general jihadi movement, with al-Qaeda core (AQC) serving more as an inspirational vanguard, a source of legitimization and justification for acts of global terrorism by affiliates, rather than as a source of the planning, financing, and execution of terrorist attacks. Regional affiliates such as AQ in the Arabian Peninsula (AQAP), AQ in the Islamic Maghreb (AQIM), and al-Shabaab in Somalia, now outnumber AQC remnants in Pakistan and remain committed to al-Qaeda ideology. Even with new revelations about bin Laden's final activities in Abbottabad, the AQ affiliates constitute the more significant contemporary terrorist threat.

Likewise, the means by which terrorists finance activities have changed, and today largely consist of criminal means conducted within a state. Formal sector transactions and even the transnational movement of funds by AQ have been severely constrained, in part due to the success to the extensive global efforts to counter the financing of terrorism (CFT). Formal sector financial institutions generally have not been used for the transfer of funds across international borders to AQ since 2003; rather, AQ affiliates have increasingly resorted to the use of cash couriers and barter trade to move funds. Self-financed criminal activities such as credit card and check fraud, theft, extortion, and kidnapping for ransom represent more common methods utilized by terrorists to finance their activities.[1] Charitable donations as a significant means of financing terrorism also appears to have diminished, as recent evidence concerning the diversion from Islamic charities is lacking (and most of the legal cases resulting in successful convictions have been based more on violations of tax and reporting rules, rather than terrorist financing). While informal value transfer systems or hawala were used for the transfer of funds prior to the attacks of 11 September and most recently by the Times Square bomber, the overwhelming majority of such transfers are legitimate and advance important social and global developmental functions.

Recognition of the changing structure and financing of AQ and affiliated groups is important, as effective strategies for countering the financing of terrorism must similarly adapt to the current threat. With more than a decade of CFT experience, now is an opportune time to take stock of what has been accomplished in order to recalibrate U.S. and international efforts to more effectively address the evolving nature of terrorist financing. I commend the subcommittee for focusing on this issue, and hope additional review will be undertaken.

In this regard, it is worth remembering that prior to 9/11, there was little concerted attention focused on terrorist financing, with al-Qaeda able to raise funds from donors in Gulf States and charitable organizations and move them through financial institutions. Few requirements other than those mandated by UNSCR 1267 existed to restrict financing, with almost no emphasis on implementation (indeed, country reports prior to 2001 largely consisted of one sentence—"We have taken all necessary steps to comply with the resolution.") In the past decade, there has been a sea-change in the recognition and implementation by Member States of legal, administrative, and enforcement measures to combat terrorism financing.

CFT DEVELOPMENTS AND CHALLENGES

Since 9/11, we've witnessed an impressive global initiative to disrupt financial support for terrorism. The United States has worked diligently to launch a worldwide campaign to make it more difficult, costly, and risky for AQ and affiliated groups to raise and move money around the world. As a result, new and significant international institutional frameworks have evolved to address CFT, including cru-

[1] Note that this is not the case with the Taliban which has adapted over time in Afghanistan and Pakistan, in large part due to territorial control facilitating revenues through taxation of drug production, transiting goods, diversion of international assistance, and ransom from kidnappings.

cial roles by the United Nations Security Council, the Financial Action Task Force, the World Bank, IMF, Egmont Group, as well as private-sector initiatives like the Wolfsberg Group. UN Security Council Resolutions 1267, 1373, and 1540 (and successor resolutions) provide the legal basis and legitimacy for Member States to take necessary steps to put into place National legal and administrative mechanisms to freeze terrorist assets. Multilateral CFT efforts have been essential in stemming terrorist funds.

The global CFT regime utilized preexisting policy instruments but greatly expanded them. Through designations or listings of individuals, organizations, and corporate entities and the freezing of their assets, CFT efforts have primarily focused on preventing the use of formal sector financial institutions for the trans-border transfer of funds that could be used to support acts of terrorism. Initiatives to license informal value transfer systems and register charities have also resulted.

Notwithstanding the important accomplishments of terrorism sanctions to date, complications and unintended consequences have arisen. National and regional courts have faulted the U.N. process of designating individuals as well as with the adequacy of procedures for challenging those designations. Perceptions of unfairness in the application of targeted sanctions and potential violation of due process have generated concern and public opposition in several countries, including among legislatures, threatening to undermine the credibility and effectiveness of U.N.-targeted sanctions. The most prominent case of Saudi businessman Yassin Abdullah Kadi, is still under appeal at the European Court of Justice, but if successful could force the European Union not to implement mandatory Chapter VII sanctions thereby establishing a dangerous precedent and potentially undermining U.N. terrorism sanctions. Notwithstanding important procedural enhancements in recent years, however, legal challenges persist. This problem cannot be "solved" definitively, but rather must be managed to dissuade national or regional courts from questioning the underlying security rationale for listings. Continued review of U.N. designations and innovations in the delisting process are necessary for the legitimacy of international CFT measures and the future utility of the instrument of multilateral sanctions.

The freezing of assets or exclusion from the international financial system are indeed powerful terrorist financing tools, but such measures can have far-reaching consequences. Fears that there would be a decline in charitable contributions to Muslim charities have been realized to an extent, which could have implications for efforts to address root causes of terrorism. Targeted financial sanctions are not as targeted as they might initially appear; in the case of al Barakaat, the collateral damage of freezing the assets of the broad group of companies led to severe disruption of fund transfers to a large portion of the Somali population. Concerns for the risks involved with money service businesses (MSBs) resulted in the shuttering of Somali MSBs in several states, leaving large diaspora communities without viable means to transmit money cheaply and efficiently to relatives since there is no functioning banking system in Somalia.

Moreover, the regulatory burden on financial institutions has increased considerably. Compliance with enhanced reporting requirements, new internal procedures to screen customers, and train staff to block or freeze individual transactions have escalated costs as responsibility for CFT implementation rests primarily with the private sector. In addition, banks have terminated relationships with perceived risky sectors—MSBs, embassy banking, and certain correspondent banking relationships, resulting in the labeling of some sectors as "unbankable." The dramatic increase in the volume of information submitted by financial institutions, including the millions of SARs filed annually, which remain largely unanalyzed and continues to be a source of frustration to financial institutions. Processing information is far more important than simply accumulating it, and it is important that regulation be prudently designed with this in mind.

Likewise, the success of CFT instruments ultimately depends on parallel implementation by other countries. Despite progress since September 11, serious deficiencies of capacity within Member States to implement CFT measures exist (e.g. to criminalize terrorist financing, prohibit financial support to terrorists, and freeze the assets of those who commit or support terrorist acts). Implementation is uneven, and in some states, capacity is virtually nonexistent. Enhanced initiatives to assist countries in building the legal and administrative infrastructure to implement and enforce financial sanctions are necessary.

Overall, however, CFT efforts have constrained AQ and its affiliates in their ability to access essential support. As noted by the 1267 Monitoring Team in a recent report, financial sanctions have among other things, restricted the ability of those listed to continue to promote the objectives of AQ and their associates, alerted law enforcement to the activities of listed parties, and signaled to the world (and other potential financiers of terrorism) the resolve of the international community to com-

bat funding of terrorism. While far from perfect and with much more that can and should be done to strengthen CFT measures, it is important to keep these accomplishments in mind—indeed, the glass is more than half full!

CONSIDERATIONS FOR THE SECOND DECADE OF CFT INITIATIVES

As the United States and the international community move forward to strengthen CFT policies in the coming years, the following considerations are useful to keep in mind:

- The importance of realistic expectations as to what financial sanctions can reasonably achieve. Terrorism will continue, and AQ still exists (with access to funds). This does not mean that TF initiatives are ineffective, but rather we must be cognizant of the appropriate role of TF sanctions play as but one element in a larger CT strategy.
- When assessing the impact and effectiveness of CFT measures, it is essential to appropriately define the purposes. An innovation of the Targeted Sanctions Consortium's methodology[2] includes evaluating effectiveness of sanctions in terms of multiple and differing purposes of sanctions, to: (1) Coerce or change targets' behavior; (2) constrain terrorist activities (or access to essential resources such as funds thereby raising costs and forcing changes in strategy); and (3) signal/stigmatize targets violating international norms through terrorist acts.
- While progress has been made in CFT, terrorists are constantly evolving the means by which they raise and use funds; the international response needs to be dynamic as well. The basic framework focusing on preventing the use of formal sector institutions for cross-border transfers of funds remains largely unchanged. New strategies and tools to address current financing (e.g. cash couriers, stored-value instruments, informal value transfer systems (IVTS), kidnapping etc.) are necessary.
- CFT measures are considered among the most "effective" sanctions, yet there is public perception that sanctions generally are not effective. More needs to be done to demonstrate and make the case regarding the effectiveness of TF sanctions.

With terrorists' evolution of financing means, it is critical to continually review and adapt U.S. and international CFT responses. Military planners are famous for preparing for the last war, and it is important that those concerned with countering the financing of terrorism not make such a mistake. Al-Qaeda has changed. The nature of its fundraising has changed. The ways in which it moves, stores, and uses funds have changed. It is important that CFT efforts proceed from this knowledge, rather than squander limited resources.

The following are general areas that could be considered in future efforts to strengthen CFT measures:

Enhanced information and analysis

The old adage—the more you know, the more you realize how much you don't know—applies amply to the subject of terrorist financing There is still a great deal we do not know, for example, regarding the use of informal value transfer systems, trade diversion, traditional cash smuggling, and new electronic payment methods through cell phones, stored value cards, and digital currencies. Notwithstanding greater understanding regarding AQ's financing of terrorism, and "despite all of our sophistication, we have neither starved the beast nor produced very good intelligence on how exactly these organizations continue to finance themselves," as Lee Hamilton noted. There is a significant need for the further research and analysis in this area.

Differentiate among groups and means to finance terrorist operations

It is important that CFT initiatives distinguish between (and differentiate among) groups committing acts of terrorism. Those acting on a global scale, like AQ, have different needs and means of financing themselves, particularly when they are compared to groups acting on a local or regional scale. Territorial-based groups can extract resources in ways that approximate the state (i.e. Taliban exacting tariffs or quasi-taxes from the population). There are fundamental differences in the goals, scope of operations, and the ultimate objectives of groups acting globally and groups contained within a defined territorial space. Extending existing CFT efforts aimed

[2] For more information about the Targeted Sanctions Consortium, a comprehensive, systematic, and comparative assessment of the impacts and effectiveness of U.N. targeted sanctions regimes over the past 20 years, see *http://graduateinstitute.ch/internationalgovernance/UN_Targeted_Sanctions.html*.

at al-Qaeda to other circumstances risks diffusing the effort and decreasing effectiveness. One size does not fit all.

Develop metrics

There are relatively few quantitative indicators and reliable sources of information to assess CFT initiatives but it would be useful to try to devise additional metrics of effectiveness. Metrics most commonly associated with terrorist financing—the total number of designations and the amount of money frozen—are inadequate and can be misleading. As difficult as such an endeavor would be, it is important to attempt to assess the effectiveness of CFT efforts. The consequences of failing to do so are inappropriate and potentially ineffective policies to thwart terrorist acts. Policymakers and academics alike must demand better and more transparent sources of information in order to more thoroughly understand and assess terrorist financing efforts.

Evaluate and analyze TF information

As noted by others, FinCEN receives nearly a million Suspicious Activity Reports (SARs) from financial entities annually, of which less than 1% relate to TF, yet little systematic analysis of the information results. FinCEN generally passes SARs on to the FBI who integrates the information into their database in order to identify trends and suspicious transactions. However, the current system lacks requirements for the systematic analysis of data to be able to discern patterns that could assist FIs in screening for terrorist-related transactions.[3] The same applies to sharing of case information at the international level through which comprehensive analyses, lessons learned, policy-useful conclusions and guidance for both Government agencies and the private sector could possibly emerge. Is it an issue of resources or lack of priority? What could and should be done to most effectively mine the information reported by FIs? USG officials have previously referenced the number of cases in which financial information from SARs played a role; this information should be updated and made available.

TF prosecutions

Successful prosecution on TF grounds are limited—in many cases of suspected financing, convictions are easier to obtain on alternative charges. Should we be concerned with the relatively small number of successfully prosecuted TF cases? What are the obstacles, and are legislative changes needed?

Collaboration/information sharing with financial sector

Despite 10 years of espousing the need for closer public-private partnership to combat TF, the two-way exchange of information remains limited—in most cases, it's the financial community providing input with very little feedback. The FBI created a financial sector working group that meets periodically, but compliance officials still complain about a lack of information to help detect terrorist transactions. Analysis of SARs information that aided in law enforcement investigations could help FIs identify typologies and trends they should be alert to.

The United Kingdom has instituted a system whereby select representatives of financial institutions receive security clearances so sensitive information regarding transactions can be shared. A similar initiative has been discussed in the United States, but little progress seems to have been made. Is this a good idea, and if not, why not? What are other ways in which the USG can collaborate with financial institutions? Are additional protections (i.e. safe harbor provisions) needed?

Notwithstanding the absence of reliable terrorism financing indicators, the information provided by financial institutions remains critically important to intelligence and law enforcement efforts to disrupt terrorism. When intelligence on possible terrorist activities is shared with financial institutions, the information they provide is often vital and unavailable from other sources. New initiatives to enhance information sharing between governments and the private sector should be prioritized.

Address inadequate CTF capacity in other countries

To be effective, CFT measures must be implemented in a comparable manner by other countries. While the United Nations is an important source of legitimacy (requiring Member States to criminalize the financing of terrorism and to freeze the assets of individuals/entities designated as terrorists) only Member States can put into place the necessary legal, administrative, and enforcement measures to counter

[3] An initiative by a group of researchers to collect and analyze examples of terrorist financing (TF) through financial institutions in order to discern indicators of terrorism finance was stymied by the lack of access to information (sanitized SARs redacted of identifying info which DoJ was willing to provide).

TF. Even with successes as noted, there remain significant deficiencies in the capabilities of many Member States to meet their international CFT obligations (to criminalize terrorist financing, prohibit financial support to terrorists, and freeze the assets of those who commit or support terrorist acts). More needs to be done to provide adequate assistance for MS to put into place the necessary legal, administrative, and compliance measures, and current initiatives should be enhanced

Great public awareness and understanding of CTF initiatives

There is a need for broader understanding of the importance and utility of CFT measures, both designations and terrorist financing tracking. Most information regarding the reasons for designations and the effectiveness of the CFT in identifying networks or preventing acts of terrorism is closely held by Government agencies. While protection of sources and methods is necessary, excessive classification and lack of documentation to justify designations undermines public confidence in, and support for, the CFT regime.

Critical assessment of CFT effectiveness

Ultimately, the effectiveness of National and global efforts to counter the financing of terrorism depends on the nature of the threat (the assessment of risk) and the appropriateness of the response to that threat (i.e. that the benefits of the policy response outweigh the costs of the measures enacted). When it comes to an assessment of the benefits of CFT efforts, there is strong evidence that it is more difficult for AQ and affiliated groups to use the formal financial sector to support operations today. The capacity of AQ and others to commit acts of terrorism has been degraded. Yet there is little systematic assessment of the costs and limitations of the current approach. "Staying the course" of current policy may nor be the most appropriate action, especially given the changing and adapting nature of al-Qaeda.

Beyond these general areas, specific consideration should be given to:

Charities.—Traditionally, al-Qaeda and other groups have utilized charities, NGOs, and mosques to raise funds through direct solicitations and diversion of donations intended for humanitarian purposes. While the risk of abuse of the charitable sector remains real, a differentiated approach, distinguishing between financing humanitarian networks affiliated with resistance groups and financing terrorism, is needed. Blanket condemnation of groups providing social welfare services alienates Muslim constituencies and prevents aid from reaching those most in need. Government efforts should focus on assisting charities to be more transparent; clarifying what constitutes financing of terrorism and association; designating independent bodies to regulate and investigate charities; and accrediting charities or developing indicators of trust/approval so that contributors know the group can be trusted to deliver support to appropriate projects.

In addition, zakat contributions are central to the practice of Islam, and a policy that places charitable giving to Islamic organizations under general suspicion contributes to a perception that the effort is directed against the entire Muslim community, rather than a very small segment of that community. Not only is this profoundly unfair, but it will ultimately undercut the effectiveness of other counter-terrorism efforts. Special effort must be taken to reaffirm support for charitable giving through transparent processes.

Informal Transfers.—Regulation of remittance vehicles is necessary, but should be done in a way that is proportionate to risk and appropriate to particular socio-economic environments. In countries where informal systems exist alongside a well-functioning conventional banking sector, hawala or other informal value transfer systems (IVTS) should be registered and required to keep adequate records. In states at risk of institutional collapse or states without functioning banking systems, requirements beyond registration may not be feasible. Governments should conduct outreach efforts to consult, engage, and build consensus among IVTS operators with regard to the most appropriate measures. Positive incentives should be created for participants in the sector to implement regulatory frameworks. In this regard, greater emphasis should be placed on the traceability of transactions, rather than centralization of data and should be sufficiently flexible so as not to drive IVTS underground.

Trade Diversion.—International trade is vulnerable to abuse by terrorists, as well as other criminals, through false invoicing and the use of commodities to move funds, yet relatively little attention has been focused on this mechanism. Governments need a more concerted focus on trade diversion, both through greater understanding of the threat posed by lack of trade transparency and the techniques used, as well as specific efforts directed at anticipating, detecting, and thwarting attempts by terrorist groups or their supporters to take advantage of this mechanism. Trade transparency units to analyze, share, and track international trade data to identify

anomalies have been formed, albeit more slowly than hoped. Greater cooperation with the private sector victimized by diversion schemes should be explored, and enhanced priority placed on interagency cooperation and prosecution of trade diversion cases.

Since 9/11, an impressive global effort to regulate the trans-border movement of funds through formal sector financial institutions has ensued, but AQ and other groups have adapted and developed alternative means to raise and move funds to continue their terrorist activities. In order to be effective, CFT policies continually must be reassessed and recalibrated. Genuine partnership between the private sector and Government is critical to effective CFT policies, and new ways of sharing information and creating incentives for compliance must be explored.

Thank you for the opportunity to discuss terrorist financing since 9/11—I look forward to questions and being of assistance to the committee.

Mr. MEEHAN. Well, thank you each for your testimony. I am very frustrated that we are competing with what was a very dynamic schedule over in the House. I am going to at this point in time recess the committee, and I have to be candid in saying it is not likely we are going to be able to collect the membership that I think this issue deserves. I am hoping that we will recess and look for an opportunity to reconvene at a point in time that will be convenient for you and us. I am hoping that you would still be able to participate. The issue we are discussing is too important to rush through in this forum, and I think that you have laid the groundwork with your testimony today that will allow us to have a jumping-off point in any number of areas.

The service that you each have given to our country at the critical time as we began this process was vital to the protection of this Nation, but it is the continuing ability for us to adapt as our enemy has adapted that is going to allow us to protect this Nation in the future. Few people are talking about this. You understand it. We have got to communicate this, and do it effectively.

So I thank you. We will follow up at a later time, but at this point in time, without objection, the subcommittee is in recess subject to the call of the Chair.

The Chair indicates that we will consult with the Minority in order to provide Members with adequate notice of when we will convene.* Thank you for your testimony, and I look forward to following up with you at an another forum in which we can develop these issues far more broadly. Thank you.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned.]

*The subcommittee did not schedule a continuation of this hearing.

APPENDIX

QUESTIONS FROM CHAIRMAN PATRICK MEEHAN FOR JONATHAN SCHANZER

Question 1a. With our military successes against al-Qaeda core leadership in Afghanistan and Pakistan, there is a growing trend of al-Qaeda affiliated groups and adherents filling the void and taking the lead in launching attacks against the homeland.

Given the relatively low amount of money required to plan and launch a terrorist attack, how realistic is it to expect U.S. and international counterterrorism entities to identify funds that might be used to undertake terrorism-related activity?

Answer. The 9/11 Commission's Executive Summary notes that the United States must "expect less from trying to dry up terrorist money and more from following the money for intelligence, as a tool to hunt terrorists, understand their networks, and disrupt their operations."[1] I fully agree with this assessment. This does not mean that we should stop trying to identify funds marked for terrorist activity. But recent years have seen a decline in the identification or seizure of such funds.

Question 1b. What are some of the persistent challenges in identifying and investigating an activity suspected of financing terrorism? What are some of the trends in how terrorist groups acquiring funds to support their objectives?

Answer. My sense is that there is just not enough collection being done for this purpose. Indeed, there are too many other intelligence challenges that our Government is working to meet. As always, allocation of resources requires tough choices. In terms of trends, as I noted in my prepared testimony, terrorists are increasingly gravitating to organized crime to support their objectives. This provides an opportunity for intelligence specialists to work hand-in-hand with law enforcement.

Question 1c. Is the decision to pursue a terror financing investigation based on the amount of money suspected of being acquired for terrorism-related purposes? If so, what is the minimum monetary amount of terrorism-related funds the U.S. Government assesses as worthy of investigating?

Answer. I am no longer in a position to answer that. When I served in Government, the specific amount was not a primary consideration.

Question 1d. Can you describe the decision-making process and considerations by which the U.S. intelligence and law enforcement communities decide whether to stop terrorism-financing related activity and charge a suspect arrest or choose to allow the activity to continue in hopes of following the trail of funds to a larger network of support or to entities that may be planning a terrorist attack?

Answer. When I served in Government, the decision to designate was one undertaken by an inter-agency working group. The different agencies could, at times, disagree about the need for designation. This could sometimes slow the process.

Question 2. President Obama recently signed an Executive Order allowing the Treasury Department to freeze U.S.-based assets of persons who the White House has identified as a "threat to the peace, security, and stability" of Yemen.

Do you think this is an effective use of the designation authority? Especially when a group such as Boko Haram—who have killed thousands of civilians and are in constant contact with AQIM—remain undesignated?

Answer. AQIM and Boko Haram are important targets. But governing is about choosing priorities. In this case, I think the Yemeni designations were the more pressing ones. Juan Zarate, a former Bush administration counterterrorism adviser,

---

[1] "The 9/11 Commission Report—Executive Summary," *National Commission on Terrorist Attacks Upon the United States,* July 2004, *http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf.*

also agrees that these designations can "help steer toward political stability in Yemen."[2]

Question 3a. In 2011, the U.S. Government revealed the findings of a multi-year law enforcement operation to dismantle a complex, transnational network involved in money laundering and drug trafficking. The case involved Hezbollah, Mexican, and Colombian drug trafficking organizations, the Taliban, Lebanon, Colombia, Panama, several countries in West Africa, U.S. car buyers, a U.S. shipping company, bulk cash couriers, plans for weapons trafficking deals, and the Beirut-based Lebanese Canadian Bank (LCB).

Does the fact that groups such as Hezbollah and the Islamic Revolutionary Guard Corps continue to use criminal ventures create opportunities for U.S. enforcement mechanisms—such as our robust counternarcotics tools—to roll up these vast networks?

Answer. Yes, the involvement of terrorist groups in criminal ventures creates exploitable opportunities. David Aufhauser, former general counsel of the U.S. Department of Treasury, notes that "both terrorist financing and traditional financial crimes have one thing in common—they leave a financial footprint that allows us to trace financial flows, unravel terrorist financing networks, and uncover terrorist sleeper cells."[3] Our Government has tools at its disposal to uncover that footprint.

I have also noted that when terrorist groups—particularly religious ones—enter into the world of organized crime, it creates a liability from the perspective of public relations. When pious ideologies are sullied by criminal funds, this is something the U.S. Government should exploit.

Question 3b. How does counterterrorism fit in this increasingly interconnected underworld?

Answer. From what we have seen, Middle East terrorist groups maintain a pious public face in their home territories, but engage with the underworld in far-off places, such as Latin America or West Africa. In a few cases, such as that of the Colombian FARC, groups directly engage with the underworld to their own detriment.

Question 4a. The U.S. Government's on-going investigation of the Lebanese Canadian Bank is of particular interest from a money laundering perspective because it highlights the consequences of poor compliance with anti-money laundering regulations in the formal financial system.

Given the Lebanese Canadian Bank case, what more can be done to protect the formal financial system from exploitation by terrorists?

Answer. This case exposed the weakness of the FATF system. The system simply does not put enough pressure on countries that are less motivated to fight terrorism. We need to strengthen the international system. There needs to be tougher penalties for noncompliance.

Question 4b. How can the U.S. Government more effectively mitigate the threats posed by trade-based money laundering and bulk cash smuggling and other ways outside the formal financial sector?

Answer. This is also a problem that stems from the weakness of the FATF system. We need to apply greater pressure on those countries where trade-based money laundering and bulk cash smuggling is pervasive. The primary problem is a lack of sustained effort. But, as always, even in countries where there is a will, there may be a lack of resources.

Question 5. There is an increasing concern in the counterterrorism and intelligence community that terrorist organizations are increasingly using criminal activities that are outside of the formal international financial system to raise funds to carry out attacks and further their goals.

How important are terrorist funds derived from criminal activities for the operational sustainability of major terrorist groups compared to other non-criminal sources of funds, including state sponsors and private sector donations?

Answer. The problem is pervasive. In 2003, the Orlando Sentinel reported that according to Gen. James T. Hill, commander of the U.S. Southern Command, "Radical Islamic groups in the Middle East are getting between $300 million and $500 million a year from various criminal networks in Latin America."[4] Moreover, Brazil

---

[2] Arshad Mohammed and Jason Lange, "U.S. Sends Warning to Saleh Backers in Yemen," *Reuters,* May 16, 2012, *http://www.reuters.com/article/2012/05/17/us-usa-yemen-assets-idUSBRE84F1GS20120517.*

[3] David Aufhauser, "The Threat of Terrorist Financing," United States Senate Committee on the Judiciary, June 26, 2003, *http://www.au.af.mil/au/awc/awcgate/congress/terrorist__financing.htm.*

[4] "U.S. General: Islamic Rebels Get Cash From Latin America Gangs," *Orlando Sentinel,* March 10, 2003, *http://articles.orlandosentinel.com/2003-03-10/news/0303100117__1__latin-america-southern-command-miami.*

estimates that "more than US$6 billion a year in illegal funds is laundered in the [tri-border area]," according to a recent U.S. Government report. The same report stated that "Hizballah clearly derives a quite substantial amount of income from its various illicit activities in the TBA, in addition to financial support from the government of Iran and income derived from narcotics trafficking in Lebanon's Al Beqa'a Valley."[5]

Question 6. Foreign Terrorist Organization designation by the Secretary of State is an important tool our Government uses to deter donations or contributions to and economic transactions with terrorist organizations. There are currently 50 groups listed by the State Department as designated Foreign Terrorist Organizations.

Which FTO-designated groups would you say are the best resourced and most proficient at evading American and international financial regulations? Which use the U.S. financial system the most?

Answer. Over time, just about every designated terrorist organization has learned how to evade U.S. sanctions. They have largely dropped out of the formal financial sector and severely limited their exposure to institutions where the United States has jurisdiction. This is why it has become harder to "catch" terrorist money.

Question 7. All of the witnesses mentioned in their prepared testimony that the Government needs to interact with the financial sector to identify terrorist financing.

How should the Government develop more effective case typologies and feedback mechanisms about how terrorists use financial institutions? Is this mostly an educational issue where we need to empower financial institutions in order to monitor transactions for suspicious or anomalous behavior?

Answer. America's financial institutions employ compliance professionals to ensure that terrorists do not exploit their services. A robust continuing education program is something that could be considered.

Question 8a. The Financial Action Task Force on Money Laundering is comprised of 36 member countries and territories and two international organizations and was organized to develop and promote policies to combat money laundering and terrorist financing. The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines.

What are the areas of greatest need for improvement in the FATF surveillance process?

Answer. Special recommendations, rather than laws, create an environment where compliance appears less than mandatory. Similarly, mutual evaluations carry less weight than official oversight. FATF's multilateral structure makes it easy for countries to do the minimum required of them. This is a culture that, in my opinion, needs to be addressed.

Question 8b. How does the United States evaluate the threats to the global economy arising from money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction?

Answer. I don't believe I am equipped to answer this question.

Question 8c. How should we be prioritizing these threats and how effectively has the FATF process been in addressing these threats?

Answer. I don't believe that FATF has been terribly effective in addressing these threats. These are topics of conversation at FATF, but not necessarily action items. As for the United States, our Government continues to assess threats and makes decisions based on priorities. In all of these areas, our Government has allocated significant resources.

Question 9. KPMG, a private consulting firm, released in October 2011 the findings of an anti-money laundering survey of major international banks. They found that 80% of respondents reported an increase in costs associated with anti-money laundering that averaged around 45% since 2007. The major sources of cost increases identified by the KMPG survey were: (1) Enhanced transaction monitoring, (2) increased external reporting requirements to internal regulators and external law enforcement agencies, and (3) increased anti-bribery and anti-corruption activities.

In your opinion, are there sufficient resources devoted to countering the financing of terrorism and money laundering? Alternatively, are the resource costs associated with implementing such financial regulations too burdensome on either the private or public sectors?

---

[5] "Terrorist and Organized Crime Groups in the Tri-Border Area (TBA) of South America," *Federal Research Division—The Library of Congress,* December 2010, *http://www.loc.gov/rr/frd/pdf-files/TerrOrgCrime__TBA.pdf.*

Answer. According to a Congressional Research Service report, "traditional anti-money-laundering tools appear to be of limited use in disrupting terrorist financing."[6] Accordingly, it may not make much sense to devote more resources to the anti-money-laundering component of the problem. Critics also question the need for increased funds going to the Treasury's counterterrorism efforts because less and less cash has been frozen. But this fails to take into account how effective Treasury has been in squeezing Iran with sanctions. This effort, designed to help prevent Iran from attaining a nuclear weapon, also happens to deprive the regime of the cash that it previously used to finance terrorism. This has been a net positive. For this reason, I believe the funding of Treasury's programs should continue.

Question 10. There has been growing concern at DHS, particularly within ICE, about the widespread use of prepaid and stored value cards as a way of smuggling illicit funds into the country which could fund terror activity. Some estimates are that $1 billion annually is moved into the country this way, with most of those funds nearly impossible to track.

Would you agree that prepaid and stored value cards are a growing danger to being able to target terrorist financiers? What steps would you recommend DHS and the Department of the Treasury take to combat this emerging trend?

Answer. According to Dennis Lormel, "There is no empirical statistical data establishing the nexus between credit card exploitation and terrorism." Based on my experience, I largely agree with this. When I served at Treasury, I personally saw cases that proved to be rare exceptions.

Lormel also states that "The focus for credit card fraud should be placed on both the source and availability or distribution of funds." He notes that "Al-Qaeda operatives commit credit card information theft and fraud more on an individual basis than as a group or cell activity; however, depending on the circumstances, they will commit fraud as a group or cells." In contrast, he says that "Because Hezbollah functions like an organized crime family, their criminal activities, which include credit card information theft and fraud, are more likely to be group or cell oriented."[7] These are trends that need to be examined moving forward.

Question 11a. On June 29, 2012, the Obama administration imposed sanctions on a pair of informal money-exchange networks—known as hawalas—in Afghanistan and Pakistan in what officials described as the first use of the tactic to attack the financial underpinnings of Taliban militants who rely on the system to fund their insurgency. The Treasury Department said that the designations were coordinated with similar measures adopted by the United Nations as part of a broad effort to slow the flow of cash used by the Taliban to pay salaries and purchase weapons for attacks in Afghanistan. The United Nations also added the names of the same two institutions and their principal backers to a list of groups officially associated with Taliban militancy, meaning they will be subject to international sanctions as well.

Considering how widespread their use is, how difficult is it for U.S. Government to really get a handle on some of the terror financing and money laundering activities being conducted under the hawala system?

Answer. The hawala system is a tough challenge. While tens of billions of dollars pass through hawaladars each year, a recent GAO report states that "officials and researchers we spoke with could not provide estimates on the extent of terrorist use of informal banking systems and other alternative financing mechanisms."[8]

According to the 9/11 Commission's monograph on terror financing, the hawala system has become less of an issue when tracking the funds of al-Qaeda. After we began actively tracking terror financiers, operatives shifted to bulk cash smuggling.[9]

And while hawalas may continue to pose a significant terror finance threat, according to Robert Looney, "a crackdown by Arab and South Asian governments at the behest of Western governments is simply not feasible. The vast majority of the money is from legal, legitimate sources, and the hawala organizations are numerous and extremely powerful." He correctly adds that, "if the desire of the authorities is to constrain or significantly reduce the importance of hawala activity, this means reducing the economic incentives to use the Hawala system. There is probably no

---

[6] Rensselaer Lee, "Terrorist Financing: The U.S. and International Response," *Congressional Research Service,* December 6, 2002, *http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL31658__12062002.pdf.*

[7] Dennis Lormel, "Terrorism and Credit Card Information Theft," *Shift4 Corporation,* September 2007, *http://www.shift4.com/pdf/s4-wp0806__terrorism-and-credit-card-information-theft.pdf.*

[8] "Terrorist Financing," *Government Accountability Office,* November 2003, *http://www.gao.gov/new.items/d04163.pdf.*

[9] "Monograph on Terror Financing," National Commission on Terrorist Attacks Upon the United States, Accessed July 23, 2012. *http://www.9-11commission.gov/staff__statements/911__TerrFin__Monograph.pdf.*

better way to accomplish this than to facilitate cheap, fast remittances across international boundaries, and to do away with dual and parallel exchange markets, which are always an incentive to keep transactions underground."[10]

Question 11b. How could the United States be more effective in targeting the hawala systems being used by drug traffickers to fuel the Taliban insurgency in Afghanistan and Pakistan?

Answer. If we have not done so already, the U.S. Government needs to establish assets within these hawala systems who could help identify these individuals and entities.

Question 11c. Would closer collaboration with the United Nations help our Government's ability to identify hawala networks engaged in illegal behavior?

Answer. While the United Nations can be effective in some specific instances, I don't have faith that it can have an impact here. The problem of hawalas is a sensitive one. I believe there is little to no chance that Member States would risk the political backlash that would undoubtedly arise from targeting these informal financial networks that effectively prop up the economies in some of the world's most neglected places. In short, the United Nations fosters an environment where the consensus determines policy. This will ensure that the United Nations remains largely irrelevant in the fight against illicit hawala transactions, and more broadly, terror finance, for years to come.

QUESTIONS FROM CHAIRMAN PATRICK MEEHAN FOR JOHN A. CASSARA

Question 1a. With our military successes against al-Qaeda core leadership in Afghanistan and Pakistan, there is a growing trend of al-Qaeda affiliated groups and adherents filling the void and taking the lead in launching attacks against the homeland.

Given the relatively low amount of money required to plan and launch a terrorist attack, how realistic is it to expect U.S. and international counterterrorism entities to identify funds that might be used to undertake terrorism-related activity?

Answer. Detecting the rather miniscule amount of funds needed to launch small-scale terrorist attacks is a daunting challenge. For example, the attempted 2010 cargo plane bombing is estimated to have cost our adversaries approximately $4,200. In my opinion, intelligence from human sources, coupled with robust analytics, are probably our best countermeasures.

Question 1b. What are some of the persistent challenges in identifying and investigating an activity suspected of financing terrorism? What are some of the trends in how terrorist groups acquiring funds to support their objectives?

Answer. In my experience, policy makers' early over-reliance on "financial intelligence" to combat terror finance continues to be a tremendous bureaucratic and operational roadblock. Regulations have been the priority over field investigations. Another obstacle has been our intelligence and law enforcement officers' unfamiliarity with terror finance methodologies. A third impediment has been our over-reliance on sanctions and designations. A fourth impediment has been the decimation of Treasury enforcement after the creation of the Department of Homeland Security. And, a fifth issue has been the unwillingness to utilize known capabilities to assess the financial intelligence that both industry and the Government spends tremendous resources on to produce.

The most troublesome trend because it is so widespread is what I call "local crime" to finance terror. Narcotics trafficking, intellectual property rights violations, cigarette smuggling, etc. are just a few examples. Yet this development also holds promise because by cracking down on local crime—predicate offenses for money laundering—we might also disrupt terrorist operations. I believe this premise would hold true for domestic crime and encouraging problematic countries to be more vigilant investigating predicate offenses.

Question 1c. Is the decision to pursue a terror financing investigation based on the amount of money suspected of being acquired for terrorism-related purposes? If so, what is the minimum monetary amount of terrorism-related funds the U.S. Government assesses as worthy of investigating?

Answer. I am not currently in a position to answer this question. However, given evolving abilities to link actors and actions, what might appear to be small dollar activities can now be traced to larger networks of actors and activities, as we are seeing in medical fraud for example. My hope is that FinCEN and other agencies

[10] Robert E. Looney, "Following the Terrorist Informal Money Trail: The Hawala Financial Mechanism," *Strategic Insights,* Volume 1, Issue 9 (November 2002), *http://www.nps.edu/Academics/centers/ccc/publications/OnlineJournal/2002/nov02/southAsia.html.*

aren't using dollar values as the litmus test because it simply isn't a good indicator of harm.

Question 1d. Can you describe the decision-making process and considerations by which the U.S. intelligence and law enforcement communities decide whether to stop terrorism-financing related activity and charge a suspect arrest or choose to allow the activity to continue in hopes of following the trail of funds to a larger network of support or to entities that may be planning a terrorist attack?

Answer. I am not currently in a position to answer this question.

Question 2. President Obama recently signed an Executive Order allowing the Treasury Department to freeze U.S.-based assets of persons who the White House has identified as a "threat to the peace, security, and stability" of Yemen.

Do you think this is an effective use of the designation authority? Especially when a group such as Boko Haram—who have killed thousands of civilians and are in constant contact with AQIM—remain undesignated?

Answer. I believe sanctions and designations are one tool of many that should be employed to combat terrorists and those that support terrorists. However, in my opinion, the United States has relied far too heavily on sanctions and designations. Sanctions, designations, and other "black lists" are also not uniformly applied. In the years immediately after 9/11, I participated in a number of interagency discussions regarding targets of designations. The interagency time and resources expended on this exercise produced few actual results. The Government has finite resources and as a result of our fixation on designations other countermeasures were shortchanged. I concur with an unnamed retired diplomat who said, "Sanctions (and designations) always accomplish their principal objective, which is to make those who impose them feel good."

Question 3a. In 2011, the U.S. Government revealed the findings of a multi-year law enforcement operation to dismantle a complex, transnational network involved in money laundering and drug trafficking. The case involved Hezbollah, Mexican and Colombian drug trafficking organizations, the Taliban, Lebanon, Colombia, Panama, several countries in West Africa, U.S. car buyers, a U.S. shipping company, bulk cash couriers, plans for weapons trafficking deals, and the Beirut-based Lebanese Canadian Bank (LCB).

Does the fact that groups such as Hezbollah and the Islamic Revolutionary Guard Corps continue to use criminal ventures create opportunities for U.S. enforcement mechanisms—such as our robust counternarcotics tools—to roll up these vast networks?

Answer. Yes. See my response to 1b above.

Question 3b. How does counterterrorism fit in this increasingly interconnected underworld?

Answer. Terrorism is increasingly financed by the underworld of transnational crime. By lifting the veil of underworld finance and operations, we can impact terror.

Question 4a. The U.S. Government's on-going investigation of the Lebanese Canadian Bank is of particular interest from a money laundering perspective because it highlights the consequences of poor compliance with anti-money laundering regulations in the formal financial system.

Given the Lebanese Canadian Bank case, what more can be done to protect the formal financial system from exploitation by terrorists?

Answer. There are no short-term fixes to protect the formal financial system from exploitation. Although imperfect, the best international countermeasure regarding compliance measures in international banking continues to be recommendations, programs, policies, and mutual evaluations undertaken by the Financial Action Task Force (FATF) and FATF-style regional bodies. I have witnessed first-hand how countries respond to FATF-led international censure by putting in place world-standard anti-money laundering and counter-terrorist finance countermeasures.

Question 4b. How can the U.S. Government more effectively mitigate the threats posed by trade-based money laundering and bulk cash smuggling and other ways outside the formal financial sector?

Answer. See No. 13 below. Additionally, I have suggested in other responses, the use of better technological solutions that can help the Government stay at least current with developing threats, and will help suggest optimal ways to mitigate, or prevent threats from being realized.

Question 5. There is an increasing concern in the counterterrorism and intelligence community that terrorist organizations are increasingly using criminal activities that are outside of the formal international financial system to raise funds to carry out attacks and further their goals.

How important are terrorist funds derived from criminal activities for the operational sustainability of major terrorist groups compared to other non-criminal sources of funds, including state sponsors and private-sector donations?

Answer. With the decline of the state sponsorship of terrorism and efforts to crack down on private-sector donations, terrorist organizations and lone-wolf terrorist actors increasingly rely on local crime to finance their activities. I do not believe it is possible to quantify the extent of any particular source of terrorist funds.

Question 6. Foreign Terrorist Organization designation by the Secretary of State is an important tool our Government uses to deter donations or contributions to and economic transactions with terrorist organizations. There are currently 50 groups listed by the State Department as designated Foreign Terrorist Organizations.

Which FTO designated groups would you say are the best resourced and most proficient at evading American and international financial regulations? Which use the U.S. financial system the most?

Answer. I am not currently in a position to answer this question.

Question 7. All of the witnesses mentioned in their prepared testimony that the Government needs to interact with the financial sector to identify terrorist financing.

How should the Government develop more effective case typologies and feedback mechanisms about how terrorists use financial institutions? Is this mostly an educational issue where we need to empower financial institutions in order to monitor transactions for suspicious or anomalous behavior?

Answer. I do not believe the burden of spotting potential terror funding should be put on financial institutions. Rather, banks and money service businesses should continue to file financial intelligence and suspicious activity reports with the Department of Treasury. The spotlight should be on the Financial Crimes Enforcement Network's (FinCEN's) inability to effectively exploit the approximately 18 million pieces of financial intelligence it receives annually and to identify suspect or anomalous behavior. FinCEN should also do a better job of alerting reporting institutions to current money laundering and terror finance schemes.

Question 8a. The Financial Action Task Force on Money Laundering is comprised of 36 member countries and territories and two international organizations and was organized to develop and promote policies to combat money laundering and terrorist financing. The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines.

What are the areas of greatest need for improvement in the FATF surveillance process?

Answer. I have spent many years working with the FATF, including participating in many mutual evaluations. In my opinion, a serious disconnect between "process" and "results" has developed. The bottom-line metric in evaluating countries' anti-money laundering "regimes" is the number of successful arrests, prosecutions, and convictions. With few exceptions, most countries fail in this regard. Over the last 15 years, the emphasis has been on the process; i.e. laws, rules, regulations, creation of financial intelligence, creation of a financial intelligence unit, etc. Yet, the fixation on process or form rather than substance, combined with lack of expertise, corruption, and lack of political will all conspire against results. It may also be that the tools being deployed in the surveillance process are outdated and unable to provide the most insightful results.

Question 8b. How does the United States evaluate the threats to the global economy arising from money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction?

Answer. I am not currently in a position to respond to this question.

Question 8c. How should we be prioritizing these threats and how effectively has the FATF process been in addressing these threats?

Answer. I am not currently in a position to respond to this question.

Question 9. KPMG, a private consulting firm, released in October 2011 the findings of an anti-money laundering survey of major international banks. They found that 80% of respondents reported an increase in costs associated with anti-money laundering that averaged around 45% since 2007. The major sources of cost increases identified by the KMPG survey were: (1) Enhanced transaction monitoring, (2) increased external reporting requirements to internal regulators and external law enforcement agencies, and (3) increased anti-bribery and anti-corruption activities.

In your opinion, are there sufficient resources devoted to countering the financing of terrorism and money laundering? Alternatively, are the resource costs associated with implementing such financial regulations too burdensome on either the private or public sectors?

Answer. In my opinion, per my response in 7a above, industry already bears too much of the regulatory AML/CFT burden. Industry produces an enormous amount of financial intelligence but there is very little return on investment. The primary reason is that the information that they spend so much money to generate is not systematically or comprehensively (strategically or tactically) exploited by Treasury's FinCEN. In that regard, I believe that FinCEN has been provided sufficient financial resources, but would question how they have utilized those resources. In particular, I don't believe they have made the best investments to help them effectively understand the financial intelligence that they already possess, nor to report that information to other Government or private-sector entities. I also question whether the Government has made proper investments in terms of recruiting, retaining, and developing the analytic community, especially with respect to evolving tools and capabilities.

Question 10. There has been growing concern at DHS, particularly within ICE, about the widespread use of prepaid and stored value cards as a way of smuggling illicit funds into the country which could fund terror activity. Some estimates are that $1 billion annually is moved into the country this way, with most of those funds nearly impossible to track.

Would you agree that prepaid and stored value cards are a growing danger to being able to target terrorist financiers? What steps would you recommend DHS and the Department of the Treasury take to combat this emerging trend?

Answer. I agree that prepaid and stored value cards are a growing danger in targeting terrorist financiers and money launderers both in the United States and overseas. I suggest Congress and the administration review the 2007 National Money Laundering Strategy that discusses prepaid and stored value cards and outlines countermeasures. Unfortunately, after 5 years little has been done. I urge Congress and the administration to hold FinCEN and others accountable for the lack of action.

Question 11a. On June 29, 2012, the Obama administration imposed sanctions on a pair of informal money-exchange networks—known as hawalas—in Afghanistan and Pakistan in what officials described as the first use of the tactic to attack the financial underpinnings of Taliban militants who rely on the system to fund their insurgency. The Treasury Department said that the designations were coordinated with similar measures adopted by the United Nations as part of a broad effort to slow the flow of cash used by the Taliban to pay salaries and purchase weapons for attacks in Afghanistan. The United Nations also added the names of the same two institutions and their principal backers to a list of groups officially associated with Taliban militancy, meaning they will be subject to international sanctions as well.

Considering how widespread their use is, how difficult is it for U.S. Government to really get a handle on some of the terror financing and money laundering activities being conducted under the hawala system?

Answer. The challenges involved in identifying the misuse of hawala and similar informal underground value transfer operations is enormous—both in the United States and overseas.

Question 11b. How could the United States be more effective in targeting the hawala systems being used by drug traffickers to fuel the Taliban insurgency in Afghanistan and Pakistan?

Answer. This is a complex question that requires a lengthy answer. To summarize, in the Afghanistan and Pakistan context trade is the primary vehicle used to provide "counter-valuation" between hawaladars. We need to work with Afghanistan, Pakistan, and countries in the surrounding region (including Iran) to promote the concept of "trade-transparency." If we present the issue as a revenue enhancer (combating customs fraud) the governments involved will be receptive. Trade-transparency should be made part of the regional Afghan Transit Trade Agreement. By promoting trade-transparency and combating customs fraud, we will shine the spotlight on underground finance and disrupt hawala operations. See the following article I wrote for more details: *http://www.johncassara.com/index.php?option=com_content&view=article&id=24:the-afghan-transit-trade-how-afpak-drug-lords-and-terrorists-are-moving-money-and-transferring-value&catid=2:articles&Itemid=8*.

Question 11c. Would closer collaboration with the United Nations help our Government's ability to identify hawala networks engaged in illegal behavior?

Answer. The short answer is no. In my experience, most countries do not recognize hawala or other similar types of underground financial systems or collect data or intelligence on financial networks.

Question 12. Mr. Cassara, in your prepared testimony you talked about "draining the swamp," or how cracking down at home on local and transnational financial crime might become one of the most effective strategies to combat terrorism. You

said that law enforcement, intelligence, and military organizations must learn to look beyond the immediate circumstances of a given local crime because these isolated acts could have more sinister ties.

How do you get State and local law enforcement to change this mentality with regard to fighting crime domestically in teaching them to "ask the next question" during the course of a routine investigation and question where the money is going?

Answer. At the State and local level the three-step solution is training, intelligence, and prioritization. Regarding training, I am familiar with a number of first-rate training initiatives such as the State and Local Anti-Terrorist Training (SLATT) program run by the Institute for Intergovernmental Research (IIR) and sponsored by the Bureau of Justice Assistance (see *www.slatt.org*). There are other training initiatives as well. Effective training programs should be expanded. Specifically, officers and analysts should be trained how to recognize terror finance indicators. They should be made familiar with the financial and analytical tools that they have available to them (sometimes these tools are not available but that is another issue). From personal experience in working with State and local law enforcement, I am appalled by the lack of knowledge of financial crimes and resources that could be made available. Once law enforcement officers and analysts have a better understanding of terror finance methodologies, they should use that information to task reporting sources to develop operational intelligence. They should also make it a matter of routine not to become fixated on the immediacy of the local crime they are investigating (narcotics, stolen cars, organized theft rings, human smuggling, etc) but rather to "ask the next question," i.e., "What about the money?" Finally, Federal, State, and local law enforcement administrations should not become absorbed with the quick "statistic" or easy bust. Rather, they should understand that money laundering and terror finance investigations are a long-term investment that often times fail. However, they are too important to short change for more immediate returns. Much of this conundrum is budget-driven. Scarce funding is provided based on perceived results; i.e. statistics. Unfortunately, the individuals that look at the statistics cannot differentiate between a quick case or an impact case because they are often reported the same way.

Question 13a. Mr. Cassara, you mentioned in your prepared testimony that by promoting trade transparency and using technology to spot anomalies or discrepancies in trade data that intelligence or law enforcement entities may already possess, we may be able to use trade as a "back door" to enter into previously hidden financial networks.

Can you elaborate on this idea and how sharing information with State and local law enforcement may aid in this process?

Answer. There are a large number of underground financial systems in the United States; they are also known as "parallel banking," "underground finance," "informal value transfer systems, etc." Examples are hawala, the black market peso exchange, and the Chinese fei-chien systems. While there are a number of ways that underground financial brokers periodically balance their books, historically and culturally trade is the preferred method of providing "counter-valuation." Over- and under-invoicing is the primary vehicle used. Thus discrepancies or anomalies in trade-data could be indicators of simple fraud or possibly the back door to underground financial networks. So if a State or local law enforcement agency identifies a business that does not make economic or market sense, caters to suspect groups, or has a side business involved with remitting money or value overseas, it could be an entry point into previously hidden financial networks. Given the amount of data that law enforcement has access to, transparency can be enhanced by the use of technologies that seek out both anomalies, as well as previously undetected patterns. These technologies can be used with vast amounts of data that can't possibly be reviewed in relevant time periods (or at least not reviewed accurately), nor, given the amount of data, can humans understand correlations and causative relationships in the data. Technology can, and can also begin to create statistically significant linkages between transactions and actors. By using these technologies, which exist now, we can better prioritize where our law enforcement should be spending time, we have more meaningful information to share, and ultimately, we can be much more productive and successful with our limited enforcement resources.

Question 13b. In some ways isn't this the future of combating terrorist financing?

Answer. Since Richard Nixon declared "War on Drugs" in 1970, our primary countermeasure in following the dirty money trail has been tracking financial flows through banks and non-bank financial institutions. Our primary emphasis has been creating a domestic (Bank Secrecy Act et al) and then later an international network (FATF recommendations) of financial transparency reporting requirements.

I believe trade-based money laundering is the "next frontier" in international money laundering and counter-terrorist finance. We should work to put in place a

similar domestic and international network of trade-transparency. That said, the technologies that are critical to understanding terrorist financing exist now, so I could say that the future has arrived.

Question 14a. Mr. Cassara, you mentioned in your prepared testimony that the Federal Government is lagging in its deployment of advanced analytical fraud frameworks such as "predictive," "social network" and "visual" analytics.

In your opinion, is this the result of a lack of manpower or funds within the Government to deploy these cutting-edge technologies?

Answer. I am not really in a position to comment except to say, in my experience, there is a critical lack of understanding about what advanced analytics are and why they are relevant to the Federal Government.

Question 14b. You rightly raise privacy and civil liberties concerns in your testimony with regard to exploiting social network analytics. Can you explain some of the technology that exists to safeguard the dissemination of personal financial information to prevent abuse?

Answer. I am not a technologist, but let me suggest a couple of thoughts. First, many analytics don't actually rely on the movement of data from databases. Instead, they utilize "metadata", which is data about data. The reason this is important is that it provides an audit trail as to what data has been used, how it has been used, and who has had access to it. Warehouses utilizing analytics can be configured to include access controls—the more sensitive the data, the higher the clearance needed. Second, in many cases, analytics can be run in a manner that either the data is anonymized or the source of the data obscured. In the case of social analytics, the analytics are not necessarily looking for the identity of the "speaker," but searching for specific content and sentiment. Visual analytics itself does not raise privacy concerns because its focus is presenting visual depiction of information derived from statistical analysis. It thus provides an easier, less abstract way of understanding data. Finally, predictive analytics has historically been misunderstood, particularly by the privacy community. I would submit that with predictive analytics, the data is allowed to speak for itself; rather than the analyst coming to the data with preconceived ideas of what is important or causative, predictive analytics allows the data to "speak for itself," to reveal previously unknown patterns, or to reveal those factors that are truly important to an activity. In all of these cases, what is important to note is that the statistics never label activities as definitively fraudulent, or definitively linked to terrorist activity. What they do, however, is provide the analyst or investigator with unbiased information relating to abnormalities that require more human investigation.

Question 15. Mr. Cassara, you also mentioned in your prepared remarks that within the next few years, approximately 500–700 million additional pieces of financial information in the form of wire transfer data will be routed annually to FinCEN.

What are the implications for the Treasury Department and the intelligence community missing out on this crucial financial intelligence if the Government is not able to employ all available technologies to exploit it and act upon it in a timely fashion?

Answer. Currently, FinCEN is tasked by the U.S. Government to receive, analyze, warehouse, and disseminate approximately 18 million pieces of financial intelligence. Currently FinCEN is not able to fulfill this mission. The reasons are many and complex, but the primary explanation is continued failed management. If FinCEN is not able to successfully complete today's mission involving 18 million pieces of financial intelligence, we should not expect that they can handle the increased workload, which is certain to occur. I worked at FinCEN for 6 years. In my first book, "Hide & Seek: Intelligence, Law Enforcement, and the Stalled War on Terror Finance," I discussed the entrenched FinCEN culture that remains the catalyst for mission failure. We can no longer afford business as usual. The implications for the U.S. law enforcement and intelligence communities are enormous. That is why in my testimony I advanced the idea of a Financial Intelligence Unit "in a box" or going further downstream with the data and the analytics directly to the consumer (see No. 16 below).

Question 16. Mr. Cassara, in 2008, you raised concerns that financial intelligence is not being adequately exploited when Treasury's Financial Crimes Enforcement Network (FinCEN) analyzes and shares the hundreds of thousands of Suspicious Activity Reports (SARs) they come across every year. Last month, FinCEN reported that number of suspicious activity reports filed by financial institutions had increased last year by 13.5% to an all-time high.

Can you explain your concerns regarding SARs to the Committee and elaborate on how you believe FinCEN should be most effectively exploiting the valuable financial intelligence in those Suspicious Activity Reports?

Answer. As noted above, SARS are filed at great cost to industry. Unfortunately, they have not been effectively exploited. The reasons are many including failed management, until recently a series of failed data mining/analytical systems, lack of skilled analysts, a revolving door of departing staff due to poor morale, and FinCEN turning itself away from its original mission of supporting law enforcement to emphasizing the regulation of the BSA. Under FinCEN's current framework, in order to address the above question regarding the lack of effective exploitation of SARS the other underlying problems will have to be addressed. However, there is a new idea on the horizon. The technology now exists to not only disseminate SARs and other financial intelligence directly to law enforcement users but allow a state-of-the-art analytics platform to accompany the data. Per law and regulation, Treasury and FinCEN would still control the financial intelligence but we could do an "end run" around the current structure of FinCEN that acts as an impediment to effective exploitation of SARs and other financial intelligence by disseminating both the data and the analytical tools directly to the end-user. In effect, we could send a Financial Intelligence Unit (FIU) "in a box" to approved users at the Federal, State, and local level.

Question 17. Mr. Cassara, you have written extensively about trade-based money laundering and invented the concept of trade-transparency units which is now a part of the U.S. Government's National Anti-Money Laundering Strategy. In addition, the Department of Homeland Security's Immigration and Customs Enforcement has adopted this concept by establishing the world's first TTU.

Can you explain this concept a bit, and how DHS has implemented their own TTU program through ICE?

Answer. FATF defines trade-based money laundering (TBML) as the "process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins." According to the U.S. State Department, this practice has reached "staggering" proportions in recent years. Although the problem is difficult to quantify precisely, TBML is found globally, including in the United States. In fact, some experts believe the majority of U.S. money being laundered abroad is moved out of the country via undervalued exports. The U.S. Department of Treasury estimates that the Black Market Peso Exchange, a single TBML methodology found in the Western hemisphere, launders billions of drug dollars every year.

Criminal and terrorist groups that abuse trade are assisted by a number of factors:

- The massive amount of global trade that takes place daily.
- Financial diversity (i.e. the wide variety of financial controls found in different countries, the diverse financial arrangements made between governments, and the innumerable different types of financial deals found in international commerce).
- The co-mingling of licit and illicit funds and trade items.
- The low risk of detection.
- Limited Government understanding and resources to detect suspect trade transactions.

Trade-based money laundering scams take a wide variety of forms. For example, it could be simple bartering or a commodity-for-commodity exchange. In certain parts of Afghanistan and Pakistan the going rate for a kilo of heroin is a color television set. Drug warlords exchange one commodity they control (opium) for others that they desire (luxury and sports utility vehicles). However, generally speaking, money laundering through simple invoice fraud and manipulation is most common. The key element of this technique is the misrepresentation of the trade good in order to transfer value between importer and exporter. The quantity, quality, and description of the trade goods can be manipulated. The shipment of the actual goods and the accompanying documentation provide cover for "payment" or the transfer of money.

In order to move money out of a country, practitioners import goods at overvalued prices or export goods at undervalued prices. In order to move money into a country, practitioners import goods at undervalued prices or export goods at overvalued prices.

It is important to understand that when a buyer and seller are working together, the price of the item can be whatever they want it to be. As long as parties in an international trade transaction do not get too greedy and cause noticeable trade anomalies, their chances of detection by bankers, customs services, law enforcement, and other authorities are miniscule.

Every country in the world has a customs service and keeps track of what comes in and what goes out. In fact, in many parts of the world customs duties are the primary source of Government revenue. So although there are differences in the

way governments gather and store trade data, enough similarities exist to conduct effective analysis and TBML investigations. Such investigations require three basic elements:

- Access to import and export data. Moreover, if the trade data can be augmented by combining it or overlaying it with other data such as financial, travel, commercial, law enforcement, etc. following the suspect activity will be further enhanced.
- The ability to promptly exchange data (adhering to standard international safeguards and privacy concerns) with other countries.
- Expertise in analyzing and investigating TBML.

Recognizing the growing threat of TBML, in 2004 the Department of Homeland Security's Immigration and Customs Enforcement (ICE) established the world's first trade-transparency unit or TTU. Subsequently, other TTUs have been created in Argentina, Brazil, Paraguay, Colombia, Panama, Mexico, and other countries. As demonstrated above, by comparing one country's targeted imports or exports against the corresponding data of another country, trade anomalies can be detected that could be indicative of customs fraud, tax evasion, contraband smuggling, or trade-based money laundering. The data could even be the back door into underground financial schemes including those linked to terror finance. I am pleased that DHS is beginning to look at how to augment this data analysis through the use of robust technologies that can parse through enormous amounts of data in very short time increments. Of course, data analysis will only go so far. Investigations in the field are also needed.

The U.S. law enforcement and intelligence communities agree that one of the most effective counter-measures against organized crime, terrorists, systematic corruption, fraud, and many other types of serious crime is to "follow the money trail." In the years to come, I am convinced we will increasingly learn to "follow the value trail."

QUESTIONS FROM CHAIRMAN PATRICK MEEHAN FOR DENNIS M. LORMEL

Question 1a. With our military successes against al-Qaeda core leadership in Afghanistan and Pakistan, there is a growing trend of al-Qaeda affiliated groups and adherents filling the void and taking the lead in launching attacks against the homeland.

Given the relatively low amount of money required to plan and launch a terrorist attack, how realistic is it to expect U.S. and international counterterrorism entities to identify funds that might be used to undertake terrorism-related activity?

Answer. Nominal funding requirements to support terrorist activity can be very challenging for U.S. and international counterterrorism entities to identify. It is possible to identify such funding but highly improbable. Counterterrorism entities need to develop and implement investigative and analytical methodologies to increase the probability factor. Few, if any, entities existed before 9/11 that were dedicated to identifying, investigating, and disrupting terrorist financing. Since then, many entities were established with the mission to investigate terrorist financing. By using the combination of financial intelligence, human intelligence, and signal intelligence, mechanisms have been, and will continue to be, developed to identify even nominal amounts of money. By analyzing case studies, ranging from grand to simple, such as the Mumbai bombing and lone wolf schemes like that of Farooque Ahmed, who planned to detonate a bomb in the Washington, DC Metro Transit System, counterterrorism entities responsible for terrorist financing can build typologies and develop proactive and progressive investigative strategies.

Question 1b. What are some of the persistent challenges in identifying and investigating an activity suspected of financing terrorism? What are some of the trends in how terrorist groups acquiring funds to support their objectives?

Answer. One of the persistent challenges I encountered in the FBI, and that I would continue to be concerned about today is the timely collection and assessment of financial intelligence. Did my FBI Section, the Terrorist Financing Operations Section (TFOS), have intelligence information that we did not identify that could have led us to a plot or potential attack? We collected and assimilated a tremendous amount of intelligence information that we endeavored to turn into actionable intelligence for field investigators. This is particularly important in cases where a lone wolf operative did not have a record, was unknown to intelligence agencies, and used funds from a legitimate job to finance terrorist plans. Time sensitivity in these matters was always challenging.

A trend that has continued since 9/11, and has grown significantly since then, has been the movement to criminal activity as a fund-raising mechanism for terrorists. In the aftermath of 9/11, the United States and our international partners made a

concerted effort to cut off the flow of legitimate money from wealthy donors and charities. The more these efforts succeeded, the more terrorists were driven to criminal activity. This continues today. It will be interesting to assess the success of the sanctions against Iran and the revolution in Syria, two State sponsors of terrorism. This will probably result in the continued increase in criminal activity.

Question 1c. Is the decision to pursue a terror financing investigation based on the amount of money suspected of being acquired for terrorism-related purposes? If so, what is the minimum monetary amount of terrorism-related funds the U.S. Government assesses as worthy of investigating?

Answer. Terrorist financing investigations were not predicated on monetary considerations when I ran TFOS at the FBI. Terrorist financing investigations are probably still not and should never be predicated on monetary thresholds. Such investigations should be predicated upon the relation to terrorism and the potential threat represented. While I was still at the FBI in 2003, a process was established whereby all terrorism cases contained a financial investigative component. Terrorist financing investigations should focus on identifying all funding streams and disrupting terrorist activities through denying terrorists money. For terrorists to succeed, they must have a source of funds and access to their money when they need it. Disrupting the sources and/or access to money makes it extremely difficult for terrorists to succeed.

Question 1d. Can you describe the decision-making process and considerations by which the U.S. intelligence and law enforcement communities decide whether to stop terrorism-financing related activity and charge a suspect arrest or choose to allow the activity to continue in hopes of following the trail of funds to a larger network of support or to entities that may be planning a terrorist attack?

Answer. Terrorist financing investigations are a component of counterterrorism. They should be conducted in coordination with the broader counterterrorism mission and in conjunction with terrorism investigations. Terrorist financing is one tool in the arsenal. Terrorist financing investigations should be conducted with other investigative techniques to include undercover operations, use of informants, and/or wiretaps and tracking telephone calls and/or emails. The combination of these investigative techniques can be extremely productive.

The decision to allow a terrorist financing or broader terrorism investigation to continue or to take it down is extremely important. It should be based on whether an attack is imminent or not. If an attack is imminent, you need to take down the investigation immediately and prevent the attack. If an attack is not imminent, you allow the investigation to continue. In so doing, you can develop evidence to identify additional co-conspirators and funding streams. As an example, consider the Lebanese Canadian Bank investigation. Although Hezbollah was involved, and is a violent terrorist organization, there was no specific threat or imminent danger associated with the investigation. In that situation, you allow the investigation to play out. In this case, the investigation was a multi-year investigation. A number of funding streams and co-conspirators were identified and dismantled. Take a case such as the Time Square bomber. As a hypothetical, had law enforcement and intelligence agencies been aware of Faisal Shahzad and his plan to detonate a bomb in Time Square, they would have allowed the plot to unfold up to the point of imminent danger. In that case, had they been aware and determined there was no imminent danger, they probably would have identified the funding source, through the Hawala operator. Had there been imminent danger, or if imminent danger could not be determined, they would have arrested Shahzad and developed additional information and evidence in the aftermath of the take down.

When I ran TFOS at the FBI, we strove to take terrorist financing investigations in two directions: Forward to the strike team and backward to the point of financial origin. I believed there were three funding tracks, and I wanted investigations to disrupt activities in all three tracks. First, there was a fundraising track. Large sums of money, from the hundreds of thousands to millions of dollars, would be generated through mechanisms to include donations from wealthy donors, charities, State Sponsors (Iran most notably), criminal activities and other means. The money flowed into the terrorist organization for organizational use. Second, funding would be provided in a track from the organization, through a single facilitator or multiple facilitators, and to an operation. The funding flow here would be less than the flow into the organization. It would range from the hundreds of thousands to a few thousand dollars. Our primary investigative attention would be focused on the facilitators because that would take us to both the organization and to the operatives. Third, there was a track from the operation, through the facilitator(s), to the operatives. The funding flow here would be in the thousands to the hundreds of dollars.

In general, when conducting terrorist financing investigations in the first track, the organizational track, you would be more inclined to allow the investigation to continue over a longer period of time and be more deliberate and methodical in your investigative methodology. When conducting investigations into the second track (operations) and the third track (operatives) you have to deal with a greater sense of urgency and constantly assess whether an attack is imminent. Most of these investigations were shorter term because, at some point, you had to be concerned about the threat of attack.

Question 2. President Obama recently signed an Executive Order allowing the Treasury Department to freeze U.S.-based assets of persons who the White House has identified as a "threat to the peace, security, and stability" of Yemen.

Do you think this is an effective use of the designation authority? Especially when a group such as Boko Haram—who have killed thousands of civilians and are in constant contact with AQIM—remain undesignated?

Answer. If evidence exists to support designations, I am an ardent supporter for the designation process. Such actions disrupt funding flows and serve as a deterrent. Boko Haram is a violent and dangerous group. They have been very active and pose a formidable threat in Nigeria. With respect to designating other groups, I would not make designation decisions by comparing one group, such as Boko Haram, to other groups. A number of factors must be taken in consideration in the decision process to include the level of overall terrorist threat, threat to the United States, diplomatic considerations, and the need to continue the classification and protection of intelligence information.

Question 3a. In 2011, the U.S. Government revealed the findings of a multi-year law enforcement operation to dismantle a complex, transnational network involved in money laundering and drug trafficking. The case involved Hezbollah, Mexican and Colombian drug trafficking organizations, the Taliban, Lebanon, Colombia, Panama, several countries in West Africa, U.S. car buyers, a U.S. shipping company, bulk cash couriers, plans for weapons trafficking deals, and the Beirut-based Lebanese Canadian Bank (LCB).

Does the fact that groups such as Hezbollah and the Islamic Revolutionary Guard Corps continue to use criminal ventures create opportunities for U.S. enforcement mechanisms—such as our robust counternarcotics tools—to roll up these vast networks?

Answer. All criminal activity undertaken by Hezbollah, the Islamic Revolutionary Guard Corps and other terrorist organizations leave them vulnerable to detection by law enforcement and intelligence services. Law enforcement, particularly the DEA and FBI, deserve considerable credit for conducting a well-disciplined, focused, and comprehensive investigation that tied transnational criminal organizations together with terrorist groups and a number of facilitation tools to include the Lebanese Canadian Bank. Through comprehensive investigation and financial tracing, multiple funding streams between Central America, the United States, Lebanon, West Africa, and Europe were identified and dismantled. There have been at least four other significant investigations conducted by the FBI and other agencies that exposed Hezbollah's involvement in raising large amounts of money through criminal activities in the United States. The most notable of these cases was the North Carolina cigarette smuggling case known as Operation Smokescreen. A Hezbollah cell operated an elaborate scheme to smuggle cigarettes from North Carolina to Michigan. This cell generated approximately $25 million in illicit funds.

Question 3b. How does counterterrorism fit in this increasingly interconnected underworld?

Answer. The nexus between criminal and terrorist organizations has continued to grow. This trend will persist. As the U.S. Government and our allies continue to exert pressure and cut off funding streams, terrorists will further align themselves with criminal organizations and participate in criminal activity to raise much-needed money. Terrorists are extremely adaptable and consistently look for new funding mechanisms. Many terrorist organizations have become engaged in drug trafficking because drug trafficking is the most profitable criminal activity. These terrorist groups are evolving into hybrid criminal and terrorist organizations. As they do, their ideology tends to give way to greed. Greed is a vulnerability law enforcement can exploit, unlike ideology. This makes these groups more susceptible to criminal investigation and prosecution.

Question 4a. The U.S. Government's on-going investigation of the Lebanese Canadian Bank is of particular interest from a money laundering perspective because it highlights the consequences of poor compliance with anti-money laundering regulations in the formal financial system.

Given the Lebanese Canadian Bank case, what more can be done to protect the formal financial system from exploitation by terrorists?

Answer. There are some egregious examples of anti-money laundering (AML) compliance breakdowns that facilitated terrorists being able to exploit the formal financial system. The biggest failure in the Lebanese Canadian Bank case was the complicity of the Lebanese Canadian Bank with transnational organized criminal groups, a Mexican drug cartel, and Hezbollah. First, there was a total failure by the bank to have an AML program. This enabled criminal and terrorist elements to place money in the formal financial system, the first step in the money laundering process; and then to layer it, which is the second step, by moving it to other financial institutions and giving it a sense of legitimacy; and then in integrating the funds, the third step in the money laundering process, by using the illicit, but seemingly legitimate funds to purchase goods, in this case used cars from the United States, and shipping them to Africa for sale as legitimate transactions.

One way to help strengthen the formal financial system is to make a comprehensive case study out of the Lebanese Canadian Bank and specifically show financial institutions how they were exploited in this case. By developing typologies that could be built into scenarios that could be incorporated into rules for AML transaction monitoring, we can improve the system. This case study should also be used as a wide-ranging training exercise.

The Lebanese Canadian Bank case was exacerbated by the fact that Lebanon does not recognize Hezbollah as a terrorist organization. Therefore, banks in Lebanon, and banks in other countries that do not consider Hezbollah to be a terrorist organization, are inclined to bank Hezbollah. International consensus on who is a terrorist organization has been a longstanding problem.

There are other cases that can be cited, such as HSBC. The Senate Permanent Subcommittee on Investigations conducted a thorough investigation and issued a formal report on July 17, 2012, in conjunction with a public hearing involving executives from HSBC. The hearing and report serve as tools for lessons learned and should provide a deterrent to other institutions for serious shortcomings in their AML programs.

It should be pointed out that an overwhelming number of banks operating in the United States have outstanding AML programs. The AML compliance professionals in these institutions take a great deal of pride in their work ethic and dedication to rooting out money laundering and terrorist financing. I have seen this first-hand, both as an FBI agent and today as a consultant doing work in the financial services industry.

Question 4b. How can the U.S. Government more effectively mitigate the threats posed by trade-based money laundering and bulk cash smuggling and other ways outside the formal financial sector?

Trade-based money laundering has had a long history as a successful mechanism for criminals and terrorists. The Lebanese Canadian Bank case demonstrates how criminals and terrorists collaborated in different trade-based money laundering schemes to launder illicit funds. Likewise, bulk cash smuggling has long been, and continues to be, a significant problem for criminals and terrorists. In 2010 and 2011, both the Treasury Department and FBI reported that bulk cash smuggling was a huge terrorist financing concern.

In my view, one of the most significant problems and vulnerabilities we are confronted with outside the formal banking system in the United States is unlicensed and unregistered money remitters. These illegal money remitters provide hawala-like services and do not comply with Bank Secrecy Act (BSA) reporting requirements. Many banks are unaware of how many of their clients operate as illegal money remitters. This is in spite of rigorous due diligence requirements. I believe that about 80% of money remitters in the United States are illegal.

To the question of how the U.S. Government can more effectively mitigate the threats of these informal mechanisms, the answer is two-fold. First, the Government interagency community should conduct targeted investigative initiatives addressing these problem areas. Through interagency cooperation, communication, and coordination, the Government should identify the highest-priority targets in these areas and determine which agencies could make the best impact by taking the lead and develop multi-agency strategies. Second, as a component of these initiatives, the U.S. Government should bring in the private sector and subject matter experts who could provide a different perspective and different sets of information that could develop valuable financial intelligence. Public-private partnerships like this are woefully lacking.

Question 5. There is an increasing concern in the counterterrorism and intelligence community that terrorist organizations are increasingly using criminal activities that are outside of the formal international financial system to raise funds to carry out attacks and further their goals.

How important are terrorist funds derived from criminal activities for the operational sustainability of major terrorist groups compared to other non-criminal sources of funds, including state sponsors and private sector donations?

Answer. Following the terrorist attacks of 9/11, the United States and our allies made a concerted effort to deter donations to terrorists from wealthy donors, charities, and other funding sources to include State Sponsors. This was accomplished in the form of sanctions, OFAC and State Department designations, and targeted investigations by law enforcement and intelligence agencies. As a result, numerous funding sources were shut off and terrorist groups had to develop alternative funding mechanisms. They gravitated to criminal activity, which has consistently expanded over the years. Drug trafficking, kidnapping, extortion, counterfeit goods, and a variety of other crimes have become a staple for terrorist organizations.

As mentioned earlier, terrorists must have a continuous flow of funds available that they can immediately access in order to succeed. As otherwise legitimate sources of funding have diminished, terrorists have had to increasingly rely on criminal activity as a funding mechanism.

As more sanctions and pressure are exerted on Iran, it is less likely they will be able to maintain the level of State Sponsorship provided to Hezbollah and other terrorist organizations. Likewise, as Syria faces a regime overthrow, it is unlikely they will be able to provide funding and support to terrorists. This will result in an even steadier reliance on criminal activities by terrorist groups.

Question 6. Foreign Terrorist Organization designation by the Secretary of State is an important tool our Government uses to deter donations or contributions to and economic transactions with terrorist organizations. There are currently 50 groups listed by the State Department as designated Foreign Terrorist Organizations.

Which FTO-designated groups would you say are the best resourced and most proficient at evading American and international financial regulations? Which use the U.S. financial system the most?

Answer. When it comes to resources, proficiency and exploitation of the U.S. financial system, as well as the global financial system, Hezbollah is in a league by themselves. In my view, Hezbollah is not only the most proficient terrorist organization; they are the most competent criminal organization in the world. Their global infrastructure could serve as a model for organized crime. Hezbollah has an incredible world-wide infrastructure that enables them to operate criminal enterprises and function as a serious terrorist threat. Including the Lebanese Canadian Bank case, there are at least five significant investigations involving Hezbollah operations that touch on the United States that demonstrate Hezbollah's criminal organizational skills. In aggregate, their activities represent hundreds of millions of dollars in criminal activity having a U.S. nexus.

In today's environment and especially with the sanctions confronting them, Iran poses a significant challenge for the formal financial system. Their ability to hide behind shell companies and opaque beneficial ownership is a hindrance to meaningful sanctions. In addition, Iran's ability to use foreign banks as correspondent banks and to strip SWIFT messaging information from transactional records enables them to circumvent OFAC screening requirements. This is a huge problem that surfaced with Lloyds Bank a few years ago and currently with Standard Charter Bank. This is an issue that must be dealt with forcefully with offending institutions if we intend to have meaningful sanctions against Iran.

Question 7. All of the witnesses mentioned in their prepared testimony that the Government needs to interact with the financial sector to identify terrorist financing.

How should the Government develop more effective case typologies and feedback mechanisms about how terrorists use financial institutions? Is this mostly an educational issue where we need to empower financial institutions in order to monitor transactions for suspicious or anomalous behavior?

Answer. In my written testimony for the record, I made six recommendations about improving the possibility and probability of identifying terrorist financing. Three of those recommendations address how the Government should develop more effective case typologies and feedback mechanisms for terrorist financing cases. They are:

"A consistent and comprehensive feedback mechanism from law enforcement must be developed that demonstrates the importance of BSA reporting, especially the significance of Suspicious Activity Reports (SARs). FinCEN's SAR Activity Review is a good mechanism that provides insightful information. In addition, specific feedback from law enforcement to financial institutions concerning the value and benefit of BSA data, including SAR filings, would have a dramatic impact on the morale of individuals responsible for SAR reporting.

"There must be an assessment by the Government of all SARs related to or identifiable with terrorism cases. Such a review would identify specific red flags that could be used as a training mechanism and more importantly, could be factored into identifying typologies that could be used for the monitoring/surveillance capabilities of financial institutions. In addition, a determination could be made as to why the financial institution filed a SAR. In many instances, the SAR was filed for violations other than terrorist financing. Understanding what triggered the SAR filing; in tandem with how the SAR ultimately was linked to terrorist interests would be insightful.

"In addition to assessing SARs, the Government and industry should collectively identify and assess as many case studies, of terrorist financing-related investigations, as can be identified and legally publicly accessed. The case studies should be compared to determine what types of commonalities and patterns of activity exist. In addition, common red flags should be easily discernible. This type of case study assessment, coupled with the SAR analysis, would provide more meaningful information to consider in identifying terrorist financing characteristics, especially in cases involving more nominal financial flows. This would enable financial institutions to more effectively use surveillance and monitor techniques to identify questionable transactional information."

Financial institutions are required by the BSA to monitor transactions for and report suspicious activity. Overall, U.S. banks do a good job of reporting suspicious activity. This process could be improved through a meaningful feedback mechanism from the Government where the Government emphasizes the importance of SAR reporting, coupled with demonstrating "how" terrorists used financial institutions to move, store, and spend money.

In addition, terrorist financing specific training would be important. This was another of the six recommendations I spoke about in my written testimony. Terrorist financing is not well understood. As I stated in my testimony, "(w)ithout specific training, the ability to understand and disrupt terrorist financing is more difficult to achieve."

Question 8a. The Financial Action Task Force on Money Laundering is comprised of 36 member countries and territories and two international organizations and was organized to develop and promote policies to combat money laundering and terrorist financing. The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines.

What are the areas of greatest need for improvement in the FATF surveillance process?

Answer. The FATF mutual evaluation process is one of the most significant accomplishments of the FATF 40 Recommendations regarding money laundering and terrorist financing as it provides peer and public pressure to enact and then operationalize AML laws. There are approximately 170 jurisdictions who have adopted the FATF 40 Recommendations (FATF plus the FATF style regional bodies).

FATF revised the 40 Recommendations and the methodology for assessment in February 2012. According to FATF, the FATF Standards have been revised to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. At the same time, these new standards will address new priority areas such as corruption and tax crimes.

Ted Greenberg, a former Department of Justice and World Bank official, is an expert on FATF. He was involved in writing the 40 Recommendations and has participated in the FATF evaluation process. According to Mr. Greenberg, the current methodology has proven to be repetitive in its application, not focused on assessment of effectiveness, and failed to take account of corruption issues in law. Mr. Greenberg believes the new process should focus on the main weaknesses in each jurisdiction, why they are/are not effective and make recommendations to fix the problem areas. He also believes the new process must focus more on corruption issues and their impact on AML.

Question 8b. How does the United States evaluate the threats to the global economy arising from money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction?

Answer. When I was responsible for TFOS at the FBI, I was the FBI's representative on the Policy Coordinating Committee (PCC) for Terrorist Financing. All Government agencies with a nexus to money laundering and terrorist financing participated in that PCC. As an interagency group, we evaluated the threats from money laundering and terrorist financing. We collectively identified and prioritized the most significant threats. The PCC was then chaired by David Aufhauser. During

that time period (2001–2003), Mr. Aufhauser served as General Counsel at the Treasury Department. As I mentioned in my written testimony, "Mr. Aufhauser was a true leader who marshaled the interagency collaborative initiative. He was an unsung hero and visionary." My understanding is that this interagency working group is now directed by the National Security Council. The group is no longer referred to as the PCC for Terrorist Financing. I am not sure what it is currently identified as.

Question 8c. How should we be prioritizing these threats and how effectively has the FATF process been in addressing these threats?

Answer. In the United States, the threats should continue to be evaluated and prioritized by the interagency working group. Stopping the flow of funds to terrorists should be an extremely high interagency priority. Overall, the FATF evaluation process has been successful. When FATF first started there was no peer evaluation process of money laundering laws. In fact, few countries had AML laws. Since then, the FATF evaluation process has been widely accepted and followed. FATF has revised the evaluation process, which should result in an improved process.

Question 9. KPMG, a private consulting firm, released in October 2011 the findings of an anti-money laundering survey of major international banks. They found that 80% of respondents reported an increase in costs associated with anti-money laundering that averaged around 45% since 2007. The major sources of cost increases identified by the KMPG survey were: (1) Enhanced transaction monitoring, (2) increased external reporting requirements to internal regulators and external law enforcement agencies, and (3) increased anti-bribery and anti-corruption activities.

In your opinion, are there sufficient resources devoted to countering the financing of terrorism and money laundering? Alternatively, are the resource costs associated with implementing such financial regulations too burdensome on either the private or public sectors?

Answer. Overall, I do not believe sufficient resources are devoted to countering the financing of terrorism and money laundering, both in the private and public sectors. In the private sector, AML compliance is considered a cost center, as opposed to a revenue center. As such, AML compliance does not receive the support from business entities within a financial institution that should be given. The HSBC case illustrates this shortcoming. This problem was magnified during the financial crisis when banks were reducing staff. Invariably compliance staffs were cut before business staffs. The battle cry in AML compliance was "do more with less". The only winner under those circumstances is the money launderer. In the last few years, as the economy improved, AML compliance resources have improved. However, until the business entity (revenue center) versus compliance entity (cost center) mentality is dealt with, AML compliance will not be adequately resourced. As far as the Government is concerned, these are lean budget times. Consequently, staffing is impacted. In general, Government agencies responsible for investigating money laundering and terrorist financing do not have the necessary staffing. However, the Government has consistently done outstanding work in addressing the money laundering and terrorist financing crime problems.

Question 10. There has been growing concern at DHS, particularly within ICE, about the widespread use of prepaid and stored value cards as a way of smuggling illicit funds into the country which could fund terror activity. Some estimates are that $1 billion annually is moved into the country this way, with most of those funds nearly impossible to track.

Would you agree that prepaid and stored value cards are a growing danger to being able to target terrorist financiers? What steps would you recommend DHS and the Department of the Treasury take to combat this emerging trend?

Answer. The use of prepaid cards has exploded and continues to gain popularity at a rapid pace. There are many legitimate and convenient uses of prepaid cards. However, prepaid cards have been a source of vulnerability since they came on the market. Law enforcement has constantly been concerned about criminals and terrorists using prepaid cards in furtherance of their illicit activities. The problem is not just a one-way problem. Prepaid cards coming into the country to support a potential terrorist attack is a direct threat to National security and should be considered a significant problem. There is also a serious outbound problem. One area where this is extremely problematic is with the Mexican drug cartels. Prepaid cards are being purchased in the United States for shipment to Mexico with drug proceeds.

The Treasury Department, through FinCEN, established rules regarding prepaid cards in September 2011, which went into effect in March 2012. The rules, while helpful, do not solve the problem. What is needed is legislation making prepaid cards monetary instruments and subjecting them to BSA reporting requirements.

Most notably, prepaid cards should be subject to reporting requirements when individuals travel internationally.

The Treasury and Homeland Security Departments should work with the interagency community, especially the interagency working group for money laundering and terrorist financing to develop a Government-wide investigative strategy to deal with the threat posed by prepaid cards being exploited by terrorists. Likewise, the interagency community should reach out to the private sector to form strategic partnerships to address this crime problem.

Question 11a. On June 29, 2012, the Obama administration imposed sanctions on a pair of informal money-exchange networks—known as hawalas—in Afghanistan and Pakistan in what officials described as the first use of the tactic to attack the financial underpinnings of Taliban militants who rely on the system to fund their insurgency. The Treasury Department said that the designations were coordinated with similar measures adopted by the United Nations as part of a broad effort to slow the flow of cash used by the Taliban to pay salaries and purchase weapons for attacks in Afghanistan. The United Nations also added the names of the same two institutions and their principal backers to a list of groups officially associated with Taliban militancy, meaning they will be subject to international sanctions as well.

Considering how widespread their use is, how difficult is it for U.S. Government to really get a handle on some of the terror financing and money laundering activities being conducted under the hawala system?

Answer. The problem of illegal money remitters operating in the United States is one of the most significant and challenging facing the U.S. Government. This is one of the biggest challenges facing the financial services sector. Financial institutions do not know the number of their customers who use their businesses to conduct illegal money remittance operations. This is a form of hawala. The interagency working group dealing with money laundering and terrorist financing should conduct a targeted and coordinated investigative initiative on two levels to identify and dismantle illegal money remittance operations. On an international level, hawalas linked to terrorism should be identified and targeted. The Government should employee techniques to identify wire transfers to and from the United States involving these hawalas, as well as telephone numbers and emails, among other communication modes linked to the hawalas. From there, investigation should focus on the identified illegal money remitters in the United States. Coordinated take-downs of targeted hawalas in the United States and abroad should take place. This would involve coordination with our international partners. On a second level, there should be an initiative to arrest a large number of illegal money remitters in the United States for operating illegal (unlicensed and unregistered) money remittance operations. This would generate considerable media attention to this problem, be impactful and have a deterrent effect on these types of businesses.

Question 11b. How could the United States be more effective in targeting the hawala systems being used by drug traffickers to fuel the Taliban insurgency in Afghanistan and Pakistan?

Answer. DEA has had the lead in the area of drug trafficking in Afghanistan. DEA should develop investigative strategies with the Department of Defense, law enforcement, and intelligence agencies. Those strategies should be fully coordinated. The collective financial intelligence from the various agencies should provide actionable intelligence information to prioritize and target hawala dealers who support the Taliban. The key is coordination, communication, and cooperation.

Question 11c. Would closer collaboration with the United Nations help our Government's ability to identify hawala networks engaged in illegal behavior?

Answer. On a practical operational level, collaboration with the United Nations would have little impact on U.S. investigative efforts. On a policy level, especially in considering regulating hawalas, collaboration with the United Nations and other international bodies could be extremely beneficial.

Question 12. Mr. Lormel, in your written testimony you mentioned the Lloyds Bank "stripping" case as a prime example of how correspondent banking was used by Iran as a facilitation tool.

This was a pretty egregious example of Iran using the formal banking system to skirt international financial system. Do you think this was a one-off or an instance of a larger problem, particularly with regard to SWIFT?

Answer. I believe the problem of "stripping" is much larger. It is not a one-off situation. The Lloyds case was investigated jointly by the District Attorney of New York (DANY) and the Department of Justice. At the time the case was brought forward, DANY announced it was investigating nine other banks for similar "stripping" activity. On August 6, 2012, the New York State Department of Financial Services announced it was investigating Standard Charter Bank for "stripping" information related to Iran.

SWIFT is not the problem. The problem is that certain banks have chosen to do business with Iran. There is tremendous profit for the banks in dealing with Iran, especially with the strong U.S. sanctions. However, Iran needs access to U.S. dollars, therefore the banks who are dealing with Iran must transact in the United States. They must have a correspondent banking relationship with a U.S. bank to access U.S. dollars. In the cases of Lloyds and Standard Charter, the banks knew that if they provided the proper SWIFT messaging data, the identities of the Iranian banks they were transacting with would have been disclosed through their correspondent relationship with a U.S. bank. They knew full well that if that occurred the U.S. bank would have declined the transaction. The U.S. bank's OFAC monitoring system would have identified the sanctioned Iranian bank and returned the transaction. Therefore, Lloyds and Standard Charter "stripped" out any reference or mention of the Iranian bank in the transaction, circumventing the OFAC monitoring. This gave the appearance to the U.S. bank that either Lloyds or Standard Charter were the originating bank in the transaction.

Question 13a. Mr. Lormel, you suggested that providing security clearances to select personnel in financial institutions in order to share limited intelligence information that could be scrubbed against bank monitoring systems to identify transactional information associated with terrorists.

How would you envision this to work?

Answer. The Government provides security clearances to individuals working in the defense contracting industry. This enables defense contractors and consultants to work on classified projects, which is in the Government's best interest. The same should be true in the financial services industry. Financial institutions are a repository for significant financial intelligence information. If the Government could share selective classified information with a limited number of vetted and cleared bank officials that information could be run through transactional information. Hits in the transactional data, that otherwise would not have been identified, would be reported back to the agency providing the information. Legal process would have to be put in place to ensure any information provided back to the Government did not violate Bank Secrecy Act privacy provisions.

Question 13b. What would you think of sending members of Treasury's Office of Financial Intelligence, or of the intelligence community, to certain high-risk financial institutions, in essence detailing them there for this purpose? Would this not also help with the challenge of helping the financial sector to identify activity consistent with typologies of terrorists?

Answer. The idea of detailing members of the Treasury's Office of Financial Intelligence or from law enforcement is worth consideration. It would be important to distinguish law enforcement and the intelligence community in the sense that the CIA should be precluded from collecting domestic intelligence, especially involving U.S. persons. The FBI or other law enforcement agencies dealing with classified intelligence would be the appropriate Government representatives. However, before considering sending Government personnel to select high-risk institutions, a number of impediments would need to be resolved. The General Counsels from the financial institution and Government agencies would need to assess the legality and potential liabilities of such a relationship. Two other considerations would need to be considered. First, by sending personnel to select financial institutions would the Government be unwittingly providing that institution with an unfair competitive advantage? Second, does the Government have the resources to devote to this type of initiative?

While I ran TFOS at the FBI, we actually had an operation with a financial services provider, similar to what was suggested in the above question. We worked through the impediments and formed a public-private partnership that achieved extremely productive investigative results. This was a terrific model of how the financial services sector and law enforcement could form a strategic partnership in furtherance of National security. Because of the sensitivity of that initiative, I cannot comment about it any further.

QUESTIONS FROM CHAIRMAN PATRICK MEEHAN FOR SUE E. ECKERT

Question 1a. With our military successes against al-Qaeda core leadership in Afghanistan and Pakistan, there is a growing trend of al-Qaeda affiliated groups and adherents filling the void and taking the lead in launching attacks against the homeland.

Given the relatively low amount of money required to plan and launch a terrorist attack, how realistic is it to expect U.S. and international counterterrorism entities to identify funds that might be used to undertake terrorism-related activity?

Answer. Response was not received at the time of publication.

Question 1b. What are some of the persistent challenges in identifying and investigating an activity suspected of financing terrorism? What are some of the trends in how terrorist groups acquiring funds to support their objectives?

Answer. Response was not received at the time of publication.

Question 1c. Is the decision to pursue a terror financing investigation based on the amount of money suspected of being acquired for terrorism-related purposes? If so, what is the minimum monetary amount of terrorism-related funds the U.S. Government assesses as worthy of investigating?

Answer. Response was not received at the time of publication.

Question 1d. Can you describe the decision-making process and considerations by which the U.S. intelligence and law enforcement communities decide whether to stop terrorism-financing related activity and charge a suspect arrest or choose to allow the activity to continue in hopes of following the trail of funds to a larger network of support or to entities that may be planning a terrorist attack?

Answer. Response was not received at the time of publication.

Question 2. President Obama recently signed an Executive Order allowing the Treasury Department to freeze U.S.-based assets of persons who the White House has identified as a "threat to the peace, security, and stability" of Yemen.

Do you think this is an effective use of the designation authority? Especially when a group such as Boko Haram—who have killed thousands of civilians and are in constant contact with AQIM—remain undesignated?

Answer. Response was not received at the time of publication.

Question 3a. In 2011, the U.S. Government revealed the findings of a multi-year law enforcement operation to dismantle a complex, transnational network involved in money laundering and drug trafficking. The case involved Hezbollah, Mexican and Colombian drug trafficking organizations, the Taliban, Lebanon, Colombia, Panama, several countries in West Africa, U.S. car buyers, a U.S. shipping company, bulk cash couriers, plans for weapons trafficking deals, and the Beirut-based Lebanese Canadian Bank (LCB).

Does the fact that groups such as Hezbollah and the Islamic Revolutionary Guard Corps continue to use criminal ventures create opportunities for U.S. enforcement mechanisms—such as our robust counternarcotics tools—to roll up these vast networks?

Answer. Response was not received at the time of publication.

Question 3b. How does counterterrorism fit in this increasingly interconnected underworld?

Answer. Response was not received at the time of publication.

Question 4a. The U.S. Government's on-going investigation of the Lebanese Canadian Bank is of particular interest from a money laundering perspective because it highlights the consequences of poor compliance with anti-money laundering regulations in the formal financial system.

Given the Lebanese Canadian Bank case, what more can be done to protect the formal financial system from exploitation by terrorists?

Answer. Response was not received at the time of publication.

Question 4b. How can the U.S. Government more effectively mitigate the threats posed by trade-based money laundering and bulk cash smuggling and other ways outside the formal financial sector?

Answer. Response was not received at the time of publication.

Question 5. There is an increasing concern in the counterterrorism and intelligence community that terrorist organizations are increasingly using criminal activities that are outside of the formal international financial system to raise funds to carry out attacks and further their goals.

How important are terrorist funds derived from criminal activities for the operational sustainability of major terrorist groups compared to other non-criminal sources of funds, including state sponsors and private-sector donations?

Answer. Response was not received at the time of publication.

Question 6. Foreign Terrorist Organization designation by the Secretary of State is an important tool our Government uses to deter donations or contributions to and economic transactions with terrorist organizations. There are currently 50 groups listed by the State Department as designated Foreign Terrorist Organizations.

Which FTO-designated groups would you say are the best resourced and most proficient at evading American and international financial regulations? Which use the U.S. financial system the most?

Answer. Response was not received at the time of publication.

Question 7. All of the witnesses mentioned in their prepared testimony that the Government needs to interact with the financial sector to identify terrorist financing.

How should the Government develop more effective case typologies and feedback mechanisms about how terrorists use financial institutions? Is this mostly an educational issue where we need to empower financial institutions in order to monitor transactions for suspicious or anomalous behavior?

Answer. Response was not received at the time of publication.

Question 8a. The Financial Action Task Force on Money Laundering is comprised of 36 member countries and territories and two international organizations and was organized to develop and promote policies to combat money laundering and terrorist financing. The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines.

What are the areas of greatest need for improvement in the FATF surveillance process?

Answer. Response was not received at the time of publication.

Question 8b. How does the United States evaluate the threats to the global economy arising from money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction?

Answer. Response was not received at the time of publication.

Question 8c. How should we be prioritizing these threats and how effectively has the FATF process been in addressing these threats?

Answer. Response was not received at the time of publication.

Question 9. KPMG, a private consulting firm, released in October 2011 the findings of an anti-money laundering survey of major international banks. They found that 80% of respondents reported an increase in costs associated with anti-money laundering that averaged around 45% since 2007. The major sources of cost increases identified by the KMPG survey were: (1) Enhanced transaction monitoring, (2) increased external reporting requirements to internal regulators and external law enforcement agencies, and (3) increased anti-bribery and anti-corruption activities.

In your opinion, are there sufficient resources devoted to countering the financing of terrorism and money laundering? Alternatively, are the resource costs associated with implementing such financial regulations too burdensome on either the private or public sectors?

Answer. Response was not received at the time of publication.

Question 10. There has been growing concern at DHS, particularly within ICE, about the widespread use of prepaid and stored value cards as a way of smuggling illicit funds into the country which could fund terror activity. Some estimates are that $1 billion annually is moved into the country this way, with most of those funds nearly impossible to track.

Would you agree that prepaid and stored value cards are a growing danger to being able to target terrorist financiers? What steps would you recommend DHS and the Department of the Treasury take to combat this emerging trend?

Answer. Response was not received at the time of publication.

Question 11a. On June 29, 2012, the Obama administration imposed sanctions on a pair of informal money-exchange networks—known as hawalas—in Afghanistan and Pakistan in what officials described as the first use of the tactic to attack the financial underpinnings of Taliban militants who rely on the system to fund their insurgency. The Treasury Department said that the designations were coordinated with similar measures adopted by the United Nations as part of a broad effort to slow the flow of cash used by the Taliban to pay salaries and purchase weapons for attacks in Afghanistan. The United Nations also added the names of the same two institutions and their principal backers to a list of groups officially associated with Taliban militancy, meaning they will be subject to international sanctions as well.

Considering how widespread their use is, how difficult is it for U.S. Government to really get a handle on some of the terror financing and money-laundering activities being conducted under the hawala system?

Answer. Response was not received at the time of publication.

Question 11b. How could the United States be more effective in targeting the hawala systems being used by drug traffickers to fuel the Taliban insurgency in Afghanistan and Pakistan?

Answer. Response was not received at the time of publication.

Question 11c. Would closer collaboration with the United Nations help our Government's ability to identify hawala networks engaged in illegal behavior?

Answer. Response was not received at the time of publication.

QUESTIONS FROM RANKING MEMBER BRIAN HIGGINS FOR SUE E. ECKERT

Question 1. Ms. Eckert, have Government officials identified any specific indicators of terrorist financing? What are the triggers that actually "tip" law enforcement into knowing that a specific group is engaging in illegal financial schemes that are actually funding terrorism? Would there be an exhaustive list given our diverse threat?

Answer. Response was not received at the time of publication.

Question 2. Ms. Eckert, what metrics are in place to actually measure the success of the targeted sanctions and statutes put in place to prevent terrorism funding since 9/11? What do we use to measure? We cannot count the amount of lives saved, but we can assess dollar figures and convictions, but these may also be misleading? What do you suggest?

Answer. Response was not received at the time of publication.

Question 3. Ms. Eckert, earlier this year, the American Bar Association had a panel discussing the disparate impact of terrorist finance enforcement on charities and non-profits. Explain how this enforcement has a disparate impact and what if anything that you know that the Treasury and Department of Justice are doing to make sure that their terrorist financing enforcement is fair?

Answer. Response was not received at the time of publication.

Question 4. The threat to the United States has diversified greatly since 9/11. How have our terrorist financing enforcement mechanisms adequately kept up with the diverse threat?

Answer. Response was not received at the time of publication.