AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COULD AMERICA DO MORE? AN EXAMINATION OF U.S. EFFORTS TO STOP THE FINANCING OF TERROR

HEARING

BEFORE THE

TASK FORCE TO INVESTIGATE TERRORISM FINANCING

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 9, 2015

Printed for the use of the Committee on Financial Services

Serial No. 114–48

U.S. GOVERNMENT PUBLISHING OFFICE

99–727 PDF WASHINGTON : 2016

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
ROBERT HURT, Virginia
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
DAVID SCHWEIKERT, Arizona
FRANK GUINTA, New Hampshire
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
JOHN C. CARNEY, JR., Delaware
TERRI A. SEWELL, Alabama
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
PATRICK MURPHY, Florida
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

TASK FORCE TO INVESTIGATE TERRORISM FINANCING

MICHAEL G. FITZPATRICK, Pennsylvania, *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
PETER T. KING, New York
STEVE STIVERS, Ohio
DENNIS A. ROSS, Florida
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
DAVID SCHWEIKERT, Arizona
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
FRENCH HILL, Arkansas

STEPHEN F. LYNCH, Massachusetts, *Ranking Member*
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
AL GREEN, Texas
KEITH ELLISON, Minnesota
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
KYRSTEN SINEMA, Arizona

CONTENTS

	Page
Hearing held on:	
September 9, 2015	1
Appendix:	
September 9, 2015	43

WITNESSES

WEDNESDAY, SEPTEMBER 9, 2015

Larkin, Daniel, retired FBI Unit Chief, and Founder of the National Cyber Forensics and Training Alliance	9
Modell, Scott, Managing Director, the Rapidan Group	5
Rosenberg, Elizabeth, Senior Fellow and Director, Energy, Economics, and Security Program, Center for a New American Security	11
Shelley, Louise, Director, Terrorism, Transnational Crime and Corruption Center, George Mason University	7

APPENDIX

Prepared statements:	
Larkin, Daniel	44
Modell, Scott	52
Rosenberg, Elizabeth	57
Shelley, Louise	66

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

King, Hon. Peter:	
Report of the American Gaming Association entitled, "American Gaming Association Best Practices for Anti-Money Laundering Compliance," dated December 2014	80

COULD AMERICA DO MORE? AN EXAMINATION OF U.S. EFFORTS TO STOP THE FINANCING OF TERROR

Wednesday, September 9, 2015

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE TO INVESTIGATE
TERRORISM FINANCING,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 10:04 a.m., in room HVC–210, the Capitol Visitor Center, Hon. Michael Fitzpatrick [chairman of the task force] presiding.

Members present: Representatives Fitzpatrick, Pittenger, Stivers, Ross, Barr, Rothfus, Schweikert, Williams, Hill; Lynch, Sherman, Meeks, Green, Ellison, Himes, Foster, Kildee, and Sinema.

Ex officio present: Representative Waters.

Chairman FITZPATRICK. The Task Force to Investigate Terrorism Financing will come to order. The title of today's task force hearing is, "Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terror."

Without objection, the Chair is authorized to declare a recess of the task force at any time.

Also, without objection, members of the full Financial Services Committee who are not members of the task force may participate in today's hearing for the purpose of questioning the witnesses.

The Chair now recognizes himself for 3 minutes for an opening statement.

As expert witnesses in prior hearings have correctly noted, the threat of new, expansive criminal networks capable of self-funding and financing terror is a very real risk around the globe. From the Middle East to South America to the U.S. financial institutions, the threats posed by an evolving sphere of terror syndicates require a robust response both internationally and domestically. While the United States has significant tools at its disposal to degrade and inhibit terrorist financing and money laundering, it is unclear to what extent such tools have been effectively utilized.

As part of this task force's vital mission, today's hearing will examine the current state of counterterrorist financing efforts within the Federal Government to ensure that they are meeting their intended purpose and, should they not be, to identify areas which need improvement.

Furthermore, it must prepare us to evaluate the degree of cooperation between the various Federal agencies involved in coun-

tering terrorist financing and assess whether there should be more involvement between the government and the private sector to increase successful outcomes. Throughout the life of this task force, we have heard from a myriad of experienced professionals who have expressed insight from both the public and the private sectors. There have been several mentions of legislative actions Congress could take to strengthen U.S. anti-money laundering and counterterror finance measures, such as revising the Bank Secrecy Act to allow greater communication and data sharing among banks or amending beneficial ownership and control rules to ensure local and State enforcement personnel have the ability to get information pertinent to any AML/CTF investigation.

Improving the U.S. counterterrorism finance capabilities could be a simple matter of increased funding for agencies which are currently overwhelmed. Since its inception, FinCEN has taken on an increasing number of responsibilities, thanks in part to the ever-evolving field of cyber warfare, payment systems, and the inclusion of policing money services businesses. With the addition of so many responsibilities, isn't it necessary to provide additional resources to ensure effective implementation?

This is a small selection of topics I wish to discuss with our panel today. This task force has clearly sounded the alarm of the threat posed by self-financing terrorist organizations and must ensure every option is considered in the U.S. response to this danger. Today's hearing is an important part of accomplishing the mission of this group in better protecting American lives from increasingly well-funded and financed terror syndicates. I look forward to the testimony of our witnesses and the discussion between our Members.

I now recognize for an opening statement the ranking member of the task force, the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

I also want to thank Vice Chairman Pittenger for holding today's hearing. And I want to thank our distinguished witnesses for their willingness to help us with our work on this task force. I am pleased with the efforts our task force has made since it was created earlier this year. During our first congressional hearing this past April, we confronted the diversity and scope of terrorist threats which have become more varied and localized since the September 11th attacks. Our subsequent hearings have investigated outstanding challenges related to terrorist financing, including beneficial ownership, cybersecurity threats, the nexus between crime, corruption, and terrorism, and the Iran nuclear deal and the implications that may have on our antiterrorist financing efforts.

At today's fifth and final hearing in this iteration of the task force, we will examine policy proposals that aim to help improve our Nation's efforts to combat terrorist financing. Detecting and disrupting the flow of funding to terrorist groups is essential in our fight against terrorism. And we are all very aware of the threats presented by terrorist organizations, such as the Islamic State and Hezbollah in the Middle East, and Boko Haram and Al-Shabaab in Africa. Without financial resources, these organizations will not be able to fund their attacks, pay their fighters, and otherwise support

their operations. Thus, to effectively stop these groups, we must cut off their funding.

One of the ways we can do this is by supporting regional financial intelligence units (FIUs). This is why I am pleased with our witness Scott Modell's recommendations that we take full advantage of the information collected and stored by FIUs. I also agree with Mr. Modell's suggestion that we explore new ways to better analyze and use that information collected by FIUs in order to stop illicit money flows. During overseas codels, I try to make it a point to meet with regional FIUs to get updates on efforts to combat terrorist financing around the world. Witnessing the important work of FIUs around the globe demonstrates the need for the United States to continue to support international government efforts to develop robust legal, regulatory, and operational frameworks to combat terrorist financing and money laundering. It is also crucial to strengthen the relationship between FIUs, particularly with the Financial Crimes Enforcement Network, our FIU, the U.S. financial intelligence unit. This should be done in accordance with the landmark recommendations issued by the Financial Action Task Force, which is an intergovernmental body consisting of over 30 member jurisdictions dedicated to strengthening worldwide antiterrorist financing and anti-money laundering policies. I look forward to hearing from our witnesses so that we can examine these issues further. I yield back the balance of my time.

Chairman FITZPATRICK. I now recognize for an opening statement the vice chairman of the task force, the gentleman from North Carolina, Mr. Pittenger, for 2 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

And thank you, Mr. Ranking Member, for your hard work and dedication to these issues throughout the efforts of the task force. Over the past five hearings, briefings, and roundtables, we have gained important insight into the threats facing our Nation, how they are funded, and the many obstacles we face in intercepting those funds.

Just last week, the chairman, my friend, Mr. Meeks, and myself had the chance to meet with officials in Europe and the Middle East to further understand these threats and those obstacles. The theme of my discussions was Iran and the $100 billion it will receive as part of this Administration's deal. Preventing those dollars from funding terror should be a major priority. The delegation visited FATF in Paris, Turkey, Qatar, and Kuwait. We got a chance to see firsthand the challenges that they face.

While I oppose this Iran deal, it should be a diplomatic priority for this Administration to reach out to those countries and others in the region to ensure that they utilize their resources, capabilities, and incentives to fully enforce their counterterrorism finance laws within their sovereign borders. But this hearing is on the challenges we face domestically. Over these past few months, we have often heard about information sharing. And increasing the information we have and use will give us a better opportunity to stop the flow of funds to terrorists. Our hearing today will focus on exactly that, the steps we can take to better ensure that we are cutting the funding to terrorists, and protecting the security of America against our enemies.

I look forward to the testimony from the witnesses before us and the opportunity to strengthen our efforts. And I look forward to working with my colleagues on this task force in a bipartisan manner to implement the ideas before us today.

Thank you, Mr. Chairman. I yield back.

Chairman FITZPATRICK. I now recognize the gentlelady from Arizona, Ms. Sinema, for an opening statement.

Ms. SINEMA. Thank you, Chairman Fitzpatrick, and Ranking Member Lynch. The title of today's hearing is, "Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terror." The answer is clearly yes. I appreciate our witnesses' testimony and I agree that the Federal Government must change its approach and mindset to counter the financing of terrorism. My focus throughout these hearings has been on countering ISIL funding. ISIL fights locally and inspires terror internationally. But it is different from other transnational terror organizations. Its economic engagement with the outside world is limited. And it derives most of its funds from areas near or under its control.

This task force has received testimony that the internal sale of oil is a significant source of income. But it is the taxation, extortion, and theft throughout the entire supply chain that funds the organization. ISIL levies taxes and fees at every stage of production, at key roadway crossings, ports of entry, and areas under its control. It replicates this model in other markets, like banking, where it robs and then operates local bank branches, gaining money through the taxation or extortion of the population and businesses it controls. Given the closed nature of the majority of ISIL's revenue streams, how can we do more to counter ISIL's revenue sources? I look forward to hearing more from our witnesses today about how we should restructure our counterfinance operations so we have the flexibility to effectively counter ISIL's largely domestic revenue streams and fight other terrorist organizations with different funding models.

Thank you, Mr. Chairman. I yield back.

Chairman FITZPATRICK. We now welcome our witnesses.

And I recognize Mr. Rothfus of Pennsylvania for the purpose of introducing his constituent from Pennsylvania.

Mr. ROTHFUS. Thank you, Mr. Chairman. It is my pleasure to welcome and to introduce Mr. Dan Larkin from my hometown of Pittsburgh, Pennsylvania. Mr. Larkin served in the FBI for more than 24 years and established the first cyber fusion unit for the Federal Government, enabling government and law enforcement to effectively co-locate with subject matter experts from industry and academia. This unit substantially enhances resource sharing to the mutual benefit of all participants. Private sector partners include numerous financial services organizations, telecommunications, technology, and e-commerce. Law enforcement partners include a growing list of Federal, State, and local agencies, as well as international investigators from more than a dozen countries.

Mr. Larkin also developed one of the first high-tech crime task forces in the United States. This unique collaboration of assets also led to the development of the first national public-private alliance to identify and combat cybercrime. It is known as the National

Cyber Forensics and Training Alliance. Mr. Larkin also co-authored the FBI National Cybercrime Strategy in 2002.

Again, it is my pleasure to welcome Mr. Larkin here today. And I am sure that we will all benefit from his experience and expertise on these important issues.

Chairman FITZPATRICK. Welcome, Mr. Larkin.

Mr. Scott Modell is managing director at the Rapidan Group. Mr. Modell is a highly decorated former Central Intelligence Agency officer who served for 13 years in the Directorate of Operations with five tours conducting Iranian operations in Latin America, Western Europe, and the Middle East. He also participated in post-9/11 operations in Afghanistan as a member of paramilitary counterterrorism teams composed of CIA officers and local Afghan forces. Mr. Modell is fluent in Spanish, Farsi, and Portuguese, and received his master's degree from the Georgetown School of Foreign Service.

Dr. Louise Shelley is founder and director of the Terrorism Transnational Crime and Corruption Center at George Mason University. Dr. Shelley is also the Omer L. And Nancy Hirst Endowed Chair and professor at George Mason University. Dr. Shelley is a leading expert on the relationship between terrorism, organized crime, and corruption, as well as human trafficking, transnational crime, and terrorism. From 1995 until 2014, Dr. Shelley ran programs in Russia and Ukraine, with leading specialists on the problems of organized crime and corruption. Dr. Shelley holds a master's degree in criminology and a Ph.D. in sociology, both from the University of Pennsylvania. She received her undergraduate degree from Cornell University in Russian literature and penology.

Elizabeth Rosenberg is the senior fellow and director of the Energy, Economics, and Security Program at the Center for a New American Security. Ms. Rosenberg served as a senior advisor at the U.S. Department of the Treasury, where she helped to develop and implement financial and energy sanctions. She also helped to formulate anti-money laundering and counterterrorist financing policy and oversee financial regulatory enforcement activities. Ms. Rosenberg received an MA in Near Eastern Studies from New York University and a BA in politics and religion from Oberlin College.

The witnesses will now be recognized for 5 minutes each to give an oral presentation of their written testimony.

And without objection, the witnesses' written statements will be made a part of the record. Once the witnesses have finished presenting their testimony, each member of the task force will have 5 minutes within which to ask questions. On your table, there are three lights: green; yellow; and red. Yellow means you have 1 minute remaining. And red means your time is up. The microphone is sensitive, so please make sure you are speaking directly into it.

With that, Mr. Modell, you are recognized for 5 minutes.

Welcome.

STATEMENT OF SCOTT MODELL, MANAGING DIRECTOR, THE RAPIDAN GROUP

Mr. MODELL. Chairman Fitzpatrick, Ranking Member Lynch, and members of the task force, good morning. Thank you for the opportunity to testify today. Terrorism financing has become one of the most pressing national security challenges. Yet, in my opinion,

the plans, programs, and practitioners are falling short of where they need to be. My contention today is simple: many in the U.S. Government know just enough to be dangerous about finance or transnational organized crime but not enough to significantly impact crime or terror organizations.

For the past decade or so, the U.S. Government has attempted to develop a professional cadre of law enforcement agents, civilian and military intelligence officers, analysts, and others to pursue a new field of operations which has been called counter threat finance. Their purpose was to effectively counter the financial and logistical depth and sustain the capacity of our adversaries who are engaged in irregular warfare. It was thought that hitting the finances, financiers, and illicit networks would become an important means of warfare. But progress has been limited.

Looking ahead, it would serve us well to take an agency-by-agency account of what we collectively know about terrorism finance, an audit of each agency's CTF track record and current trajectory, and ways to either add or pare down their respective roles and missions as part of a whole-of-government approach. This should not seek to bring all agencies together all the time. Threat mitigation working groups or interagency task forces and the like are usually stood up with the best of intentions and may last for a while but often end with poor results.

A few of my recommendations today include the following: Number one, we need a detailed and comprehensive starting point for ourselves and for our liaison partners. We need to agree on how to better prosecute a results-dependent intelligence and law enforcement campaign, not just a series of one-off strikes, arrests, or asset recruitments. The way to begin is by building a CTF order of battle that maps key networks on a global scale, along with a tactically flexible and transnational plan of attack.

Number two, I say we need to take the gloves off. I think that intelligence collection, law enforcement actions, and even covert action must take place inside some of the worst financial havens and terrorist-enabling states such as Kuwait, Qatar, and Lebanon. Too many U.S. missions around the world maintain an ultra-cautious posture when it comes to investigations, arrests, and other operational activities inside countries where financial terrorism targets are active.

A prime example is Hezbollah. We too often avoid operations against Hezbollah's illicit financial apparatus inside Lebanon because we don't want to destabilize the Lebanese banking system or embarrass corrupt Lebanese government officials who work alongside Hezbollah.

Number three, we need to develop career professionals who better understand finance and transnational organized crime. To attack prime terror pipelines that run through the international trade and banking system, we need to have more officers who have hands-on expertise to be able to think creatively in this space in order to understand the constantly evolving illicit trade craft and sophistication employed by truly transnational organizations. This requires basic and advanced training in international finance banking and trade, of which there is not nearly enough today.

Number four, I think we need to rebuild the operational capacity of our Treasury attaches, start by taking complete after-action account of OFAC designations on key target sets, starting with Iran. If you want to put Treasury on a war footing, it needs to better understand precisely how our sanctions designations and so forth have affected banks, investment companies, exchange houses, and other financial nodes of terrorist networks, how those entities and individuals have countered, and the degrees to which they have been disrupted, dismantled, or destroyed.

Stronger Treasury force should be engaged in up-close and personal investigations of banks, hawalas, exchange houses, and others that continue to operate even after being designated. The last two things I would suggest are, one, information operations, usually reserved for the military, but it is a capability that I think could be used effectively in the CTF realm. To magnify the impact of CTF law enforcement operations, information operations should use U.S. and local media outlets to expose terrorists and their supporters, educate publics that are largely unaware of how terrorists move money through corrupt financial systems, and warn them of the consequences of abetting terrorists. Information operations can also be used to positively bolster the reputation of foreign police, intel and military efforts, or to negatively embarrass governments, companies, and individual collaborators.

Finally, I would say the Rewards for Justice Program—in my experience, money is probably the single biggest incentive to sources, facilitators, and testifiers who assist U.S. law enforcement investigations and operations or intelligence operations, for that matter. I think we need to think about how to use Rewards for Justice in a much more creative way as a tool to motivate not only individual sources, but also our foreign liaison partners. A coalition of well-intentioned states, which I think we have, that is based on a common aversion to transnational organized crime is good, but it will only go so far. I think we will have a lot more success when it is linked to potential financial reward. Thank you.

[The prepared statement of Mr. Modell can be found on page 52 of the appendix.]

Chairman FITZPATRICK. Thank you, Mr. Modell.

Dr. Shelley, you are now recognized for 5 minutes.

STATEMENT OF LOUISE SHELLEY, DIRECTOR, TERRORISM, TRANSNATIONAL CRIME AND CORRUPTION CENTER, GEORGE MASON UNIVERSITY

Ms. SHELLEY. Thank you. It is a great honor to be here and address this task force. I think we need to broaden our concept away from terrorist financing and focus on the concept of the business of terrorism. Why do I believe this? Terrorism financing looks at what has been done and is being done to fund a terrorist organization. It is reactive, rather than proactive. But terrorist groups function like multinational businesses and are always looking for future opportunities to stay in business. Therefore, the business of terrorism examines more broadly the way terrorists generate funds and solicit personnel for future activity, just as we have seen with ISIS and its sophisticated recruiting schemes. The business of terrorism looks at marketing strategies, targets of opportunity, and

other methods that they use. And terrorist financing fails to address the fact that terrorists are acting like businesspeople and need to be countered as business competitors. That is why it is very useful to partner much more with the business community, as I will be talking about.

Almost all terrorism these days is funded by crime, although much of transnational crime remains independent of terrorism. Therefore, we need to stop stovepiping the separate responses to crime and terrorism and to analyze them together and have countermeasures that work in this way. This is being done successfully by the New York and Los Angeles Police Departments, integrating local efforts with Federal efforts. And it needs to be expanded to other jurisdictions. We need to focus more on the drug trade and concentrate not only on the drug trade but concentrate on the smaller scale illicit trade that supports so much terrorism in the United States, Europe, and North Africa. One of the Kouachi brothers responsible for the Charlie Hebdo massacre in Paris traded in counterfeit Nikes and cigarettes. Similar crime is found as crucial support to terrorists by NYPD.

Terrorists use corruption to execute their business activities just as organized crime always has. Therefore, we need to integrate analyses of corruption into crime and terror analyses. Public-private partnerships are key in addressing the business of terrorism. Businesses have insights on how to combat business competitors. And these insights need to be shared with governmental personnel who have less experience with business. And I also give illustrations in my written testimony of concrete examples of successes. And I am sure we will hear more about this in the cyber area. We can hear about this in the energy sector.

And we need to collect intelligence on terrorist financing derived from diverted and counterfeit examples of commodities. But I should also add that I think we need to also be focusing on money laundering by terrorist groups into the real estate sector. We have a hole in the PATRIOT Act in reference to real estate. And I believe it is being exploited not just generally but even in the Washington, D.C. area, talking to real estate agents. So I think that this is an area that needs much more focus.

What do we need to be doing? We need to be focusing on terrorist business rather than just financing, looking at trade and products, targets of opportunity, use of technology, as we are going to hear, and recruitment of personnel. We need to establish working and advisory groups with sectors of the business community whose products are likely targets of terrorists. I know there have been good working relationships with the technology sector, but not as much with those in manufacturing goods, pharmaceuticals, cigarettes, and oil, that need to be integrated into this. As I mentioned previously, we need to be using terrorists or antiterrorist models based on LAPD and NYPD. And we need to develop more controls over crypto currencies such as bitcoin and many other emerging Web-based currencies that are hard to trace and are key to the financing and the trade of terrorists that is going on both in the real and the virtual world. Thank you.

[The prepared statement of Dr. Shelley can be found on page 66 of the appendix.]

Chairman FITZPATRICK. Thank you, Dr. Shelley.

Mr. Larkin, you are recognized for 5 minutes.

STATEMENT OF DANIEL LARKIN, RETIRED FBI UNIT CHIEF, AND FOUNDER OF THE NATIONAL CYBER FORENSICS AND TRAINING ALLIANCE

Mr. LARKIN. Good morning, Chairman Fitzpatrick, Ranking Member Lynch, and members of the task force. I appear today as a former FBI Unit Chief and the founder of the National Cyber Forensics and Training Alliance, better known as the NCFTA. Thank you for the opportunity to share some personal experiences I have had in my 24-plus years with the FBI in developing models of better cyber threat collaboration between the public and private sectors. I understand the task force is interested in functional models that might foster additional public-private partnerships to assist in the fight against international money laundering and terrorist financing. I believe the NCFTA serves as an excellent model for such collaboration.

Successful public-private collaborations are essential in combatting cyber threats. The vast majority of computer networks belong to the private sector. And, as a result, most of the intelligence on those threats resides with the private sector as well. Effective public-private collaboration also depends on trust amongst the parties, which has to be earned, as well as strong privacy protections and transparency to ensure the trust of the public.

The genesis of the successful NCFTA model actually began in the 1990s after I was reassigned from FBI headquarters to the Pittsburgh division of the FBI. In the late 1990s, it was apparent that business was rapidly moving to the Internet and, not surprisingly, so were the criminals. FBI Pittsburgh had a long history of working multiagency task forces to address a variety of criminal activity. And at this time, the idea was developed to launch a new, high-tech, cyber task force. I initially gained support of the law enforcement community for this task force and also suggested that we include representatives from the CERT Coordination Center, which was established in the 1980s at Carnegie Mellon University in Pittsburgh. Representatives from that organization at that time had become experts in cyber threats. And they were essentially in our backyard.

Ultimately, the relationship between law enforcement and the CERT Coordination Center would prove instrumental to the formation of the NCFTA. But first, we had to overcome some reluctance on the part of CERT Coordination Center members to work with the FBI and other law enforcement. This was largely due to the concerns that information shared with law enforcement regarding potential vulnerabilities might become public. To overcome these concerns, I suggested that we detail an FBI cyber agent to the CERT Coordination Center to essentially serve as a fly on the wall and to offer support for the CERT Coordination Center and their clients. This program demonstrated that the FBI could actually work with the CERT Coordination Center members and help them more fully understand the scope of the threats they are facing and that the CERT team and its clients could actually work cooperatively work with the FBI without negative consequences. This im-

mersion program also encouraged individuals to get to know each other, gain a better understanding of resources that might be shared, and to collaborate.

This environment helped to develop trusted relationships among participants and became an early principle of the NCFTA model. This early success of this immersion program led to a focus group meeting in 1988 with approximately 30 cross-sector organizations that came together to consider embedding resources in a common location in their common fight against international cyber threats. Out of this focus group, a White Paper was developed which summarized the core objectives of a new public-private alliance which eventually became the NCFTA.

These objectives include the continuation of a neutral, meet-in-the-middle environment to foster public-private collaboration, including the sharing of knowledge and expertise among public and private subject matter experts; the identification of joint initiative based primarily on a consensus view of the private sector on priority threats; use of nondisclosure agreements among parties to protect confidential and proprietary information; and training programs to help ensure common understanding of permissible private sector involvement in information sharing, as well as best practices for identifying and combatting cyber threats.

As a result of these efforts and the work of numerous individuals, the NCFTA was officially incorporated in 2002 as a 501(c)(3) nonprofit. Since that time, numerous investigative initiatives have been developed through the NCFTA with cross-sector partners spawning hundreds of investigations, both domestically and foreign. A common thread through many of these investigations has been international organized crime, money laundering, and, in some cases, ties to terrorist financing.

Today, numerous private sector organizations imbed resources at the NCFTA, alongside a growing pool of domestic and international law enforcement. Hundreds of additional subject matter experts connect to the NCFTA through various realtime communications channels.

So, what are some of the key takeaways from the NCFTA both in combatting cybercrime and considering future public-private partnerships? Significant global threats may initially manifest themselves only to the private sector. Their true significance and scope, however, may not be realized until those dots are fully connected through resources like those at the NCFTA. Cybercriminals will enlist many different and creative schemes to generate funds. And efforts to respond must also continue to evolve with the same or more advanced creativity.

The NCFTA leverages existing resources in giving them a better environment in which to perform. From this perspective, it is a very efficient workforce multiplier. Relationships are vital to making the collaboration work. And they can be fragile. Making it personal, knowing your partner's perspectives and needs is essential. And the human capital development aspects of the NCFTA are substantial. Thank you again for the opportunity to address the task force. I am pleased to respond to any questions at the appropriate time.

[The prepared statement of Mr. Larkin can be found on page 44 of the appendix.]

Chairman FITZPATRICK. Thank you.

And, finally, Ms. Rosenberg, you are recognized for 5 minutes.

STATEMENT OF ELIZABETH ROSENBERG, SENIOR FELLOW AND DIRECTOR, ENERGY, ECONOMICS, AND SECURITY PROGRAM, CENTER FOR A NEW AMERICAN SECURITY

Ms. ROSENBERG. Thank you, Chairman Fitzpatrick, Vice Chairman Pittenger, Ranking Member Lynch, and distinguished members of this task force. I appreciate the opportunity to testify before you today on U.S. efforts to stop the financing of terrorism. The proliferation of terrorist threats and the growing diffusion and autonomy of terrorists cells internationally demands a whole-of-government response. Stemming the flow of terrorist financing is critical to this effort. The most important defenses against terrorist financing are rigorous Know Your Customer (KYC) and customer due diligence (CDD) practices. With robust KYC and CDD measures, financial institutions can detect and freeze terrorist-linked financial flows and suspicious activity.

Financial policymakers, regulators, and law enforcement officials, of course, have responsibility for ensuring that requirements for such safeguards in the U.S. financial system are strong and that they are upheld. They use the suspicious activity reporting by financial institutions, often produced as a result of KYC and CDD practices along with intelligence analysis, to stem terrorist financing and activity. This may occur in the form of Treasury Department sanctions designations, legal enforcement actions against terrorists, and Defense Department targeting of terrorist threats abroad. To close a critical gap in U.S. efforts to combat terrorist financing, policymakers should advance new requirements for tougher CDD practices and disclosure of beneficial ownership information for legal entities.

The Treasury Department is working on a new CDD rule, as I am sure many of you are aware. And the 2016 Federal budget includes new requirements for beneficial ownership information gathering and sharing tied to the corporate formation process. These initiatives should be swiftly and fully advanced as crucial measures to improve sanctions enforcement and combat criminal and terrorist activity.

Additional steps that would further strengthen financial sector resiliency against terrorist financing threats include new measures to extend anti-money laundering and countering the financing of terrorism or CFT requirements to unregulated financial entities, including investment advisers and real estate agents, as was just mentioned, and, as well, to new digital currencies. Congress should take the leading role in setting new policy in these areas.

To address another serious deficiency in U.S. CFT efforts, policymakers should work to remove barriers that prevent the flow of customer and beneficial ownership data across national boundaries. Such barriers make it difficult for global financial institutions to identify and track illicit finance across the jurisdictions in which they operate. These restrictions also make it difficult for government officials to identify and target sanctions evasion or criminal

activity to connect the dots. And the restrictions also hinder efforts to identify new nodes in terrorist networks and links between terrorist groups and criminal enterprises or their criminal activities.

To be sure, sharing information related to terrorism threats presents civil liberties, competition, and financial inclusion challenges. Nevertheless, to facilitate effective law enforcement and successfully combat terrorist financing, policymakers must urgently contemplate new strategies for facilitating the flow of financial data across national borders. A good policy goal would be to significantly ease the transfer of beneficial ownership data between banks with correspondent relationships that are in different jurisdictions.

To achieve this, Treasury Department officials and financial services policy leaders in Congress should engage foreign counterparts, advocating for legislative changes, where appropriate, to allow such information sharing. They can also explore the idea of safe harbor frameworks between the United States and foreign financial jurisdictions to create mechanisms, including appropriate safeguards, for cross-border financial data flows. As terrorist threats are global, we rely significantly on the strength of foreign financial systems and the will of our foreign financial regulatory and law enforcement counterparts to combat terrorist financing. Investing in partner capacity building to combat this threat is directly beneficial to our own national interests. Congress should expand current Federal efforts to help foreign partners strengthen KYC and CDD requirements in their own jurisdictions, as well as laws that criminalize the financing of terrorism or support for terrorism. Allocating funds in the current budget to the new counterterrorism partnership fund will help advance these efforts.

Finally, as an additional measure to combat terrorist financing, legislators should set the tone for ensuring that our government aggressively exposes and targets terrorist financing with financial sanctions. This involves careful oversight of the Treasury and State Departments, which have the responsibility for implementing sanctions and, crucially, the appropriation of sufficient resources to these agencies and to the intelligence community to fulfill this important mission. Thank you for the opportunity to testify today. I look forward to answering any questions you may have for me.

[The prepared statement of Ms. Rosenberg can be found on page 57 of the appendix.]

Chairman FITZPATRICK. Thank you, Ms. Rosenberg, and I thank all of the witnesses for not just your testimony, but also for the many different roles you have played, and for your service to our Nation in protecting the safety and security of our institutions, and ultimately our citizens and our country.

I now recognize myself for 5 minutes. Each of the members of the task force will have 5 minutes to ask questions.

Each of you, in your testimony, has identified challenges or gaps in anti-money laundering and counterterror financing efforts and laws currently on the books here in the United States.

Mr. Larkin, you have identified a 501(c)(3), sort of a private effort in which you have engaged. And I just want to start by asking you to identify those gaps in policy that the NCFTA, the National Cyber Forensics and Training Alliance, seeks to address.

Mr. LARKIN. Thank you. Primarily, the NCFTA leverages, as I mentioned, existing cross-sector resources. And I think, as pointed out by Dr. Shelley and some others, the information that is out there available to us that possibly will identify early warning signs of terrorist financing or other significant activity might manifest itself in a number of different ways, across a number of different sectors. The NCFTA allows for those cross-sector groups to come together and have a more active discussion on what they are seeing that is relevant on that radar screen.

Also, the NCFTA has become sort of a unique workforce development entity. They actually bring in three cycles of grad students every year to train alongside industry and law enforcement and to become better cyber analysts for all of us to leverage. So that has become a phenomenal human capital development project. Actually, as well, it has become an unprecedented coordination deconfliction entity with domestic and international law enforcement working very actively together in this environment where they don't typically do that in other settings.

Chairman FITZPATRICK. Dr. Shelley, you testified that you believe that U.S. efforts to date have been more reactive than proactive. And you actually identified a gap that you see and you identified the PATRIOT Act in the real estate space, a loophole that is being exploited by those who want to do us harm. And I would ask each of the witnesses, if you could, to identify the gap that you think is most serious, and a legislative fix, if you have one, a suggestion that you might make, whether regulatory or legislative, I will say.

And we will start with Mr. Modell.

Mr. MODELL. Again, I think Congress needs to look very closely at covert authorities to reexamine the possibility of going beyond the military. One of the things I mentioned was looking at ways of better using resources overseas, giving Treasury and law enforcement the authority it needs to work closely with the military to actually magnify the impact of CTF operations overseas. A lot of it has to do with education overseas, awareness. And I think that the ability to operate with just relying entirely on financial intelligence units simply isn't enough.

Chairman FITZPATRICK. Mr. Modell, do you see the Treasury officials who are serving us overseas in different embassies more as representatives or diplomats or law enforcement?

Mr. MODELL. In my experience, they are much more diplomatically inclined. They are representatives. And they are not involved to the degree they need to be in rolling up their sleeves and doing day-to-day investigations. They don't have the support. They don't have the coverage. And they don't have the resources.

Chairman FITZPATRICK. Dr. Shelley?

Ms. SHELLEY. I would also add that I think we need to have more funding of research. Just as Mr. Larkin was talking about having graduate students at CERT and how helpful this is, I think to help locate some of these new areas of financing, we need analysis.

To give an example, on ISIS, working with my former graduate students, I had the identification of Captagon, which is a drug that is produced synthetically in the Middle East, and seems to be used

extensively as a funding source for terrorism, but is not cropping up in our research and analysis. So part of this is we need to have financial support and authorization in different government agencies to help fund cross-national research in this area that allows us to see things that other people are not identifying.

Chairman FITZPATRICK. Mr. Larkin?

Mr. LARKIN. One of the existing inhibitors that is still out there today is clarity on what are the safe harbor provisions. Within the financial services industry, I think there are clearer safe harbor provisions within PATRIOT Act 314(b) and obviously the SARs, safe harbor. But the reality is that the stakeholder community that actually has the information and that needs to share is much broader than financial services. So some of the early warning signs will manifest within telecommunications, and some will be in retail, merchant, e-commerce, and other areas where there is a hesitation to share information because they don't truly feel there is a clear safe harbor that protects those organizations from doing so.

Chairman FITZPATRICK. Thank you.

Ms. Rosenberg?

Ms. ROSENBERG. Thank you. I will speak to this briefly. The greatest area of concern I would highlight is the inadequacy of current laws requiring or inadequacy of laws that could require the gathering and sharing of beneficial ownership information, particularly at the company formation process. It requires a congressional fix. Regulation cannot do it alone. It is an area that was publically identified almost a decade ago by the Financial Action Task Force in which the United States has a critical deficiency. It does not lead the world in this area. And it should.

Chairman FITZPATRICK. Have you taken a look at any legislation currently pending here in Congress? There are some bills.

Ms. ROSENBERG. Yes. Particularly the language that is written into the current 2016 budget that would create the opportunity for gathering beneficial ownership information by the IRS and its sharing without a court order in the process of conducting investigations would go a long way to helping but it is not fully adequate.

Chairman FITZPATRICK. I thank the witnesses again.

And I will recognize Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

The typical way that we have been addressing anti-money laundering and counterterrorism efforts on this task force has been, and I think for our FIUs as well, partnering with central banks in other countries and setting up FIUs. I know that the members on this task force have been to Tunisia, Jordan, Morocco, obviously Afghanistan and Iraq, a bunch of countries, just trying to get them to adopt anti-money laundering legislation and then enforce that. And the idea there is to squeeze out the terrorists from using the formal financial system.

We have a different animal in ISIL. They are autonomous. A lot of the things that we normally do to shut them out are not effective because they rely on, they have rolled over a couple of Iraqi banks, a couple of Syrian financial institutions. They are using taxation in cities like Mosul and other places. They are using antiquities sales. They have a pretty active oil or at least petroleum trade program

going in terms of the Syrian and, until recently, the Turkish border. So they are generating all this revenue. And it just seems that our model that we usually use to fight this is not effective against them because they are a different situation.

Do you have any ideas about how to approach that problem? Because, obviously, the successful things we have been using against other situations where you have Al Shabaab or Hezbollah raising money sort of on the margins or on the seams of a legitimate banking system or using hawalas or hawaladars to finance small operations. Again, if you go back to what ISIL is doing, they are autonomous. And we can't seem to get at them using our usual toolbox. Do you have any ideas about how we might be more effective against them?

Mr. Modell? And I will go right down the line.

Mr. MODELL. In my brief experience in working with DOD, the answer to that question, I think, in short is this is brute force on the ground, doing the things that you just referred to. This isn't them penetrating banks in Switzerland. This requires brute force. You have to take a very close look at the DOD processes that are involved in getting the proper authorities for taking action, kinetic action, against legitimate targets in country. And I think it is too cumbersome to get to key targets in places like Syria where, again, you have a terrorist force that is exercising its will by brute force and terrorism. So, for me, it is a military authorities issue to a large degree.

Mr. LYNCH. I understand. Our problem is separating them from the population. If we just use brute force in Mosul, we are going to have a lot of folks signing up for ISIL pretty quickly because of the civilian casualties. That is the problem.

Mr. MODELL. I think there is enough information about validated targets to actually reduce the potential for collateral damage. It is just a matter, to a large degree, from what I heard, of political will to actually go forward and do things on the ground.

Mr. LYNCH. Thank you for sharing that. Thank you.

Dr. Shelley?

Ms. SHELLEY. The problem that you are describing with ISIL is in large part a problem of trade-based money laundering and fundraising. And I think there are things that can be done other than military action. For example, the Captagon trade, which is being taxed and has become a much more important revenue source according to colleagues in the Middle East, has precursor chemicals. And we could be following much more in cutting off some of the precursor chemicals that are leading to this production.

We could be working with some of the problems of corruption that have been identified in Kurdish Iraq that have helped move the oil into Iraq. We could be working more in Turkey trying to follow the initial financial flows. So there are things that business does, an analysis of what is going on in anomalies in their market that would be extremely helpful in trying to identify and target their opportunities.

Mr. LYNCH. Thank you, Dr. Shelley.

Mr. Larkin?

Mr. LARKIN. I have to say that being almost 5 years removed from the FBI, I don't have enough detail on what you are talking about to actually speak to it. So, I apologize.

Mr. LYNCH. That is fair enough, Ms. Rosenberg?

Ms. ROSENBERG. In addition to the military options that were laid out, there are a number of options I would bring to your attention in the financial services sector that can be brought to bear against this challenge. Specifically, working with the banks that have local bank branches in this area to ensure as a basic principle that this can be the area under ISIS control is a closed economy and to try and prevent money that comes in and out. Of course, the local bank branches inside the territory is one area. So creating restrictions on any wire transfers moving in and out or additional precautions on deposits made there or removed from there. Additionally, working with the local financial regulators and neighboring jurisdictions, Turkey, in particular, to ensure that where money comes into those financial institutions there from the smugglers, from the truck drivers, from anyone who is moving these counterfeit goods, stolen antiquities, illegally marketed oil, that they are stopped and the money is arrested before it can enter the formal financial system and be moved.

Additionally, looking at the cash that is couriered into ISIS territory by foreign fighters, who are asked, they are solicited by ISIL leaders to bring with them money into this territory. That is an issue for border control to arrest cash moving in, as well as for cyber financial authorities looking at the movement by wire of money into ISIS territory by these foreign fighters.

Mr. LYNCH. Thank you. I yield back.

Chairman FITZPATRICK. The vice chairman of the task force, Mr. Pittenger, is recognized for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Ms. Rosenberg, in your testimony you talked about the necessity for information sharing, those obstacles that exist. When David Cohen testified last year, when he was with Treasury, he said that we are looking to do our part to improve the sharing of information by exploring changes to the rules governing information sharing among financial institutions and between financial institutions and the government. This included the flow of information from the government to financial institutions and between financial institutions themselves. Are you aware of any changes that have been made since that time? And what changes should we make to achieve this goal that would give us an increase in information?

Ms. ROSENBERG. Thank you for the question. I believe you mean changes since Undersecretary Cohen's testimony. I am not aware of particular changes that have occurred since his testimony. Although the effort to try and expand opportunities for sharing information between government and the private sector moving in both ways presents a particular challenge, as well as you mentioned between financial institutions themselves. The option I suggested in the context of across national border information sharing contemplating safe harbor arrangements I think may pose an interesting example to explore. Creating protections or a comfort, if you will, for financial institutions to be able to bring forward potential risks

or threats without the fear of liability in such a safe harbor arrangement is critical.

One option that already exists is specific outreach by government institutions to stakeholder communities within certain financial sectors, for example, through people who have security clearances outside of the government and who are able to, in a confidential manner, discuss potential threats. Of course, there are competition, anticompetition challenges associated with that. But much more needs to be done in that area to make sure that everyone, they are common stakeholders in preventing terrorist movement, terrorist financial movement, they are able to do their job.

Mr. PITTENGER. Thank you very much. As a result of the Iran deal, there are 46 banks in Iran that will be lifted in their sanctions and be able to transmit funds through the SWIFT authority. The Administration says it will impose sanctions on these banks if they continue to transfer funds for financial terror. How can the Financial Services Committee and the Congress enforce this statement made by the Administration? And what support would you give of congressional efforts to remove the Administration's waiver authority to lift sanctions from Iranian banks?

Mr. Modell, we will start with you.

Mr. MODELL. One of the biggest things that I have been asking myself as I am looking at the Iran deal and I am looking at it play out and wondering how the implementation is going to go, assuming we get that far, is how are you going to recalibrate our own government resources overseas to figure out if they are cheating, if they are not cheating, if they are going to go back to doing what they have done for so long, which is their own whole-of-government approach? It uses the private sector. It uses charities. It uses banks. So what you are talking about is a massive problem. So for Congress to figure, to start thinking about what is it the U.S. Government can better do to figure out how Iran is going to honor its agreement or not. We need to start thinking about all of our existing relationships with financial intelligence units, all the ways in which, whether it is the FBI or the agency overseas, how they are collecting, what they are collecting on, how they are going to work with the IAEA. The reintegration of Iranian banks causes a huge problem because that illicit apparatus hasn't gone away. It was frozen. When it is unfrozen, it is going to go back to doing what it did before, to a large degree.

Mr. PITTENGER. Dr. Shelley?

Ms. SHELLEY. I don't have Mr. Modell's specialization on this. But I will add that there is another component other than foundations and their use that he enumerated, which is the problem of Iranian involvement in criminal activity, such as trafficking in women to Turkey as a way of generating funds. This has been written about and researched in Turkey. So what we are looking at is not just an overt network, but a criminal network that will be generating funds that needs to be watched of how that money moves and how it integrates with the financial system.

Mr. PITTENGER. Thank you.

Mr. Larkin, quickly?

Mr. LARKIN. I apologize, I don't have the background or expertise to answer that.

Mr. PITTENGER. All right.

Ms. Rosenberg?

Ms. ROSENBERG. Thank you, Congressman.

There are a couple of suggestions I would make. The first is to ensure that additional sanctions under E.O. 13224 for terrorism concerns are aggressively pursued against Iranian financial institutions. Successful efforts in that domain will rely on excellent new intelligence work which I think needs greater resources in order to make sure that the kind of diverse money laundering schemes associated with terrorism can be found that may come forward in the future.

In addition, the 311 action taken by Treasury's FinCEN previously could be revised and updated to highlight particular concerns related to Iran's support for terrorism and its use of financial institutions in order to give clarity and information to financial institutions in the United States and, of course, elsewhere about the particular methodologies of concern that they may anticipate seeing in the future.

Mr. PITTENGER. Thank you very much.

I yield back.

Chairman FITZPATRICK. We have been joined by the ranking member of the full Financial Services Committee, Ms. Waters, and I recognize her for questions.

Ms. WATERS. Thank you very much.

I wish we had a lot more time to talk about the agreement in Iran because it has been stated so many times that when we lift the sanctions, over $100 billion will be available to Iran. And some say that much of that would be used for terrorist activities, et cetera.

However, I think I better go to Dr. Louise Shelley. In your prepared remarks, you wrote that the New York and Los Angeles Police Departments are particularly effective at following the money connected to terrorism. And you suggest that the model they employ where resources for combatting crime and terrorism are shared could be replicated across the country. That is very impressive. And since I am from Los Angeles, I would like to get a sense of how that works. And what kind of systems do they have to track the financing of terrorism?

Ms. SHELLEY. Thank you for this very good question. In my book, "Dirty Entanglements: Corruption, Crime, and Terrorism," I provide an illustration and quite significant detail of how the joint activities between the crime and analytical branch of the police and the terrorism branch are coordinated so that literally the police are going out and doing their undercover work, undercover work on the crime. And that often leads to hints of terrorist activity. And then they have regular meetings where they integrate their observations and their insights from their informants with Federal law enforcement.

So, in this remarkable case, they found a linkage between a Chechen funding cell that was working with an Armenian organized crime group through a front charity that was shipping hundreds of cars out of Los Angeles to raise money that were going back to support Chechens in the attack in Beslan that killed hundreds of children and family members. And recently we had a joint

French-American meeting, which we called Track 1½ Diplomacy, and we had a presenter from LAPD present to this group because the French have had so many tragedies lately by not having this integrated analysis. And they thought this was one of the best lessons learned and hoped to bring this over to inform the French government soon.

Ms. WATERS. So given that information and that fine example that you just shared with us, can you see any possibility of Federal legislation that would incentivize or inspire police departments across the country to develop those kind of integrated systems where they would have those working on crime talking with those working on terrorism, sharing that information, and making it work to be able to identify money laundering and terrorism, et cetera? Do you have any thoughts about possible legislation that could help?

Ms. SHELLEY. I think that is your bailiwick is to come up with the legislation. But that is exactly why I wanted to bring it to your attention so that there would be efforts made in this. Thank you.

Ms. WATERS. We better start thinking about that. Thank you very much.

I yield back the balance of my time.

Chairman FITZPATRICK. The gentleman from Pennsylvania, Mr. Rothfus, is recognized for 5 minutes.

Mr. ROTHFUS. Thank you, Mr. Chairman.

Mr. Larkin, I would like to talk a little bit with you. CyFin, one of the National Cyber Forensics and Training Alliances' initiative-based models, is dedicated to identifying, mitigating, and neutralizing cyber threats targeted at the financial services industry. As I understand it, the initiative has grown to include more than 75 members and played a key role in developing and advancing significant investigations by domestic and international law enforcement agencies. This has resulted in millions of dollars in compromised accounts that had been secured before financial losses could occur. CyFin and the NCFTA generally seem to be great examples of private-public partnerships and the benefits of information sharing. Do you know whether these instructions are being replicated anywhere?

Mr. LARKIN. That is being considered. I know that the FBI and other agencies are considering how this model is working today and whether or not it can be replicated in other regions. But one of the prime considerations in doing that is to ensure that it is a complimentary project and not something that is viewed as competing.

Mr. ROTHFUS. Would there be anything that would inhibit the development of such other organizations?

Mr. LARKIN. Not that I am aware of. I think it is just attending to the fundamental premises that the NCFTA holds and to make sure that, again, those succeeding models are set up in a way that they are complementary and coordinated with the current one.

Mr. ROTHFUS. Mr. Modell, you mentioned in your testimony that there should be greater oversight of correspondent banking between financial institutions and foreign entities. I agree that correspondent accounts present a great challenge. And I would be interested to hear whether you have any specific recommendations on

policy changes to address this issue or suggestions on how this greater oversight might be structured.

Mr. MODELL. We did a number of things with DEA and a couple of other government agencies looking at the way that Hezbollah runs transnational organized crime, particularly trade-based money laundering. And we were looking at the ways that they were working with the Iranians running money through correspondent accounts through the United States. We were looking at it from a very operational perspective, correspondent baking accounts emerged as a clear target set that we need to do more against. From a legislative perspective, I have to apologize, I don't have any recommendations specific for you.

Ms. ROSENBERG. Congressman, could I speak to that?

Mr. ROTHFUS. Yes.

Ms. ROSENBERG. Thank you. From my perspective, the best way that financial institutions that maintain correspondent banking accounts with each other have to make sure that the money flowing through customer accounts, wire transfers, what have you, is safe and legitimate money is to make sure that they can properly exchange information about the client, including beneficial ownership information. National level restrictions that prevent the flow of that information make it such that that information cannot always be shared, even within the same financial institution that crosses a national boundary, which can mean that it is possible for the financial institution and the financial system broadly to be abused. So the ability for financial institutions to make their decisions about which correspondent banking relationships to maintain is significantly affected and will be supported if that information can be shared across national boundaries.

Mr. ROTHFUS. Thank you.

If I could just pop back to Mr. Modell for a second. You suggest that informational operations campaigns should be used to educate the public on how terrorist organizations move their illicit money and to embarrass foreign governments, businesses, and individuals in an effort to keep them out of corrupt financial systems. You suggest that this is particularly appropriate for Iran. And as we consider the Iran deal, we know that part of the deal, as Congressman Pittenger reminded us, is that many Iranian banks, companies, and individuals will be delisted for purposes of both U.S. and international sanctions. Some have suggested that this delisting brings new legitimacy to these entities, even if they are part of the Islamic revolutionary guard corps. With that in mind, how harmful do you think the nuclear agreement will be to this effort of keeping people out of the corrupt Iranian financial system?

Mr. MODELL. I think that—one of the biggest oversights of the agreement is exactly that. If we are going to go forward and try to figure out how to build a compliance and verification mechanism on Iran's nuclear program, in other words, are they going to live by the fundamental tenets of the agreement, how are we not all on the same page with regard to illicit procurement or their re-entering into the banking system? To answer your question, I think when you are going to bring back IRGC-related entities, when you are going to bring back banks online, you are doing a real disservice to the international financial systems. So when you are

talking about information operations and their ability to actually deal with this gap in the Iran deal, it is about exposing things that need to be exposed.

Mr. ROTHFUS. Would businesses in Europe, China, and Russia—really, are they going to be shamed out of entering the Iranian marketplace?

Mr. MODELL. In my opinion, I think people underestimate the degree to which the European businesses see the risk in returning to Iran, particularly if the United States is going to maintain a hardline approach. I think some will not be deterred. I think when you talk about China, for instance, and certain partners that are already ready to engage or have been engaging despite sanctions, like the Chinese and the North Koreans, there are going to be certain business environments that aren't going to be affected whatsoever. And information operations in those environments wouldn't work because we wouldn't have the local support of local media outlets and partners in any case.

Chairman FITZPATRICK. The gentleman's time has expired.

The Chair now recognizes the gentleman from New York, Mr. Meeks, for 5 minutes.

Mr. MEEKS. Thank you, Mr. Chairman.

Let me first thank you, Mr. Chairman, for leading a great trip where we did a lot of investigations in talking to individuals, whether it was from France, Turkey, Qatar, or Kuwait. And I know we tried to get into Lebanon, but unfortunately, we couldn't get in there. But we had a good conversation with its prime minister. So I very much appreciate the trip and I gained a lot of knowledge on the travel talking about this very subject matter. I want to first thank you for that. It was very good.

And given that, because one of the things that seemed clear to me on this trip is that the group that is a threat to everybody, whether it is the United States, whether it is Israel, whether it is even Iran and Russia and France, is this group called ISIL or Daesh. And everybody seems to be very much concerned about how they were being funded and how the dollars would go through.

So, to that, let me ask, first, Mr. Modell, because I believe in your writing, you discussed how intelligence collection for law enforcement and covert action needs to take place within countries that, using your words, are the most financial safe havens and terrorism enablers. Now, I was really taken aback to some degree when we were in Kuwait and Qatar, particularly, because they seemed to be very forward with what they were trying to do and what they could not do, or had not been done. A lot of that had to deal with some of the cultural questions, like a lot of people utilize cash as opposed to credit cards or anything else. Cash is harder to trace, et cetera, and a lot of them were making new laws with regards to the charity law because money was being funneled through that. But there also seem to be some concerns culturally, because culturally they bank differently than, say, Westerners have, different things, and that nature.

So my question to you is, how would such actions take place in these areas where they have the potential of destabilizing? When I talk about the Kuwait, for example, the June 26th date, for the first time, they had their own bombing at a mosque. They seem to

be very focused on doing what they need to do to try to be very helpful here, but at the same time, they said, we have to move things to give confidence to our people. So how do you balance, what do you see the balance of the two, so that we could make sure we don't destabilize other regions of the area as we try to make sure we prevent them from passing dollars through?

Mr. MODELL. Yes, thanks for your question. I think it goes down to the fundamental issue of liaison relationships. You have to have more people who are constantly engaging with the Qataris, and the Kuwaitis, and saying: Listen, we have priorities. We realize you can't subvert your entire banking system because it is totally corrupt with terrorist financiers. But there have to be priorities. There has to be more action.

In the case of Qatar, there are serious Al Qaeda and ISIS financiers sitting in Doha, and they know it. So it is not a cultural issue. It is not an unawareness issue. It is that they have their own motivations for doing what they do. And they have their red lines. For us to strike the right balance between understanding where their red lines and limitations are and our need to actually stop the flow of money into Syria and Iraq, that is why I am calling for a different type of engagement overseas.

If you have Treasury people who are covering four, five, or six different countries or FBI or agency people who don't have the adequate amount of resources to actually engage in a fulsome way with financial intelligence units, with the police, with the military, with law enforcement, and incentivize them and really develop a systematic way of creating a culture there, a liaison relationship culture, where they natural incentives—and I talked about some of the things that we can offer them to do that—you are not going to get any changes.

I will give you an example. The DEA has told me very frequently in certain places in the Gulf, when they approach the financial intelligence units or when they approach their police counterparts or their counterdrug counterparts, they get nowhere. They get the requests delivered and they say, we will get back to you, and they don't get back to you. So if it is financial issues, there are the blank stares. If it happens to be really serious narcotic issues, they will. Again, I think it is a matter of political pressure combined with changing the culture and changing the incentives on the ground, and that starts at liaison relationships overseas.

Mr. MEEKS. Let me try to get one question in with the time I have remaining to Mr. Larkin. Because, Mr. Larkin, you talk about in your remarks cybersecurity landscape, law enforcement, needs private industry's help more than the reverse. So, given this, what types of incentives exist that we might give and how might they be improved to ensure that government has the appropriate level of access to actual threat information, and how do we protect, utilize public-partnerships? How should they be structured so that we can also have privacy and promote transparency?

Mr. LARKIN. Thank you for the question. I think the model that the NCFTA presents is one that has been given a lot of thought in setting up the policies and procedures for how information is shared and how those relationships are developed. I think, as I mentioned earlier, the incentives, or I guess the confusion around

how information can and should be shared and when largely comes from a misunderstanding on what the safe harbors are, what the appropriate sharing of information can be. I think the FBI and other agencies have gotten better about sharing information back with industry, and I think they have learned over the years that there are a lot of good things that come from that; when you arm industry with more specifics about what the threat looks like from your side, they can actually go find more information and bring it to you in a more timely and more effective manner.

Chairman FITZPATRICK. The gentleman's time has expired.

I recognize the gentleman from Florida, Mr. Ross, for 5 minutes.

Mr. ROSS. Thank you, Mr. Chairman. Mr. Chairman, it is my understanding that this is the last meeting of this task force. Is that correct?

Chairman FITZPATRICK. I'm sorry?

Mr. ROSS. It is my understanding this is the last meeting of this task force?

Chairman FITZPATRICK. Yes, it is.

Mr. ROSS. And that is a shame, because I think the task force with you, Mr. Chairman, and with the ranking member has done a very diligent job objectively identifying some of the greatest threats that we see today in terrorism financing. And I would implore Chairman Hensarling to do more to keep this task force going.

Because what we have learned, I think, in the brief period this task force has been around is undisputed that Iran is the largest state sponsor of terrorism. And despite ongoing sanctions, they continue to finance terrorism activity throughout the world, that they are led by extremist clerics, who are committed to the destruction of Israel and Iran, and that if this Iranian deal goes through, the relief of at least $100 billion in sanctions would flow more money to terrorist groups throughout the world and make this world even less safe.

Ms. Rosenberg, you speak of allowing for other opportunities, if you will, when we are in an engagement of usual and customary financial transactions through the infrastructure of the financial services arena, for example, continued stronger anti-money laundering, increased sanctions. Those sound good. How do we go about implementing that? In other words, we are about ready to probably see the release of sanctions against what has been deemed to be the central bank of terrorism, Iran, and yet, we know that we have to do something so long as they are within the infrastructure, if you will, of financial services, and those would include further sanctions. What would you propose?

Ms. ROSENBERG. Thank you for the question. In order to counter the threat that Iran poses to our financial system and, indeed, to our national interests as the state sponsor of terror, there are a number of things that we can do from a policy and regulatory perspective to address this. One is the modification of the 311 on Iran, as I mentioned previously. Additionally, I would suggest doubling down on sanctions targeting the IRGC and its links to terrorism. So though many sanctions including all the most significant economically punishing ones on Iran will be lifted on implementation day under this deal, assuming that takes place, sanctions on IRGC

and those that are imposed under terrorism theories are not going to be lifted, and secondary penalties would still be associated with them.

Mr. ROSS. And that has proven to be very effective too, the lifting of sanctions.

Ms. ROSENBERG. Yes. I agree. It seems that way to me, at a minimum, from the perspective of identifying, naming, and shaming entities associated with that and arresting their ability to use the financial system.

Mr. ROSS. Thank you. I appreciate that.

Mr. Modell, quickly, I know—and I will have you address that as well. But I think you had a point that I think is very important that we have to realize. And for those terrorist organizations out there that avail themselves of what we consider to be terrorist, traditional terrorist means, which don't use the infrastructure of the financial services arena, brute force is an element, and is it not an element that we have to consider as one of the tools if we are going to successfully combat the financing of terrorism throughout this world?

Mr. MODELL. Yes. Unfortunately, in a place like Syria, based on the stories that I have heard, trying to compel truck drivers to abide by the laws, try to create greater border security, all of those things I think would eventually have to happen, and we have to focus on that in the next phase. I think now, unfortunately, there has to be smart, designated, kinetic activity, at least setting ourselves up to do that.

Mr. ROSS. I agree. And I think we have to realize that as an essential tool in our tool box in order to combat this. Really quickly, yesterday, 15 governors, one of which is my governor from the great State of Florida, sent a letter to the President essentially saying that the Iranian deal highlights concerns that lifting Federal sanctions would only result in Iran having more money available to fund terrorism. They quote the Acting Under Secretary of the Treasury for Terrorism and Financial Crimes as saying that he expects to continue to see Iran funding Hezbollah and its other violent terrorist proxies.

The States do have sanctions. These States do have sanctions against Iran. They don't want to be forced into it because this has been deemed not to be a treaty, and therefore, State law preempts right here, and they are not required to lift for their sanctions.

My concern is that if these 15 States don't lift their sanctions, which I support them not doing, are we going to see Iran then look at this deal and say, U.S., you have breached—you are in violation of this deal, because you haven't lifted all sanctions? Is that a viable consequence, which then could lead to Iran saying, "Look, you breached the deal, U.S., all bets are off. It doesn't matter what you have done with the sanctions, because you have lifted them, but we are going to go forward with what you want to do?"

Mr. Modell, I will start with you.

Mr. MODELL. There are two things I would consider. I think the number one goal of the Iranians in the removal of lifting sanctions and pressure and the normalization of the nuclear program was to restore normal trade relations with Asia and Europe. America would be a bonus potentially down the road. But if U.S. States

start causing problems, keep sanctions on, start changing the fabric of the deal to some degree, or at least the spirit of the deal, I don't think it will have an impact, to be honest with you.

But let me just go back really quickly to what you were saying before. I think one of the things that we can do as Iran comes back into the financial system is expose the fact that they don't have a financial intelligence unit. They don't report suspicious transactions. They don't abide by FATF regulations. They are large state-run terrible foundations, which control billions and millions of dollars, unreportable to any authority whatsoever. And they have long been linked to terrorism. So an exposure of that in the media, in a positive media campaign for education, transparency would go a long way.

Mr. ROSS. Thank you.

And I see my time has expired, Mr. Chairman. Thank you.

Chairman FITZPATRICK. The Chair now recognizes the gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman. I would echo the commentary made by my colleague with reference to the benefits that we have derived from these various hearings, and I salute you and my ranking member for the way you have worked together to help facilitate the free flow of information. Thank you very much.

With reference to information sharing, there are arguments made with reference to technology being a problem, and then there are other arguments that are made with reference to organizational inertia, infrastructure, and culture.

How much of the fusion of information between various agencies is impeded by culture, organizational inertia, and structure within the various entities that should be conversing with each other?

Ms. Shelley, you ventured into this a little bit earlier. Would you care to respond?

Ms. SHELLEY. Yes. I would be happy to.

I see that in many areas, what I would call emerging areas of terrorist financing such as wildlife, our research is showing that the trade in this is going through key facilitators, some of whom are linked to terrorist organizations.

But we have such a segmentation of the way we are looking at drug issues, illicit wildlife trade, trafficking in animals, movement of money, that we are not coordinating and seeing that the same networks are doing them. And then, we are are not targeting the individuals who are doing this properly in terms of denying them visas to the United States, denying them access to American financial institutions and, particularly, American real estate.

And so we are much better with looking at banks and looking at financial institutions, but many of the areas of trade that intersect with this have links to the United States, and our institutions are not working together to help cut this off.

Mr. GREEN. How much of that, if you can in some way quantify it, is related to technology, the inability to automate a system that will allow this type of information to flow between entities? How much of it is related to the technology versus the culture within the various organizations?

Do we have organizations that have somehow structured themselves such that it is very difficult for them to pass information on even when there is a desire to do so?

Ms. SHELLEY. I am not sure that it is necessarily a failure to pass information. I think it is a failure to have adequate coordination among different branches of the U.S. Government that never thought that they were dealing with the same crime and terrorist networks so that you do not have the enforcement arm of Fish and Wildlife working in the past with DEA, working with the Defense Department.

And so it is not so much a problem in this case that I have given you of lack of information—of technology, but of absence of coordination within our structures.

And as the point has been—and I have tried to make is that we also have linked it between this trade-based money laundering that is funding terrorism and our own economy. And we are also not making those connections either.

Mr. LARKIN. If I can speak to that?

Mr. GREEN. Yes, sir.

Mr. LARKIN. I can say from my experience it is largely cultural. And I can say from what we have witnessed in developing the NCFTA and getting the agencies to come together that previously hadn't and a lot of cross-sector organizations to, it has never been a technology challenge. It has been a cultural mindset challenge. It has been a lack of incentive to come together as opposed to just saying, what is the right thing to do? So I think that is getting better than it used to be, but I don't think technology been a significant issue in that regard.

Mr. GREEN. I see one additional person—Mr. Modell, you are nodding. Do you have something you would like to say?

Mr. MODELL. I would just say, one of the things that Dr. Shelley mentioned before is the Captagon issue. Captagon is a drug used widely throughout the Middle East. And when you look at the U.S. Government's approach to going after a group like Hezbollah, right, one of our leading terrorist challenges, I agree with Mr. Larkin, it is a real bureaucratic problem. The intelligence community sees Hezbollah as not very involved in drug trafficking. They see them as a terrorist organization, and our main objective is to stop terrorist attacks. And I don't disagree with that, but when you look at the extent to which a group like Hezbollah is a global transit national organized criminal network, right, and the disagreement among U.S. Government agencies as to that truth, that reality and how to approach it, you are going to run into some real problems, real limitations. And so for me I would just like to emphasize, it is really is a bureaucratic issue. We are not all on the same page with regard to tackling these issues.

Mr. GREEN. I have exceeded my time.

Thank you, Mr. Chairman. I yield back.

Chairman FITZPATRICK. The gentleman from Arkansas, Mr. Hill, is recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman.

And thank you, Mr. Ranking Member, for your excellent stewardship of this task force.

Dr. Shelley, I would like to begin with you and talk a little bit about this real estate exception to the money laundering statutes that you have referenced. Presuming a buyer has a bank and withdraws money from that bank, and presuming a seller has a bank and deposits the proceeds into that bank, describe kind of more specifically the gap that you have identified that is being exploited. And you even referenced right here in the booming real estate market of the beltway. So could you go into a little bit more detail about that?

Ms. SHELLEY. I would be delighted to.

What you can do to move this money is that you can set up a company, and then you have the money moved from overseas into the front company that is going to buy the real estate for you. And then you buy this piece of real estate that is quite expensive. I believe this happened in the house next to me. And nobody ever commented on this buyer. He was buying massive amounts of real estate in Washington, and nobody had to report this. It was a person of, I want to say, but from the Middle East, whom if you did a search on Google, you would find him linked to many charities that are marked by our law enforcement community and intelligence community.

And so you could move this money through a front company very easily. I have had real estate agents telling me the things that are going on in Georgetown where money has moved out of Yemen and some of the purchasers are even dead people who have been buying property. I brought this to the attention of people in Treasury, and no one ever went and followed up with these real estate agents to find out what these anomalies were in our financial markets.

Mr. HILL. So do you think that a solution would be that REALTORS® would be subject to filing a SAR? Is that the direction you would take?

Ms. SHELLEY. That is absolutely an essential part of it. And I think we have to tighten up the requirements on the real estate community. We have to have seminars. We have to have much more responsibility because from what I have been observing, it seems to be a central target. Just as we are having many corrupt officials, many transnational criminals moving money into real estate, a piece of this seems to be supporting terrorist groups as well.

Mr. HILL. And in my example, you are just suggesting they are not caught on the depository end of either one of those transactions is your presumption?

Ms. SHELLEY. Exactly.

Mr. HILL. So that leads me, Ms. Rosenberg, to the issue of beneficial ownership. Obviously, the IRS captures everybody who is involved as a director in a Form 990 in the nonprofit sector, and they have an elaborate disclosure capability that is online and publicly available. And for all passthrough companies, like Dr. Shelley is talking about, Subchapter S or an LLC, which is the most common form of real estate "shell company" process, the IRS has all that beneficial information and that you file, obviously, a K-1 to one of those beneficial owners every year on that real estate.

So my question to you is, what is it that we are not doing? We have the information at the IRS, and if there is a criminal inves-

tigation, you are not suggesting that the IRS doesn't turn that over to a U.S. Attorney or an FBI agent, are you? Or are you?

Ms. ROSENBERG. I think you can with a court order, the challenge is making that information more easily accessible and movable to various authorities in a position to investigate and pursue appropriate legal action or who are in a position of needing to understand the methodologies in order to create better policy to prevent threats in the—from terrorist threats and others from accessing and using the financial system. Additionally, that is at the IRS level, and this doesn't extend to the creation of legal entities at the State level, where it would be quite useful to gather additional beneficial ownership information from legal entities when they are formed and verifying that information over time.

Mr. HILL. Wouldn't you suggest, though, that the burden shouldn't be there on a commercial bank but ought to be on the secretaries of States and on the update requirements for beneficial ownership change at the State level and which would be rarely automated, I would assume, in all 50 States? So we haven't heard a lot of discussion about the responsibility of individual secretaries of State at the state level for incorporation standards. What should the—what role does the Federal Congress have on that?

Ms. ROSENBERG. Partly because of the burden it would place collecting and verifying this information on the States and putting it at the Secretary of State level and others, there is not a great level of interest by the States in pursuing new laws and policies in this domain, which is one of the reasons why it was incumbent upon Congress to create national-level policy in this area. I don't want to diminish the significance and the burden that this will be on the Sates, but as has been testified by my colleagues from the panel and by other witnesses in your prior hearings, the nature of the threat that is posed by abuse of our financial system by terrorists and entities involved in corrupt activities is commensurate with the burden that it would be on our financial system and on the Sates in order to make this a reality.

Mr. HILL. I thank the panel.

And I yield back, Mr. Chairman. Thank you.

Chairman FITZPATRICK. The Chair will now recognize the gentleman from Texas, Mr. Williams, for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman. I, too, would like to thank you and the ranking member for your leadership on this committee.

Over the last few months, this task force has explored an array of topics and received in-depth testimony from witnesses throughout the government and the private sector that has helped members of this task force better understand the challenges we face in dealing with terrorism financing. These challenges are real for me personally—sometimes hit too close to home—because I am a car dealer. Now, I want to start by discussing the topic of money laundering with the witnesses today. We talked a lot about that today, especially the laundering that exists here in the United States. From some of your previous testimony and also earlier when we had other folks here, we heard about legitimate businesses knowingly or unknowingly supporting terrorist organizations who launder money right here in our own backyard.

My first question to you, Ms. Rosenberg, is, in your view, what are the key terrorist financing money laundering threats facing the U.S. international financial systems to date? You have talked a little bit about that. Could you repeat it?

Ms. ROSENBERG. The key threats, maybe I could take this by offering you my views on the key vulnerable abilities by which these threats can enter and abuse our financial system. So I mentioned the hole that exists in the gathering and the sharing of beneficial ownership information, as well as information sharing, not just to highlight one particular challenge that exists across national boundaries. But the challenge of sharing information and, indeed, aligning expectation between independent regulators and overseers within our own financial system is a challenge. And by that, I mean the challenge in coordinating law enforcement financial supervisory authorities and policymakers in their various expectations and about what best practices are and what kind of activity should be pursued with law enforcement activity.

Mr. WILLIAMS. "Sharing" is a big word here, isn't it?

Now, also, the private sector has a role in this in working in conjunction with the Federal authorities to stop some of the money laundering schemes from existing. I bring this up because there are legitimate businesses trying to sell a product. For example, we have heard testimony about terrorist groups in the United States using the car market to launder hundreds of millions of dollars. We even heard a figure of a billion dollars going back and forth. As I said, I am a small business owner. I am a car dealer. And when I heard this, it amazed me. And I know how this works, but, Mr. Modell, what would you—could you focus a little bit on this relationship with the car industry and all this money going back and forth and what you think we need to focus on and who we need to talk to?

Mr. MODELL. I follow the Lebanese use of this. The used cars that are purchased here and sent to West Africa—I think previous testifiers have discussed that. In my discussions with the DEA and the FBI and others who have been involved in pursuing that, they have expressed some degree of frustration that, first of all, nothing is done in West Africa whatsoever. So you have massive West African car lots that are sitting there with cars piling up. The purpose was just to bring them to transfer drugs or to launder money en route to Europe or other areas in the Middle East. These are global things that we don't have enough cooperation with our partners overseas. So starting with overseas nodes of cooperation, that has to improve.

Here in the United States, I think when you go to Detroit and other places where there are car dealers who have been implicated in this, I don't think we have been punitive enough. I think they are still in business. They haven't been put out of business. So I think tougher measures have to be put at hand to actually stop this type of activity. And my sense is that is not happening.

Mr. WILLIAMS. We need to talk to the auctions, don't we? And we also need to find a track to the banks. Because I know how people buy cars through an auction.

Ms. SHELLEY. Yes.

Mr. WILLIAMS. And it is a legitimate concern and one you would agree we need to address further, another reason I hope we continue our task force because this is something that really concerns me.

One more: According to assessments, some $300 million worth of criminal proceeds are laundered through the U.S. financial system each year, probably more, I think we would agree. How significant is this number relative to the amount of such funds laundered worldwide? Dr. Shelley?

Ms. SHELLEY. I think that the laundering of money is significant, and I wanted to add that there has been money traced through from the car industry, the used car industry, into our financial system, and this is a very significant amount of money, probably estimated at least $100 million and probably a multiple of that linked to just that element of terrorist financing. So we have a lot more that we could be doing looking at this trade-based money laundering and how it turns up in our financial system.

Mr. LARKIN. Can I make a quick comment, too? Actually, one of the initiatives that I mentioned as developed out of the NCFTA with significant input from the industry, one of those initiatives is an international auto auction and sale and fraud initiative that has been going on for quite a number of years with significant international organized crime and money laundering. It is a great example of how law enforcement and industry can come together to better identify how these threats look at the earliest stages and empower industry with more constructive knowledge about what money is going through their hands that is bad money.

Mr. WILLIAMS. We will visit some more. Thank you for your testimony.

I yield back.

Chairman FITZPATRICK. The gentleman from California, Mr. Sherman, is recognized for 5 minutes.

Mr. SHERMAN. Thank you.

Certainly, one source of terrorism is Iran. We are entering into this deal in which we are supposed to waive the sanctions that were enacted to deal with their nuclear program. But in doing so, we are going to be waiving the sanctions that were designed to discourage them from engaging in terrorism.

The most specific example of this is the Iran Sanctions Act, which in its terms, which Congress declared we had three major reasons, only one of which was weapons of mass destruction, and weapons of mass destruction includes nuclear missile and biological and chemical concerns. I will strike "missile" from that because the structure was the weapons, not the delivery systems. But still, nuclear was one-third of one-third of Congress' announced reason for adopting the Iran Sanctions Act. Under this deal, it is going to be waived.

What I am concerned with is especially designated nationals list, which is the no-go list for international finance. And you have a lot of countries that are on the list because of their involvement in nuclear activities that we never bothered to put on the list because of their involvement in terrorist activities, for example, Bank Melli, which has been involved with Palestinian Islamic jihad, Hezbollah, Quds force, et cetera.

Dr. Shelley, are you confident that the United States will put Bank Melli on the terrorist list, or are we going to ignore their support for terrorism in the future because they used to be involved in proliferation activities?

Ms. SHELLEY. I think that is a great question. I think we have to do a lot of very careful analysis and make sure that we are not throwing the baby out with the bath water. And so—

Mr. SHERMAN. I want to assure you, Bank Melli is the stinkiest bath water out there. This is not a beautiful baby.

But I want to go on to something else, and that is, the real benefits to remittances. They go to the poorest people in the world. They do more for development than our whole foreign aid program.

What can we do to make sure that people who want to send 400 bucks a week are able to do so at reasonable cost without—I mean, yes, it is possible, ISIS could get—such small amounts of money could benefit a terrorist organization. But, frankly, I don't think we can prevent ISIS from getting its hands on 400 bucks here, 400 bucks there.

Are we going—I will go back to baby and bath water. The baby is legitimate remittances. Are we doing too much to restrict remittances to families in Somalia, Iraq, and other places? Dr. Shelley?

Ms. SHELLEY. In the past, we have done some superb—Treasury has done some superb analysis on when remittances are not being used for their intended purposes. That is that people are generating too many remittances based on their income, which leads to a geographic targeting order. And that is why I put this emphasis on research and analysis in that if a few individuals are sending $400 a month, that should not be restricted. But if you are finding that there are nodes that are being abused where people are sending much, much more and that can be identified, then you have a problem, but it is not that hard to identify.

Mr. SHERMAN. TSA has a trusted traveler program. Should we have a system here in the United States where you can fill out a form to the government, "here is who I am, here is how much I make, I plan to send roughly this amount, depending upon circumstances, to my relatives in such and such a country," and be certified as trustworthy when you lay out a plan that make sense?

Ms. SHELLEY. I am not as concerned about the individuals being trustworthy, but much of what goes on behind illicit finance are facilitators. And so we need to be focusing on the facilitators, and when we see that they are being abused and go after them rather than the small fry who are sending their money.

Mr. SHERMAN. And I would add, I think it was Mr. Modell talking about being tough enough, the Iraqi Government that we support with blood and treasure, is paying people in Mosul because they were on the civil servant list. And as far as we know is providing free electricity for which ISIS is free to collect a bill. So we have to start treating this economics element seriously.

And I yield back.

Chairman FITZPATRICK. The gentleman from Kentucky, Mr. Barr, is recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman, and Chairman Fitzpatrick, Vice Chairman Pittenger, and Ranking Member Lynch. I also want to join my colleagues in complimenting you all for your leadership

in convening this task force and giving the testimony that we have heard here today and the other hearings before this task force. We obviously have many gaps and deficiencies in the way in which our country counters terrorism financing. And I look forward to working with each of you in developing perhaps a legislative package that adopts some of the recommendations made here today and in—from the other witnesses we have heard from in other hearings.

With respect to the proposed Iran nuclear deal, the joint comprehensive plan of action, I wanted to ask Mr. Modell a question about the impact that a finalized deal would have on the existing deficiencies that you testified about. In particular, you testified that terrorism finance has become one of our most pressing national security challenges, yet the plans, programs, and practitioners are falling far short of where they need to be. My question to you, Mr. Modell, is will we fall further behind if this deal is finalized? And, secondly, is there a way to quantify how much further behind will we be if this deal is finalized?

In other words, how much additional pressure will this place on the efforts to counter the financing of terrorism?

Mr. MODELL. Thank you for your question. The simple answer to your question is yes, I think we will fall further behind because if you look at the thousands of individuals and entities that have been designated as a result of Iran's illicit activities over the years that are now going to be exonerated essentially by this deal, of course, it is a setback. Those are people who are willfully engaged in criminal activity on behalf of the Iranian regime. So the idea that they are suddenly going to be brought back into Iran or some sort of international system in which they behave according to laws and regulations and good behavior doesn't make much sense to me. I don't know why that large, very large group of people, many of whom we don't have full understanding of what they are doing now or to the extent to which sanctions have actually impacted them over time, the assumption that those people no longer need to be watched is disturbing. So, yes, I think the answer is yes.

Mr. BARR. Can you give us a concrete example of how the sanctions relief in the deal would complicate our efforts or make more difficult the existing efforts to counter the financing of terrorism and, specifically, you referenced Hezbollah. You talked about the deficiencies in operations against Hezbollah as illicit financial apparatus within Lebanon. Maybe you could take that as the example.

How would the deal, the sanctions relief in the deal, specifically complicate our efforts to counter those activities in southern Lebanon?

Mr. MODELL. If you believe that the deal was going to lead to a windfall of tens if not over a hundred billion dollars to the Iranian government, and there have been disputes as to how that takes place and over what time, but nevertheless a very large amount of money, go back to 2012 and 2013, when the U.S. Government was getting very clear indications that because of the sanctions entire units of the IRGC who were acting overseas in places like Syria and Iraq and Lebanon and other places where we have a real problem with them, where our interests collide, those units were put on

hold, those activities were put on hold. When President Rouhani was elected in Iran, and we started to move towards a deal and now that we have a deal in place, the economy started to turn around. And now we have the promise of this money, operational budgets have already gone up. The entire budget of the IRGC and the Iranian intelligence force publically, as stated, has gone up. It has gone up by 50 percent over the last year. So the idea that you are not going to have a situation where those same entities, which we have had problems with for 36 years are not going to increase their activities in things that we find problematic or contrary to our interests.

Mr. BARR. Sorry. Can you elaborate also—with my limited time remaining, you testified about how it would be more complicated to verify compliance on the nuclear components of the deal if we are not fully tracking the flow of Iranian sanctions relief. Can you elaborate on that? Because Secretary Kerry has told Members of Congress and the public that most of the sanctions relief—he has attempted to assure us that most of the sanctions relief will go to internal improvements within Iran. So the question is, can you elaborate on the verification of the nuclear component to the agreement?

Mr. MODELL. First of all, I think that when you look at Iran's external apparatus for doing all the things, a lot of things with its nuclear program that we have found so problematic, in other words, illicit procurement, things that directly aid their program, you need to have a vast mechanism in place, U.S., U.S. allies, and the IAE working together. Without having an understanding of how that is going to work and how the Iranians are going to spend their money, or if you actually believe, like I do, that the Iranians have already strongly indicated that a significant amount of the money is going to be spent outside, contrary to what Secretary Kerry says, then you have the makings of a real problem.

Let me just touch briefly on what you said about Lebanese Hezbollah. One of the things that Lebanese Hezbollah, one of the reasons why it is such a problem, why Iran and Hezbollah have created this apparatus, it is so difficult to counter, is one of the things that Dr. Shelley mentioned was trade-based money laundering, repeatedly mentioning that. Since the early days of Hezbollah, Iranians and Hezbollah have gotten together and they had a very clear vision of how to create a commercial apparatus that enabled terrorist activity, criminal activity. That exists today. Iran still benefits from that, whether it is Hezbollah-related or nuclear-related, and that is going to continue.

Mr. BARR. Thank you. I yield back.

Chairman FITZPATRICK. The gentleman from Minnesota, Mr. Ellison, is recognized for 5 minutes.

Mr. ELLISON. Thank you, Mr. Chairman, and thank you, Mr. Ranking Member, for this hearing. I also would like to thank all of our panelists who have been so responsive and helpful to our understanding.

My first question is to Ms. Rosenberg. Ms. Rosenberg, on this Iran deal, you did publish an article, for which I want to commend you, and I thought it was well-written. One of the things you said is a successful agreement is by far the best way to reduce Iran's

nuclear threat, but for any deal to work, Tehran needs to know that if it cheats, economic pain will turn in full force.

If you believe the deal, what we do have—there is a deal, there is a fair chance that there will remain one, how should we move forward given that we are going to have to monitor whatever—and have—provide oversight to how things are going? If we assume that the people who want to kill the deal are not successful, and that is a fair assumption at this point, what is your assessment on the day after, and what we should be doing?

Ms. ROSENBERG. Thank you, Congressman, for the question.

I think that the appropriate way to move forward for the United States policymakers in particular is to ensure that the deal—assuming it does move forward—is carefully and aggressively implemented, and that includes the orientation of U.S. policymakers to act independently if necessary or certainly collectively within the mechanism of the U.N. to reimpose sanctions in part or in whole if Iran is shown to be cheating on its commitments. There is nothing in this agreement that says that the U.N. has to completely reimpose all sanctions which puts quite a high bar on Iran's cheating in order to do so. It can do so—the U.N. can snap back partial sanctions. The United States should also affirm its right and ability to reimpose sanctions or take other measures outside of those financial coercion mechanisms in order to make sure that Iran is complying with the deal.

And relevant to the conversation that was just occurring before you had your time on the floor here, I think it is true that we should be concerned that Iran will be a greater threat, terrorist threat, through itself and through its practice in the region if the United States and allies abroad do nothing further. That is why we have heard a number of suggestions about additional steps U.S. policymakers should take in order to ensure that Iran is not able to move money around itself or through its proxies. For concerns about countering trade-based money laundering that Hezbollah and others are associated with, as well as Iran's use of newly undesignated financial institutions, to the extent that there is a current evidentiary record supporting that will illuminate illicit finance and that Iranian banks are engaged in, that should be exposed publicly. The United States should designate those banks under terrorism authority, and we should urge our international partners to join us in designating those banks in order to keep them outside of the legal financial system and not able to move illicit Iranian funds around the financial system.

Mr. ELLISON. Thank you. Let me ask you a question on a different topic.

About the IRS, in particular, the bank secrecy examiners at the IRS are critical in fighting against terrorist financing. How many BSA examiners work at the IRS, if you know? And I hate asking people how many because that is like an on-the-spot question. But if you know, good. If you don't, generally. Are there enough, and how many institutions are they responsible for examining?

I guess my real question is, do we have the kind of—do we have the complement of people that we need in order for the IRS to fulfill its mission under the bank secrecy examiners—with the bank secrecy examiners?

Ms. ROSENBERG. Off the top of my head, I cannot remember a number of BSA examiners. I might have when I was still at Treasury. I am sure we can find that number.

Mr. ELLISON. I wasn't trying to—

Ms. ROSENBERG. No, no problem.

Mr. ELLISON. —put you on the spot.

Ms. ROSENBERG. But I think to your point about whether they have the adequate examination capacity, much has been said about the inadequacy of Federal functional regulators or examiners to adequately cover both the financial institutions as well as the nonfinancial institutions that are at risk for terrorist financing and other corruption and criminal activity. There are ideas that exist about how to transfer some of FinCen's for example, examination authorities to the IRS and to other—divulge those to other State regulatory authorities in order to look after potential illicit activity occurring at bank and nonbank financial institutions. But certainly the reason for such creative thinking is because there is currently an inadequacy in that area.

Mr. ELLISON. I just want to say thanks for your great work, and I look forward to reading your next article.

I yield back.

Chairman FITZPATRICK. The gentleman from Arizona, Mr. Schweikert, is recognized for 5 minutes.

Mr. SCHWEIKERT. Thank you, Mr. Chairman.

Dr. Shelley, first, I want to compliment you, because at least in your testimony, both written and what you have said, you have come closer to anyone in this committee on my fixation, my concern. We seem to be having a discussion that somehow the terrorism financing world is out there using the SWIFT system, and we are seeing the wire transfers and not understanding the scale of the distributive opportunities. When their story is coming from border patrol agents of money moving in diamonds and other types of products, when we are seeing stories of completely informal financing mechanisms, when we are seeing stories that it is money laundering for hire. So today you may be a terrorist; tomorrow you may be a narcotrafficker; next week you may be someone engaging in counterfeit products; and the week after that it is the folks who stole data who are trying to monetize it. And it is becoming a profession out there with its own accountants, with its own systems.

Dr. Shelley, how do I break my brothers and sisters and those in the bureaucracy out of the mindset that we can do this as a Treasury banking regulator and understanding the distributive world that is around us and the perverse professionalism that seems to be going into the movement of bad actors' cash?

Ms. SHELLEY. Well, thank you for your kind words, but they also captured my enormous concern on this issue. And I am very thankful for the support that is here, I got from the Andrew Carnegie Foundation, to go out and be a public intellectual on these issues and write more on this.

I cannot think of a more burning issue than the need to get out of this stovepipe way of thinking about it, and we have, all of us contributing to this discussion, where Mr. Modell was talking about Hezbollah and its involvement in the Captagon and the drug trade, and Mr. Larkin, what they are doing on the computers. And there

is a whole thing that we haven't mentioned much today of the dark Web in which we cannot even be following very easily, except through undercover law enforcement, what is going on in this illicit trade in the virtual world, which is something that you need to be looking at much more in the future.

But I think we need a reconceptualization of this, and any advice or support that I can provide or way we can work together to change this mindset is of paramount need for our country.

Mr. SCHWEIKERT. Dr. Shelley, in your research, in your reading, have you come across reasonably factual antidotes of things that you have been shocked on the creativity of how these bad actor dollars are moving—bad actor resources are moving and how much of it is actually being moved not in a cash equivalent but in commodities and our services, our documents, or even data?

Ms. SHELLEY. I think a it is a huge amount, particularly in the Middle East. As I say, it's a cultural tradition that goes back thousands of years. You go back to Hammurabi's Code in Mesopotamia, and they were already dealing with fences and how to prevent illicit trade through stolen goods.

And so, particularly in that environment, we are dealing with trade issues, and that is the financing core of it. But what we haven't also talked about is how some of this massive illicit trade that we have in illicit markets in Europe is being used to help fund people's passage to help join ISIS, and also the money that they are bringing with them. It is a global illicit trade.

Mr. SCHWEIKERT. I had someone who was insisting that they have studied this world and said many of the bad actors don't even like to touch cash, because it is too expensive to wash, and it is heavy, and they prefer moving high-value commodities, whether it be an exotic car or diamonds and those things.

Ms. SHELLEY. Or ivory tusks.

Mr. SCHWEIKERT. And my fear, Mr. Chairman, is we seem to be looking at this issue almost as traditional Westerners, with the accounting and finance backgrounds instead of understanding, just as we talk about the new distributive economy that is happening around us, well, I hate to say it, but those engaged in bad acts, whether it be terrorism, whether it be drugs, or everything else out there, may be also creating their own web of creativity.

And, with that, I yield back.

Chairman FITZPATRICK. The gentleman from Ohio, Mr. Stivers, is recognized for 5 minutes.

Mr. STIVERS. Thank you, Mr. Chairman.

I would like to commend the chairman for his leadership of this task force and the ranking member as well for your hard work here. And it is unfortunate that this is our last meeting of the task force because I think there is a lot more work to be done.

Ms. Rosenberg, it has already kind of come up a little bit. Mr. Ross talked about this a little bit, but the fact that the Iran deal could give up to $50 billion to Iran immediately, which could then be diverted to terrorism, does that, for you, give us a reason to maybe continue something like this task force, to continue to monitor what is going on out is there?

Ms. ROSENBERG. Absolutely. And, unfortunately, that $50 billion is only a marginal constituency in a broader threat about which

this task force and indeed many other stakeholders should be concerned.

Mr. STIVERS. Thank you.

Mr. Modell, you and Dr. Shelly talked a little bit about and emerging means of financing. I think you talked about mobile payment technology, trade-based methods. Dr. Shelley just referred to bitcoin a few minutes ago and the dark Web.

Are we creating sufficient protections against these emerging means of financing terrorism activities?

Mr. MODELL. In my opinion, no. And I think it goes back to what Dr. Shelley and others have alluded to, and that is we don't have enough people in government who have the sophistication to be able to understand what the current illicit mechanisms are, and what the next generation of illicit mechanisms will be. I keep going back to Hezbollah, because they have been so successful at evolving into an organization that epitomizes the problems we are talking about here. First, it is used cars. Then, they are involved in diamonds. Then, it is used clothing. So you are avoiding the use of cash. They have had mastery of it, and it has been part of their long-term vision, and it will go on.

Mr. STIVERS. Thank you.

Dr. Shelley, you and Mr. Larkin, kind of following on what Mr. Modell just said, have suggested that we do a better job of public-private partnerships. And Mr. Larkin is sort of advocating for how effective it has already been, the one that he is involved in. You talk about how DHS doesn't do enough corporate advisory work where they work with people who know what is going on out there. To both of you, wouldn't that help? Whoever wants to start.

Ms. SHELLEY. I couldn't agree with you more. The Overseas Security Advisory Council (OSAC) at the State Department has helped them. I think we need that in this area as well with many, many corporations feeding in information and sharing and giving insights.

Mr. LARKIN. I agree. And part of my written and oral testimony was intended to say that we have to be careful about defining the threat too quickly and not backing off in looking at the whole landscape because, as pointed out by my colleagues, they are going to generate funds through any means possible.

Mr. STIVERS. It is an evolving threat, to your point, and we need a very mobile and robust defense.

Mr. LARKIN. Right. And I think there can be more. It has gotten better, but I think there can be more information coming back from law enforcement as to what they found that the true terrorism groups are doing.

Mr. STIVERS. Just like in cyber defense, we don't do a very good job of sharing information back from the government to the people who face the threat.

Mr. LARKIN. Right. It's getting better, but there is still a lot of room for improvement.

Mr. STIVERS. And I think your organization, by the way, is a great model we can learn from. I really appreciate your being here, Mr. Larkin.

Mr. LARKIN. Thank you.

Mr. STIVERS. Mr. Modell, you are putting your finger in the air.

Mr. MODELL. I just want to throw something out there, as you are looking for a congressional going forward with the Iranian implementation—

Mr. STIVERS. And that is what I would like to talk about here, yes.

Mr. MODELL. I would just say, according to the structure, the way, the deal, the way I have read it is every 90 days and every 180 days, the Obama Administration and future Administrations are going to have to report to Congress the extent to which they are complying with the deal. Having a task force continue and having them look specifically at the extent to which they are complying with financially related issues, whether it is terrorism or nuclear-related, would probably be very useful.

Mr. STIVERS. Great idea. One last follow-up for Dr. Shelley, the other thing you suggested is because of the tie between crime and terrorism financing that we better coordinate our efforts. Could DHS do a better job of helping communities? I know the New York and Los Angeles Police Departments have done a pretty good job. But could DHS do a better job of helping build capacity across our country in local law enforcement, and if so, how?

Ms. SHELLEY. I think that they could help take the model that has been developed in New York and Los Angeles—that face so many threats and have had so few acts of terrorism—and put this together and have lessons learned, handbooks that we would do, and generally a much greater operational effort to change the culture in many urban areas and regions of the United States.

Mr. STIVERS. Thank you.

Mr. Chairman, with your indulgence, could the panelists show by hands, could you raise your hand if you think the task force should continue? I will note that was unanimous.

Thank you, Mr. Chairman, for your great work.

And thank you, Mr. Lynch, for your work.

You guys have worked together on this in a way that Congress needs to continue. And I hope it continues through extending this task force. And I will certainly personally urge the chairman of the Financial Services Committee to allow you to continue the incredible work you have started. Thank you to the panelists.

I yield back.

Chairman FITZPATRICK. Without objection, two additional Members will be recognized for follow-up questions, beginning with the ranking member, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman. And thank you for your kind words. Mr. Larkin, we had an opportunity a couple months ago to go into Gaziantep in southern Turkey to meet with a group of Syrian rebels who are largely engaged in opposition to Bashar al-Assad and his regime in Syria but also against ISIL on occasion. We met with them to determine what efforts that we might bring to that fight, especially against ISIL. In our conversations, a number of these different rebel leaders indicated that they used a messaging platform called WhatsApp. It is pretty common. It provides full encryption, not end-to-end encryption. But, interestingly, it now has a banking app so that they can transfer funds in and out. The depository bank that is connected to that I think is Axis Bank in India. And we have a great relationship with India, especially

with the anti-money laundering and terrorist financing implications considered.

But if the rebels are using this as a regular funding app, I am sure that ISIL and others are doing exactly the same thing. And I wanted to know what are the implications here for us to try to wall off ISIL, even if, as Mr. Modell indicated, it is great that Turkey is in the fight now. And, actually, it looks like they are beginning to police their border in an effective way. Syria is still a mess, a very porous border. We have been out there to Al Qaim on the Iraq border. It is tough enough physically to close off that border. If this financing is going on through WhatsApp and I am sure it will just morph into something else. These things seem to be—they trend from time to time. What are the implications though for us to try to shut off financing if it is so easy to do wirelessly? And there seems to be great connectivity in that area to use these apps. What are the implications from a cyber security standpoint?

Mr. LARKIN. Thanks for the question. I can speak from my view of what we do and what we have done at the NCFTA in working with the technology experts out there. One of the regular discussions that occurs is, what is the implication of this new product or service that is out there, this new app, what are the impacts that we are going to see, and what are the things that we can potentially do to help be more proactive about the intelligence or the capabilities that can be brought together? I don't know the specific details of how that app works. But that is a good example of how the resources that come together at the NCFTA literally brainstorm on those things every day. And it is an environment that you can do that where you really couldn't do that in government space or probably had difficulty doing it in individual corporate space. But you can in a sort of a meet-in-the-middle neutral environment where that kind of conversation is a regular part what is discussed. I think there is good opportunities. The implications—I can't speak to the specifics of what those are if we don't do that. But I can tell you that I think we are moving in the right direction.

Mr. LYNCH. Maybe that is a conversation I should have with FinCEN off-line then.

Ms. ROSENBERG. May I speak to that issue?

Mr. LYNCH. Sure, Ms. Rosenberg. Absolutely.

Ms. ROSENBERG. Congressman, I think you have just laid out the perfect argument for why it is important for the bank, that banks, that app, to have a strong AML program. Now, that bank has correspondent banks which may exist in the United States. And there are financial regulators in the United States and in India which have a responsibility to ensure that app banked by that bank in India does not engage in money laundering or terrorist financing activities. So U.S. financial regulators have an opportunity directly for institutions in our jurisdiction to require them to engage in appropriate customer due diligence, to make sure that none of any illicit finance moving through that app can come back into our financial system.

Mr. LYNCH. It works well, KYC, know your customer, works very well when the person is walking into the bank. I guess I have problems conceptualizing how that happens electronically when we are

doing it as a wireless messaging platform, and it is instantaneous. I guess I have a—

Ms. ROSENBERG. If that bank in India is doing its job, what it will have, doing a good job, what it will do is gather adequate information about that app, who the beneficial owners are of this app, the kind of activity that app will be engaged in domestically, internationally, et cetera. And if anything moves beyond, they should have a requirement to file any kind of suspicious activity reports which, if it is properly shared with law enforcement in the United States and internationally, then that information will be disclosed. There are many links in that chain that can be weak ones. Nevertheless, that is the argument you have just laid out for a strong program.

Mr. LYNCH. All right. Thank you very much.

I yield back. Thank you.

Chairman FITZPATRICK. The vice chairman of the task force, Mr. Pittenger, is recognized as well.

Mr. PITTENGER. Thank you, Mr. Chairman.

I would just like to probe a little bit further with data integration. We have had discussions with Secretary Lu, as well as those who are involved in our border control, and find out that we have limitations in terms of data sharing there, albeit FinCEN has very sophisticated software in great capacities. We, as well, have had discussions with the major banks and how their capacities could be enhanced with closer integration with our systems. What structures would you recommend potentially with the private sector, and/or what oversight legislation or regulatory change would you recommend considering the privacy issues that would enable our data capacities to be better shared among agencies and among the private sector?

Mr. Larkin, we will start with you.

Mr. LARKIN. Okay. Thanks for the question. In my experience, in developing the NCFTA in particular, we have learned that sensitive information regarding personally identifiable information (PII) is often not needed. So anything that can be done to strip out PII from that information that we are trying to share is typically something that is not part of what we recommend sharing. It is the threat data. So if we can get people to understand that the inbound threat, how it looks coming at the company or coming at the person is specific to the threat actor and specific to the device they are using or the technique they are using or the malware they are using, that is the valuable information that we want to share, as well as where the exfiltration is headed, whether it is data or funds or other things that are going to be monetized. So the inbound and the outbound side of the information sharing are the critical pieces. If there are ways to strip off the PII in the middle and then move towards creating sort of a broader safe harbor for information sharing among cross-sector stakeholders, I think that is a worthwhile conversation to have.

Mr. PITTENGER. Your response, Ms. Rosenberg?

Ms. ROSENBERG. Thank you. You mentioned border control. So one of the challenges for U.S. financial institutions, such as Bank of America, Citibank, et cetera, exists when they are trying to put together suspicious activity that exists within their own financial

institution across borders. So, for the United States and in Mexico, for example, if they suspect there is activity associated with bulk cash movement, drug, narcotrafficking and the movement of drug money across a national border, the U.S.-Mexico one in particular, it can be difficult for them to move suspicious activity reports within their own financial institution that are not designed to ever move outside of it in order to put these pieces together and communicate them to Federal regulators. In addition, the idea that I had mentioned previously about contemplating safe harbor arrangements that would allow the sharing of this information and possibly a self-certification mechanism similar to what exists organized by the Commerce Department for technology sharing, technology information sharing, may be a model that can be borrowed from in the case of financial services.

Mr. PITTENGER. Thank you. How can FinCEN better track trade-based money laundering with our Customs data?

Ms. ROSENBERG. One of the challenges for FinCEN is, of course, putting together the appropriate—understanding the methodologies that are used by criminals. The case you just mentioned is trade-based money laundering. Having the adequate reporting from financial institutions when they flag certain suspicious activities that they identify as associated with trade-based money laundering—and the Hezbollah example is an excellent one—allows them to then comb through their own, organize and analyze their own massive bank of SAR material in order to create the methodologies that they can then share with the law enforcement community either as particular leads or in the form of illuminating the particular methodology that would exist from a criminal enterprise, which can then allow law enforcement counterparts to build cases and pursue them.

Mr. PITTENGER. Thank you.

I yield back my time.

Chairman FITZPATRICK. The gentleman yields back.

With that, the questions are completed for the hearing today. I do want to thank the witnesses here today. You have identified some risks, some gaps in our system. You have identified some potential legislative fixes. And you have been very responsive. So we appreciate your time and your service.

And I have to say that during our 6 months of hearings, we have had some outstanding panelists who have come to help us to do our work, which we believe is important. And we know that you believe that as well.

And during those 6 months, in my work with Ranking Member Lynch, Vice Chairman Pittenger, and really all the members of the task force, there has been no light between us on the work that is set out before us, identifying the gaps, finding the solutions, protecting our people, our country, and our constituents, including our constituents who work in the important financial service areas and industries, not just in this country but abroad. So all of you have helped us do that.

And I do want to recognize the hard work of the committee staff, especially Mr. Joe Pinder, Mr. Bill You, Chris Matarangas, of my staff, the staff of the ranking member, Mr. Lynch, and all the mem-

bers of the committee, of course, without which the staff, I am sure we agree that we wouldn't—

Mr. LYNCH. And Jackie Cahan. She's on my staff.

Chairman FITZPATRICK. We appreciate all that work. And I think we all agree we still have a lot of work to do. And you have helped us accomplish that.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

So with that, the hearing is adjourned. Thank you.

[Whereupon, at 12:17 p.m., the hearing was adjourned.]

A P P E N D I X

September 9, 2015

Written Testimony for the House Committee on Financial Services Task Force to Investigate Terrorism Financing

Effective Public-Private Partnerships: Lessons Learned from the National Cyber Forensics & Training Alliance

A Statement by Daniel Larkin
Retired FBI Unit Chief and Founder of the National Cyber Forensics & Training Alliance
September 9, 2015

Testimony of Daniel Larkin
Retired FBI Unit Chief and Founder of the National Cyber Forensics & Training Alliance
Written Testimony for the House Committee on Financial Services
Task Force to Investigate Terrorism Financing
September 9, 2015

I. Introduction

Good morning Chairman Fitzpatrick, Ranking Member Lynch and members of the Task Force to Investigate Terrorism Financing (Task Force). I appear today as a former Unit Chief of the Federal Bureau of Investigation (FBI) and founder of the National Cyber Forensics & Training Alliance. I thank you for the opportunity to share with the Task Force some personal experiences I had over the course of my 24+ years with the FBI in developing models for better collaboration between public and private sector subject matter experts (SMEs) to identify and defend against evolving cyber-based threats. I understand that the Task Force is also interested in functional models that might be used to better enable private sector organizations to collaborate with government agencies, including law enforcement, in the fight against international money laundering and terrorist financing. I believe the National Cyber Forensics & Training Alliance (NCFTA) is such a model.

In order to understand how the NCFTA model was developed, it is helpful to consider the following:

- How we define cyber threats is important, and that definition needs to evolve as the nature of globally spawned cyber threats evolves.
- Historically, law enforcement tended to organize its efforts into silos, leading to a narrow view of threats and leaving many cases unaddressed.
- The majority of significant criminal cyber-based threats involve organized crime and money laundering.
- The vast majority of computer networks belong to the private sector.

- As a result, most of the early warning signs – i.e., most intelligence on the threat – reside with the private sector and the private sector is most often best suited to identify those anomalies.
- This private sector intelligence, although sensitive in nature, is most often not classified.
- With cyber, law enforcement needs private industry help more than vice-versa.
- Trust is critical to public/private collaboration, both between the government and the private sector and with the public at large, and it needs to be earned.
- Public/private partnerships must be structured to protect privacy and promote transparency. Personal information, the content of communications, and other private material must not be shared with the government absent lawful process. All sharing must be lawful. In addition, the arrangements for, and the type of information shared, should be transparent to those involved and the public. Private sector working in neutral space – not within government space – can contribute to that effort.
- Public/private collaboration within Government space can inhibit the ability of private sector partners to access and share their real-time intelligence, significantly hindering collaboration.

II. An Early Foundation – Computer Emergency Response Team Coordination Center (CERT/CC)

In 1994, I was re-assigned from FBI Headquarters to the Pittsburgh Division of the FBI. No Federal law enforcement agency in Pittsburgh was large enough to essentially "go it alone". As such task forces were more the norm than the exception. The spirit of cooperation was, and still is, strong there.

As members of this Task Force may know, the first Computer Emergency Response Team Coordination Center (CERT/CC) was established in the 1980s at Carnegie Mellon University in Pittsburgh, and was initially funded by the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense. The developing relationship between law enforcement and the CERT/CC was instrumental to the formation of the NCFTA.

In 1997, it became evident that more and more business was moving to the Internet and, not surprisingly, so were the criminals. At the time, FBI Pittsburgh participated in numerous

task forces addressing a variety of criminal activity. In meeting with Financial Crimes Task Force members, FBI raised the idea of evolving at least part of our Task Force to a Cyber-High Tech Task Force. I initially gained support for the idea from other key Federal agencies as well as State and Local law enforcement. I then suggested that we include the CERT/CC representatives, as they had become experts relative to cyber-related threats and were essentially right in our backyard.

III. Addressing Private Sector Concerns of Working with Law Enforcement

Upon approaching managers from CERT/CC to participate in the developing Cyber-High Tech Task Force, I was surprised to learn that members of the CERT/CC were reluctant to work with the FBI (or other Federal law enforcement agencies) because of concerns that:

- The FBI would force organizations to reveal sensitive potential vulnerabilities they had shared on a confidential basis with CERT/CC.
- The FBI would possibly "drag" organizations into a prosecution which also could reveal the organization's potential vulnerabilities to the public.
- The FBI would create disruptions that would impede organizations' ability to conduct business and defend themselves against cyber threats.

I explained that the FBI and other agencies had become more sensitive to private sector concerns, and that the FBI was committed to prove that in order to gain their trust. I suggested that the FBI begin an immersion program, where an FBI Cyber Agent would be detailed to the CERT/CC to serve as "a fly on the wall" and offer support for CERT/CC and their clients, without negatively impacting their relationship.

Within the first six months of this program, the embedded FBI agent was able to help CERT/CC and two of their clients more fully understand the scope of threats they were facing, based on prior knowledge the agent had of similar incidents. Later, CERT/CC staff and their

clients worked cooperatively with the FBI to help identify threat/actors who were ultimately prosecuted, with no negative impact on the relevant company.

CERT/CC management and I later met to propose expanding the immersion program to include more law enforcement and private sector representatives, based on the recognition that the project became successful only because people sat together and collaborated. The setting encouraged individuals to get to know each other and collaborate; the environment helped to develop trust among participants and became an early principle of the NCFTA model. It was also important that the relationship was transparent, and there were appropriate procedures between the two separate spheres (public and private).

IV. Focus Group Meeting Leads to Core NCFTA Model

By this time (1998) Pittsburgh had developed a strong and growing base of high technology and financial services organizations. From this base, approximately 30 cross-sector organizations were invited to a Focus Group meeting to consider embedding resources together in order to better collaborate in the common fight against international cyber threats. Out of this Focus Group, a white paper was developed which summarized the core objectives and potential returns on investment of a new public/private alliance—which eventually became the NCFTA. These objectives included:

- Creation of a neutral "meet in the middle" environment where the government and private sector could collaborate in a timely and efficient manner.
- An organizational model that brings together private sector stakeholders with domestic and international law enforcement representatives to build trust and to identify, mitigate and ultimately neutralize significant global cyber-security threats.
- The creation of joint initiatives based primarily on a consensus view of priority threats from the private sector, with law enforcement support being sought secondarily. The theory being that if industry consensus is large enough, law enforcement will find a way to assist.

- Space should be primarily designated as Sensitive but Unclassified (SBU), with all participants undergoing background investigations tailored to their role and responsibilities.
- Creation of a simulation lab (or malware lab) where various network platforms could be simulated to evaluate how certain malware might behave, appear and be detected and mitigated.
- Participants would be vetted SMEs and be expected to share knowledge and expertise.
- Sharing of threat/risk intelligence would remain confidential with Non-Disclosure Agreements (NDAs) executed between partners to protect proprietary information.
- Joint training would be developed to ensure a common understanding of permissible private sector involvement and information sharing.
- Lawful access to appropriate law enforcement resources would be developed and streamlined.
- Training on best practices would be developed and refined regarding newly identified threats and the proper handling of digital data that might ultimately assist in combatting cyber threats.

V. Official Establishment of NCFTA as a Non-Profit

After considering several organizational options for formally establishing the project, a local law firm offered to research alternative models, taking into account the proposed vision and objectives outlined above. After approximately one month of research, the firm suggested that a 501(c)(3) non-profit entity be established to serve as that neutral "meet in the middle" body. This organizational model allowed public and private entities to establish relationships via different means, such as through representation on a Board of Directors or through a broader Board of Advisors. Over the following 18 months, a group of volunteers from the Focus Group crafted a business plan, articles of incorporation and bylaws to advance the process. Finally, in 2002 the NCFTA was officially incorporated as a non-profit in the state of Pennsylvania.

VI. Proving the Model Works

Over the succeeding 13 years, numerous investigative initiatives were developed through NCFTA with cross sector partners, spawning hundreds of investigations involving hundreds of criminals, both domestic and foreign. A common thread through many of these investigations has been international organized crime, money laundering, and in some cases ties to terrorist financing.

What began as a regionally supported effort also has shifted to an international and, from a Federal law enforcement perspective, headquarters-supported project. All law enforcement embedded at the NCFTA are assigned to their respective Headquarters, enabling them to serve as a better resource for industry in getting cases developed and assigned globally.
The NCFTA, in partnership with the FBI, also has expanded the "make it personal" objective internationally, hosting annual International Task Force sessions for three months each year. Over the years, representatives from numerous countries have spent time as embedded partners at the NCFTA, developing joint investigations and an enhanced rapport with U.S. law enforcement and private sector partners.

Today, numerous private sector organizations embed SME resources at the NCFTA alongside a growing pool of domestic and international law enforcement. Hundreds of additional SMEs connect to the NCFTA via various real-time communication channels set up to facilitate the expanded collaboration. Extensive information regarding the NCFTA and its initiatives is available at www.ncfta.net.

VII. Lessons Learned

So what are some of the lessons learned from the evolution, establishment and operation of NCFTA?

- Significant global threats may initially manifest themselves in a variety of ways known only to the private sector, and their significance may not be understood until the information is pooled.
- Early warning intelligence may give the appearance that the threat is routine or common, such as a common phishing or ID theft scheme. However, with an expanded focus through NCFTA, it may actually turn out that the scheme is part of a much larger campaign with many more tentacles and a potentially more significant impact.
- Cyber criminals will enlist many different and creative schemes to generate funds, such as through coordinated networks of domestic and international money mules, prepaid reloadable cards, virtual currency and other means. Monitoring, detection, mitigation and responses must also continue to evolve with the same creativity.
- Using a private model, in the case of the NCFTA a 501(c)(3) non-profit entity, can make open and transparent public-partnerships easier.
- The NCFTA model leverages "existing" resources by giving them a better environment in which to perform. From this perspective it is a very efficient work force multiplier.
- Relationships are vital to make collaboration work, and they can also be fragile.
- Making it personal--knowing your partners' perspective and needs--is essential to success.
- The human capital development benefits of the NCFTA model are substantial.

VIII. Conclusion

Thank you again for the opportunity to come before the Task Force today and share some of my experiences as an FBI agent and founder of the NCFTA. I would be pleased to answer any questions the Task Force may have regarding my experiences with the establishment and operation of the NCFTA or the benefits of public/private partnerships like NCFTA.

"Terrorism Finance: Options for Moving Toward a Whole-of-Government Solution"

Prepared testimony of Scott Modell,
Managing Director, The Rapidan Group
Before the House of Representatives Committee on Financial Services

September 9, 2015

Chairman Hensarling, Ranking Member Waters, Members of the Committee, good morning and thank you for this opportunity to testify on "Could America Do More: An Examination of U.S. Efforts to Stop the Financing of Terror." Terrorism finance has become one of our most pressing national security challenges, yet the plans, programs, and practitioners are falling far short of where they need to be. My contention is simple: Almost everyone in the US government "knows just enough to be dangerous" about finance, but the time for going well beyond that is long overdue.

For the past decade or so, the US government has attempted to develop a professional cadre of law enforcement agents, civilian and military intelligence officers, analysts, and others to pursue a new field of operations that came to be known as "Counter Threat Finance" (CTF) operations. Their purpose was to effectively counter the financial and logistical depth and sustainment capacity of adversaries engaged in irregular or traditional warfare. Hitting the finances, financiers, and illicit networks, it was thought, would become an important means of warfare. Progress has been limited.

Looking ahead, it would serve us well to take an agency-by-agency account of what we collectively know about terrorism finance, an audit of each agency's CTF track record and current trajectory, and ways to add or pare down their respective roles and missions as part of a whole-of-government approach. This should not seek to bring all agencies together all the time. Threat Mitigation Working Groups, Interagency Task Forces, and the like are usually stood up with the best of intentions and may last for a while, but often end with poor results.

Where to Start: Roadmaps and End States

An overarching financial order of battle should be developed and used as the basis for working with our closest liaison partners to develop operational plans by country, region, industry, etc. It should serve as the basis for conclusions on desired end states and pathways for getting there. In doing so, it is critical to know how resources will be arrayed, what successful whole-of-government CTF campaigns might look like (including the role of our foreign partners), envisioned impacts, and the CTF apparatus that should remain in place.

Leveraging the strategic clarity that will come with a clear vision how to disrupt terrorist finance cells and infrastructure should consist of several steps, including the following:

- Identifying and prioritizing target sets;
- Taking account of existing sources, ongoing operations, and a series of plans to acquire new sources and capabilities to build new operational initiatives;
- Building cases with law enforcement agencies;
- Building new intelligence collection priorities that raise the importance level of CTF-related collection, recruitments, and support to CTF operations;
- Utilizing all available inter-agency data sets to identify assets, shell/fronts, property, liquid assets, and so on; and

- Coordinating with Country Offices/Embassies to build out an expanded base of foreign liaison CTF operations.

Strategic and Tactical Recommendations

Key military, law enforcement, and intelligence bureaucracies must be properly oriented, educated, trained, and integrated into a government-wide effort that consists of coordinated CTF actions against critical financial infrastructure and personnel around the world. Some of the fundamental recommendations for beginning this process include the following:

1. Build a CTF order of battle that maps key networks on a global scale, along with a plan on how to attack high value targets transnationally. This should draw assiduously on partner country liaison services, which are indispensable for sustaining a meaningful campaign of investigations, indictments, and arrests. The emphasis here is on greater international cooperation as part of a coalition of like-minded states that are part of an open-ended strategic intelligence and law enforcement campaign – not just a series of strikes.

2. To truly prepare individual government agencies to work more seriously and collaboratively on CTF operations, bureaucratic cultures have to change. The intelligence community can undoubtedly do more to enable law enforcement to identify, target, and take down illicit businesses and revenue streams. Intelligence assets should be used in support of strategically planned law enforcement operations to expose illicit networks, arrest their perpetrators, freeze assets and attack crime-terror pipelines though the international trade and banking system. Once bureaucratic cultures are reformed and left with greater openness on interagency collaboration on CTF operations, we will be better equipped to work transnationally against an elusive and irregular target set.

3. Intelligence collection, law enforcement actions, and even a flexible range of covert action must take place inside some of the worst financial safe havens and terrorism enablers, such as Qatar, Kuwait and Lebanon. Too many US missions around the world maintain an ultra-cautious posture when it comes to operational activities against host country financial targets. A good example is Hezbollah: CTF operations cannot be taken seriously if we continue to avoid operations against Hezbollah's illicit financial apparatus inside Lebanon because we don't want to destabilize the Lebanese banking system.

4. A new Covert Action (CA) finding is necessary to broaden the authorities extended to US agencies operating globally against CTF targets. A new CA finding should come with White House backing for a more aggressive operational posture, with (and sometimes without) properly motivated third-country liaison services.

5. Build the operational capacity of our Treasury attaches. Before adding more Treasury attaches to work alongside willing and able foreign liaison services, Treasury should conduct a comprehensive study on OFAC designations. Such a study would assess the current state of designated banks, investment companies, exchange houses, and other financial nodes of terrorist networks, the impact of USG pressure over time, how designated entities and individuals have countered, and the degree to which they have been disrupted, dismantled, or destroyed. Treasury should rely less on the power of designations and more on up close and personal investigations of banks, exchange houses, hawaladars who will continue to operate with or without designations. See #6 below.

6. Treasury is not set up for financial and economic warfare or integration with other interagency partners who possess the needed level of financial operational authorities and capabilities. To be more effective, Treasury needs its own operational element to play a greater role in financial operations across the government, especially by law enforcement agencies.

7. Information Operations (IO) is a capability that has not been used very effectively or in a sustained manner in the CTF realm. To magnify the impact of CTF law enforcement operations, IO programs should use the media and other tools to educate publics that are unaware of how terrorists move money and corrupt financial systems and to warn them of the consequences of abetting them. IO can also be used to embarrass governments, companies, or even individual violators.

8. Rewards for Justice is the biggest incentive to sources, facilitators, and testifiers who assist US law enforcement investigations and operations. Rewards for Justice pay-outs should be used more creatively as a tool to motivate foreign liaison partners to conduct higher impact CTF operations. A coalition of well-intentioned states coalesced around a common aversion to terrorism is a good start, but insufficient to adapt quickly enough to adversaries who are innovative, resilient, and increasingly transnational.

Some of the driving principles that could make a difference over time include the following:

Boost Law Enforcement

Put law enforcement in a position to succeed. Law enforcement action elements of the U.S. government must have the financial, intelligence and targeting support they need to build strategic legal cases against facilitators of crime and terrorism – from individuals such as professional arms brokers to corporate entities such as banks engaged in money laundering or facilitating terrorism financing – and treat them as criminal actors in their own right. If we cannot properly resource our own law enforcement agencies, the already tough task of managing foreign liaison relationships becomes much more challenging.

Counterterrorism efforts may be able to stop attacks, but law enforcement can attack entire networks, which is why more intel-related activity should support law enforcement operations. A good example is Hezbollah, which should be treated as a transnational criminal organization. In addition to being the world's most formidable terrorist and paramilitary organization, Hezbollah is also engaged in a global crime spree, including cocaine trafficking, money laundering and racketeering. Indicting Hezbollah as a criminal organization holds great promise, including the possibility of using RICO statutes to prosecute Hezbollah, but we are only beginning to find ways of how to do that.

Define Strategic Principles, Make Changes Permanent

First, CTF operations cannot be an ad hoc add-on to more permanent operations. Their importance should be elevated in the panoply of US government actions against narco-terror organizations. Only then can we effectively integrate our international partners into CTF operations. Second, we are unprepared to take full advantage of the information collected and stored by Foreign Intelligence Units (FIUs). We should explore new ways of using FIUs in sustained lines of attack against cultural, business, and social bases of operations and lines of communication that make up "the business of irregular warfare." Businesses seek to be self-supporting, self-financing, and cloaked in licit covers. Stopping illicit money flows will be easier once we incorporate several strategic principles, such as the following:

- Synchronize activities within distinct time and space to send a clear signal
- Aim to effect key people and organizations in the target countries

- Leverage law enforcement evidence to underline legitimacy of actions and create coalitions
- Channel activities and finances to locations where we have operational advantage
- Aim for lasting disruption, not just interruption
- Increase costs, reduce access to capital, and "squeeze" financial resources to limit freedom to operate
- Transnational threats require transnational nodes of financial support to facilitate non-state insurgent, terrorist and criminal organizations. Terrorists are increasingly turning to emerging means and methods for their finances (e.g., Mobile to Mobile banking, M-Commerce, Trade Based methods, BMPE, etc.) as well traditional methods that still work (e.g., Front/Shell companies, Hawala, etc.).
- Working in an asymmetric operational environment demands looking for and seizing on asymmetric financial opportunities
- Look to expose vulnerabilities in the long admin, financial, transportation supply lines

Metrics Matter

To bring this all together, the Interagency Community should call for and ultimately support the creation of next-generation CTF performance metrics that are tied back into the overall counter-terrorism financial order of battle and the plan to attack it. However, accurate monitoring of progress in a whole-of-government campaign will be just as challenging as the execution of the campaign itself. Key determinants of success or failure will only result from a sustained flow of all-source intelligence collection and analysis on financial networks, as well as reasonable changes in bureaucratic culture over time to solidify interagency cooperation.

Information Operations Case Study: Iran

An IO program against Iran should focus on the failure of state enablers to address the risks of terrorist financing and the threat that poses to the integrity of the international financial system. It should also include pressure by calling on Iran to criminalize terrorist financing, effectively implement and act on suspicious transaction reporting, and to create a genuine Financial Intelligence Unit (FIU personnel are not authorized by law to investigate financial transactions). While insurance companies, banks, credit institutions, and charities are required to report suspicious transactions, the largest state-run charitable foundations known as "bonyads" are not.

An IO campaign should also go further to expose the hypocrisy of untaxed, unregulated, and unaudited assets worth tens of billions of dollars controlled by the bonyads and the Executive Committee of the Imam Khomeini's Order (EIKO). Some core recommendations for pursuing an IO campaign with or simply against Iran, include the following:

- Doing business in Iran: An IO campaign pointing out the dangers of business relationships and transactions with Iran, including Iranian companies and financial institutions, will dissuade foreign banks from entering into correspondent relationships, believing they are

being used to bypass international AML risk mitigation practices. This should point out the traditional shortcomings identified by the World Trade Organization and other international bodies, and include a campaign to undermine requests by Iranian financial institutions to open branches and subsidiaries in foreign jurisdictions. There should also be pressure for greater oversight of correspondent banking between Iranian financial institutions and foreign entities. A general lack of AML/CT controls and basic due diligence is lacking.

- Additionally, an IO campaign could point out that Iran's financial regulations related to the supervision of non-governmental organizations and charities, both Iranian and foreign, fall short of international standards. Iran's financial regulations are not part of a comprehensive counter-terrorism finance law, and Iran does not participate in the Financial Action Task Force (FATF) and is not a member of the Egmont Group. Iran has taken small steps, such as enacting weak anti-money laundering legislation that requires financial institutions to enforce customer identification and record keeping requirements. Iran should be pressed to join several UN conventions and protocols relating to counter terrorism, including the International Convention for the Suppression of the Financing of Terrorism.

- An IO campaign should make the link between the shortcomings of Iran's financial system and the inability of the international community to identify and disrupt the flow of Iranian money to terrorist proxies in the Middle East, South Asia, and beyond. Illicit money flows also reflect insufficient border control programs and a lack of effective multi-lateral counter terrorism initiatives with all the countries on Iran's borders.

- Restrictions on the freedom of expression, requirements of Internet service providers, web sites and blogs to register with the government and gain approval from the Ministry of Culture and Islamic Guidance; intrusive government monitoring and censorship of the Internet and the press; and even the presence of terrorist groups on Iranian territory and/or the use of Iran as a safe haven for Sunni extremist financiers should be better exploited.

- Terrorists from across the Islamic world travel to Iran to raise money, partly because there is no law in Iran that prohibits terrorist fundraising. The Iranian government provides money to the families of martyrs, free oil shipments that are sold to generate revenue (Afghanistan), and other forms of support, but don't recognize UN Security Council resolutions calling for the freezing of assets of designated companies, individuals, etc. Also, charitable and non-governmental organizations in Iran are not required to declare their sources of funding, which can include cash donations.

- Finally, a comprehensive IO campaign against the ITN must carry out sustained covert influence to shape how the world views threats emanating from Iran and its external revolutionary agenda. The objective would not be to win the war of words between Iran and the United States; most polls clearly show that Iran, its theocratic form of government and its expansionist tendencies are unpopular in most of the world, even in the Middle East. However, there are other ways of using covert influence against the ITN. A campaign against Iran's covert action programs in the Persian Gulf States should stress the destabilizing impact of Iranian subversion since 1979. In the past few years alone, Iranian officials have been expelled from numerous Gulf countries

Thank you for the opportunity to share these views.

CONGRESSIONAL TESTIMONY

Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terror
Prepared Statement of Elizabeth Rosenberg

Center for a New American Security

September 9, 2015

Testimony before the U.S. House of Representatives Financial Services Committee

Prepared Statement of Elizabeth Rosenberg
Senior Fellow and Director, Energy, Economics, and Security Program
Center for a New American Security

Chairman Fitzpatrick, Vice-Chairman Pittenger, Ranking Member Lynch, and distinguished members of the Task Force to Investigate Terrorism Financing, thank you for the opportunity to testify before you today on U.S. efforts to stop the financing of terrorism. Particularly given the evolving and complex nature of the global financial system, the dynamic nature of terrorist threats and the growing diffusion and autonomy of terrorist cells internationally, a whole-of-government approach is needed to combat terrorism. Stemming the flow of terrorist financing is a critical part of this effort. I applaud the work of this Task Force to address this threat and strategies to protect the integrity of our financial system from such abuse.

While serving in the Treasury Department, I had the honor of working with dedicated, creative and diligent public servants on policy initiatives and diplomatic engagement to counter the financing of terrorism (CFT). We worked closely with colleagues at the Departments of State, Justice, Homeland Security, and Defense, as well as with skilled analysts in the Intelligence Community and law enforcement agencies. Our coordination occurred in regular interagency meetings, as well as in interagency fusion and threat finance cells, and was supported by interagency liaisons and detailees among federal agencies.

We also worked closely with our counterparts in a variety of foreign countries. Treasury officials working to combat terrorist financing have traveled extensively to engage in "financial diplomacy" around the world.[1] By engaging counterpart policymakers and regulators, central bank governors, major financial institutions, and other financial sector stakeholders in high-risk jurisdictions, they have explained terrorist financing risks and painstakingly built an international, coordinated effort to combat such risks. This collective effort reflects the belief that broad, interagency and international efforts are required to counter terrorist threats. Diplomacy, foreign and technical assistance, sanctions, financial oversight and regulatory policy, intelligence sharing, legal enforcement actions, military strikes, and other security activities are all part of the strategy to combat terrorism and its financing.

I will focus my remarks today on three areas of policy critical to CFT efforts. They are 1) efforts to strengthen financial system integrity and transparency; 2) the United States' offensive strategy for targeting terrorist financing; and 3) initiatives for multi-lateralizing this work with counterparts abroad.

Strengthening Financial System Integrity and Transparency

[1] "Treasury Concludes Three Weeks of Global Engagement with Governments, Private Sector on Iran," U.S. Department of the Treasury, press

Some of the most important defenses against both terrorist financing and indeed the conduct and facilitation of terrorism generally, are rigorous know-your-customer (KYC) practices, particularly in the corporate formation process, and rigorous customer due diligence (CDD) practices. Without such practices financial institutions can fall victim to abuse and become wittingly or unwittingly involved in the provision of material support to criminals and terrorists. This results in reputational harm and expensive enforcement actions. But with robust KYC and CDD measures in place, financial institutions can detect and arrest terrorist-linked financial flows and suspicious activity. Financial policy makers and regulators, along with the law enforcement community, together have responsibility for making sure that requirements for such safeguards in the U.S. financial system are strong and upheld.

Suspicious activity reporting by banks and other financial institutions is often produced as a result of rigorous KYC and CDD practices. Along with intelligence reporting and analysis on financial movements by terrorist-linked entities, this body of information is critical in our government's efforts to stem terrorist financing and activity. It may be used by the Treasury Department for sanctions designations, by law enforcement investigators in bringing cases against terrorists and criminals, and by our Department of Defense in understanding and countering these threats abroad.

This Task Force heard testimony from Cyrus Vance in June, making clear that it is far too easy to form a shell company in the United States through which terrorism supporters and criminals can conceal and carry out their illicit activity.[2] And you may also be aware of similar views expressed by others, including former Under Secretary of Treasury David Cohen, who said that it is "untenable" for the United States to tolerate the risk posed by shell companies in our financial system and has called repeatedly for tougher due diligence and beneficial ownership data gathering requirements.[3] The existence of shell companies is a weak link in our efforts to combat the financing of terrorism, and to combat criminal activity broadly. Addressing such deficiencies is an urgent priority to strengthen and increase the resiliency of our financial system to such threats. It will also bring the United States into better standing in the international community, addressing a failing international technical evaluators pointed out publicly almost a decade ago.[4]

The first step in strengthening the U.S. financial system's resilience to abuse by illicit activity is tougher KYC and CDD programs. The Treasury Department and others in the administration are working on new policy in these areas, finalizing a new rule on the conduct of CDD. They are also working with Congress to strengthen information disclosure requirements about beneficial owners in the corporate formation process as part of the FY2016 budget, a critical step that would improve sanctions enforcement and identification of criminals and terrorists and may be useful in identifying the source of malicious

[2] Cyrus R. Vance, Jr., New York County District Attorney, "Written Testimony of New York County District Attorney Cyrus R. Vance, Jr. Before the U.S. House of Representatives Task Force to Investigate Terrorism Finance," Statement to the Task Force to Investigate Terrorism Finance, U.S. House of Representatives, June 24, 2015, 2-3, http://financialservices.house.gov/uploadedfiles/hhrg-114-ba00-wstate-cvance-20150624.pdf.
[3] U.S. Department of Treasury, Under Secretary for Terrorism and Financial Intelligence David S. Cohen, "Remarks of Under Secretary Cohen at the ABA/ABA Money Laundering Enforcement Conference" (ABA/ABA Money Laundering Enforcement Conference, Washington, November 11, 2014), http://www.treasury.gov/press-center/press-releases/Pages/jl2692.aspx.
[4] Financial Action Task Force, "Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: United States of America" (FATF, June 2006), http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf.

cyber activity as well. This effort will also extend anti-money laundering (AML) and CFT requirements to corporate formation agents.

Other areas of the administration's work with Congress to strengthen the integrity of the financial system include clarifying rules for suspicious activity reporting by financial institutions to give the institutions greater comfort and incentive to be forthcoming about reporting concerning activity. And the Treasury Department is also working with partners in the administration considering the extension of AML/CFT requirements to more unregulated financial entities, including investment advisors and real estate agents, the appropriate methods for requirement of reporting on new digital currency use. Treasury is also coordinating with law enforcement agencies and the states to urge greater attention at the local level to the collection and verification of beneficial ownership data for legal entities. These are all steps in the right direction, but require direct support from policymakers, such as the legislators on this task force, who understand the national security urgency of such new measures and can help bring them, and other efforts, to fruition.

Robust information sharing on terrorist financing is another crucial area of effort to CFT and protecting the financial system. Though information-sharing challenges exist at many levels, one significant challenge in this arena is the barrier that national data privacy laws present, preventing the sharing of data across borders even within one multinational financial institution. When such laws make it difficult for different divisions within the same bank, for example, to exchange information on customers or beneficial ownership data, it can make it difficult to identify sanctions evasion or criminal activity. In turn, these barriers hamper the sharing of investigative leads, suspicious activity reports (SARs), and forensic accounting data with government authorities. Such information would help government authorities track the source of terrorist networks, identify deep-pocket donors, charities, and facilitators, and spot sanctions evasion. The barriers to information sharing also hinder the work of government officials in identifying more nodes in terrorist networks and links between terrorist groups and criminal enterprises. If customer information were more easily shared across national jurisdictions, it would better help financial institutions and government authorities to understand emerging methodologies in raising and moving illicit money, including transactions in digital currency, and the scope of tools that can be employed to counter such new strategies.

The interests of the public and private sector are very closely aligned when it comes to preventing terrorist abuse of the financial system. All parties can benefit when they share information. In fact, when they do so voluntarily and in the spirit of cooperative efforts to combat a common enemy, it can lead to better outcomes for financial inclusion and protect legitimate financial activity. High-risk financial flows or institutions for terrorist financing, including remittances and money transmitters, must be carefully policed for illicit financial activity and simultaneously protected for law-abiding people who have few other choices for conducting banking activity. Excellent information sharing between the public and private sector directly contributes to both of these goals.

There is also an important role for non-governmental, non-commercial institutions and civil society organizations in information sharing relevant to terrorist financing. Charities, community organizations,

even arts and cultural associations, may have knowledge of terrorist funds movements. For example, knowledge of Syrian and Iraqi antiquities stolen and sold on the black market by ISIS, or wildlife stolen and trafficked in Africa, or sales of counterfeit goods by Hezbollah, may be usefully shared by civil society groups with authorities.[5] Creating secure, consistent channels for outreach between these groups and government is the challenge, however, particularly when terrorist methodologies evolve and spread quickly with use of the Internet.

To be sure, sharing information related to terrorist use of the financial system, particularly between government and the private sector, is challenging. There are myriad civil liberties concerns and financial inclusion challenges. And when the flow of information is from the private sector to government, there are also considerations associated with protecting proprietary information and products, intellectual property, and competition. Nevertheless, all parties have an interest in understanding and countering emerging and evolving terrorist threats and how they may use the financial system. External advisory boards for federal agencies, regular industry outreach by financial policymakers and regulators, and the establishment and maintenance of advisory relationships with outside experts holding security clearances can all help to promote public sector-private sector information sharing. And to facilitate better law enforcement and compliance on international CFT matters, policymakers must urgently contemplate new strategies for facilitating the flow of SARs and beneficial ownership data across national borders.

Expanding Offensive Activities to Target Terrorist Financing

Another area in which the United States can do more to counter the financing of terrorism is sanctions designations. By more aggressively targeting terrorist financiers and facilitators, including couriers, banks, exchange houses and other entities that may be engaged in financial or material support for terrorism, U.S. authorities will make it more difficult for such people to conduct their activities. Crucially, to the extent that such designations can make public the methods used by terrorists and their supporters to provide financial and material support, they will help the private sector not only to bar entry to terrorists but also to know the illicit strategies by which they abuse the financial system and legitimate businesses. With the dispersion and autonomy of terrorist cells globally, it is challenging for banks and regulators, to say nothing of commercial entities that do not have access to classified intelligence, to keep pace with the evolving tactics terrorists use to raise money. These tactics increasingly extend far beyond traditional donor activities to other diverse criminal enterprises, such as extortion, taxation, and counterfeiting, among others.

Particularly in the near and medium term, as Iran receives economic benefits from the lifting of sanctions under the nuclear accord it signed in July with the P5+1, this state sponsor of terror will have more funds to apply to its terrorist proxies in the region. The U.S. Treasury Department estimates that about $50 billion of Iran's foreign exchange reserves to be unfrozen under the accord will be immediately accessible

[5] Matthew Levitt, "Hezbollah: Party of Fraud," *Foreign Affairs*, July 27, 2011, https://www.foreignaffairs.com/articles/2011-07-27/hezbollah-party-fraud.

to Iran.[6] Iran will have to dedicate these reserves to defending its currency and to its most pressing economic needs. Nevertheless, Iran presumably will be able to send more money to its terrorist proxies in the region, even as an economic windfall under the nuclear deal may emerge slowly.[7]

Any marginal additional amount of Iranian funding for terrorism is too much. The United States must take an aggressive posture to combat expanding terrorist threats originating in the volatile Middle East, elsewhere in the world, and of course at home. This will demand a robust and coordinated effort, as I described previously. The Treasury Department has sanctioned around 50 Iranian-linked entities under terrorism authorities since the start of the interim nuclear agreement,[8] and Treasury Secretary Jacob Lew has pledged to aggressively enforce terrorism sanctions on Iran going forward.[9] Congress should hold the administration accountable on this pledge, demanding highest-level administration commitment to expand counterterrorism and CFT activities. This is most crucial in the area of gathering and analyzing intelligence on proliferating terrorist threats, issuing from Iran and elsewhere. Congress should also allocate additional resources to the Treasury and State Departments for enforcing the growing number of new sanctions authorities, to the Defense Department to launch covert actions or other security measures, and to law enforcement for expanded focus on investigations and prosecutions of any citizen who would support terrorism threatening our homeland.

Additional near-term steps that Congress should take to improve our country's capabilities and drive to combat terrorist financing include the creation of new sanctions, in coordination with the administration, to combat the Iranian terrorist threat. Some argue that launching new counterterrorism financial sanctions now will undermine the nuclear deal, giving Iran cause to believe that the United States is acting in bad faith and imposing sanctions removed under the nuclear deal under a new guise. This could occur. But policymakers can minimize this effect by carefully constructing new authorities that focus pointedly on Iran's support for terrorism and that are not tied to implementation or performance of the nuclear deal.

New sanctions authorities should specifically address the malign effect of Iran's sponsorship of terrorism on regional stability and demand a rigorous new focus on exposing and punishing support for terrorism by IRGC entities and individuals. By expanding the sanctions focus on IRGC entities, U.S. policymakers may help to put off-limits to responsible international investors in Iran those firms in Iran's construction, telecommunications, and airline sectors, among others, that are tainted with association to the IRGC. Congress could also call upon the Financial Crimes Enforcement Network (FINCEN) to revise the 2011

---

[6] Adam Szubin, U.S. Department of Treasury, Acting Under Secretary of Treasury for Terrorism and Financial Intelligence, "Written Testimony of Adam J. Szubin, Acting Under Secretary of Treasury for Terrorism and Financial Intelligence United States Senate Committee on Banking, Housing, And Urban Affairs," Statement to the Committee on Banking, Housing and Urban Affairs, U.S. Senate, August 5, 2015, http://www.treasury.gov/press-center/press-releases/Pages/jl0144.aspx.
[7] Patrick Clawson, "Iran's 'Frozen' Assets: Exaggeration on Both Sides of the Debate," The Washington Institute for Near East Policy, September 1, 2015, http://www.washingtoninstitute.org/policy-analysis/view/irans-frozen-assets-exaggeration-on-both-sides-of-the-debate.
[8] U.S. Department of Treasury, "Specially Designated Nationals List," http://www.treasury.gov/ofac/downloads/ctrylst.txt.
[9] Jacob J. Lew, U.S. Department of Treasury, Secretary of Treasury, "Testimony of Treasury Secretary Jacob J. Lew before the Senate Foreign Relations Committee on the Iran Nuclear Agreement," Committee on Foreign Relations, U.S. Senate, July 23, 2015, http://www.treasury.gov/press-center/press-releases/Pages/jl0129.aspx.

regulatory action it proposed under section 311 of the USA PATRIOT Act targeting Iran.[10] FINCEN should elevate concerns about Iran's support for terrorism in a new notice of proposed rulemaking. Such actions will, in practice, affirm existing legal authorities that regulators can already use to target terrorist financing. Nevertheless, they can add more specificity and scope to current counterterrorism sanctions authorities and signal a serious, renewed focus on combatting such threats. This will be important as an indication to terrorists as well as to U.S. allies, who should act in parallel to the United States to expose and constrain Iran's support for terrorism.

International Engagement to Expand Effectiveness in the Targeting of Terrorist Financing

A critical counterpart to new domestic policies and authorities for CFT are new measures to coordinate with foreign counterparts on this threat. Indeed, this is one of the oldest and most robust areas of activity of the Treasury Department's division of Terrorism and Financial Intelligence. Former Under Secretary Stuart Levey, the first leader of this division, traveled extensively to foreign banks and regulators to discuss the threat of illicit finance and the need to eradicate it from the formal financial sector.[11] Additionally, the Treasury Department, and the U.S. government broadly, have been long-time supporters of, and leaders within, the Financial Action Task Force (FATF), the global body that sets international standards for AML and CFT safeguards and works for their international application. This organization is significantly responsible for helping foreign countries to put in place the policy and legal framework for CFT, and crafting strategies to actively combat it within their jurisdictions.

U.S. officials should renew and expand their efforts to build capacity among foreign governments to identify, investigate and go after terrorist financing. Our government should help partners to strengthen their financial systems and make them more resilient to abuse by terrorists. This includes helping counterpart policymakers to strengthen their KYC and CDD requirements. Additionally, it includes the encouragement of greater electronic financial activity, instead of cash-based economic activity that is more easily used by criminals and terrorists to move money. It also includes helping partners to strengthen laws that criminalize the financing of terrorism or support foreign fighters and terrorist activities. Kuwait, which only recently criminalized the financing of terrorism, one of the last countries to do so,[12] can do much more to act on these new authorities and combat terrorism in its jurisdiction. And Kuwait is hardly alone as a state in need of much greater action in this arena.

When the United States' foreign partners are more capable of combatting terrorism financing, they make much stronger partners in investigating international terrorist financing, sharing information in a secure manner, and collaborating with us in the targeting of terrorist financiers and facilitators with sanctions and law enforcement actions. When terrorist groups raise money largely from criminal and terrorist

---

[10] U.S Department of Treasury, "Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations - Imposition of Special Measure Against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern," November 28, 2011, http://www.gpo.gov/fdsys/pkg/FR-2011-11-28/pdf/2011-30331.pdf.
[11] Rachel L. Loeffler, "Bank Shots: How The Financial System Can Isolate Rogues," *Foreign Affairs*, March/April 2009, https://www.foreignaffairs.com/articles/north-korea/2009-03-01/bank-shots.
[12] Celina B. Realuyo, "Combating Terrorist Financing in the Gulf: Significant Progress but Risks Remain," (The Arab Gulf States Institute in Washington, January 26, 2015), 6.

enterprises within their own territory, a notable practice of ISIS,[13] U.S. authorities have limited means to combat illicit money flows. We are reliant on the capabilities and political will of partners to combat such threats, and must also resort to physical means to destroy some of their revenue-generating assets. With ISIS, coordination with foreign counterpart law enforcement bodies, such as Interpol and Europol; local financial regulatory and law enforcement authorities, in Turkey, for example; as well as the private sector, can collectively help to hinder the flow of financial support for the organization outside of its territory. Security cooperation with Turkey, including the ability to use airbases there, and coordinating bombing strikes on ISIS nodes with other security partners, can help to target and destroy ISIS' criminal money-making enterprises.

Given the difficulty in sharing financial data, including SARs, across national boundaries, a new policy initiative to establish greater information flow across jurisdictions is a major priority. This will require legislative change in foreign jurisdictions, which can be bolstered and encouraged by FATF, as well as through diplomacy by U.S. administration officials and financial services leaders in Congress. U.S. financial services sector policymakers could also consider a safe harbor framework between the U.S. and partner financial jurisdictions to facilitate the flow of customer banking information that will directly support efforts to identify and counter illicit finance threats. A good goal for cross-border information sharing would be to significantly ease the transfer of beneficial ownership data of customers between banks with correspondent relationships in different jurisdictions. This will help U.S. banks, and indeed responsible multinational institutions more broadly, to know which customers they should take on, who may be evading sanctions, and which transactions to flag in reporting to regulators. Additionally, it will help them make more informed decisions to manage business in high-risk jurisdictions or with high-risk classes of customers, including money services businesses.

Furthermore, the $5 billion Counterterrorism Partnership Fund, established last year, is an excellent mechanism to support U.S. investment in foreign partners to combat terrorist financing. No money was allocated to this fund in the 2015 budget, but money dedicated to the Defense and State Departments under this fund for the 2016 budget year could go a long way to support U.S. core counterterrorism interests, including countering terrorist safe havens, countering the flows of foreign fighters, as well as attacking Iran's support for terrorism, including through proxy groups in the Middle East.

Conclusion

Congress has an important role to play in countering the diverse, proliferating and increasingly diffuse terrorist threats confronting our country. Legislators should lead the effort to close some of the most concerning gaps in our CFT policy and regulatory architecture, particularly when it comes to the issue of CDD and collection and sharing of beneficial ownership data. They should also rigorously oversee the aggressive implementation and enforcement of targeted measures to attack terrorist financing nodes, one of the most critical tools in our national security kit. Engaging in these activities will ensure that the

[13] Matthew Levitt, "The Islamic State's Backdoor Financing," The Washington Institute of Near East Policy, March 24, 2015, http://www.washingtoninstitute.org/policy-analysis/view/the-islamic-states-backdoor-banking.

United States is a clear leader in protecting the global financial system from illicit activity and advance vital counterterrorism efforts for the security of our homeland.

Thank you for the opportunity to testify today. I look forward to answering any questions you may have for me.

Biography

Elizabeth Rosenberg
Senior Fellow and Director, Energy, Economics and Security Program, Center for a New American Security

Elizabeth Rosenberg is a Senior Fellow and Director of the Energy, Economics and Security Program at the Center for a New American Security. In this capacity, she publishes and speaks on the national security and foreign policy implications of energy market shifts and the environmental effects of climate change. She has testified before Congress on energy issues and been quoted widely by leading media outlets in the United States and Europe.

From May 2009 through September 2013, Ms. Rosenberg served as a Senior Advisor at the U.S. Department of the Treasury, to the Assistant Secretary for Terrorist Financing and Financial Crimes, and then to the Under Secretary for Terrorism and Financial Intelligence. In these senior roles she helped to develop and implement financial and energy sanctions. Key initiatives she helped to oversee include the tightening of global sanctions on Iran, the launching of new, comprehensive sanctions against Libya and Syria and modification of Burma sanctions in step with normalization of diplomatic relations. She also helped to formulate anti-money laundering and counter-terrorist financing policy and oversee financial regulatory enforcement activities.

From 2005 to 2009 Ms. Rosenberg was an energy policy correspondent at Argus Media in Washington D.C., analyzing U.S and Middle Eastern energy policy, regulation and trading. She spoke and published extensively on OPEC, strategic reserves, energy sanctions and national security policy, oil and natural gas investment and production, and renewable fuels.

Ms. Rosenberg studied energy subsidy reform and Arabic during a 2004-2005 fellowship in Cairo, Egypt. She was an editor of the Arab Studies Journal from 2002-2005 and researched and wrote on Middle Eastern politics at the Council on Foreign Relations in 2003. She received an MA in Near Eastern Studies from New York University and a BA in Politics and Religion from Oberlin College.

Testimony of Louise Shelley, Omer L. and Nancy Hirst Endowed Chair
Director, Terrorism, Transnational Crime and Corruption Center (TraCCC)
University Professor, School of Policy, Government and International Affairs
George Mason University, Arlington, Va.

To the Task Force to Investigate Terrorism Financing *Could America Do More? An Examination of U.S. Efforts to Stop the Financing of Terrorism*, Wednesday September 9, 2015

EXECUTIVE SUMMARY:

I) We need to discuss the concept of ***the business of terrorism*** **and move away from the concept of** ***terrorist financing*** for the following reasons:
   a) *Terrorist financing* looks at what has been done and is being done to fund a terrorist organization, it is reactive rather than proactive.
   b) The *Business of Terrorism* examines more broadly the way terrorists generate funds and solicit personnel for future activity.
   c) The *Business of Terrorism* looks at terrorists' marketing strategies, targets of opportunity and other business strategies.
   d) *Terrorist financing* fails to address the fact that terrorists are acting like business people and need to be countered as business competitors.

II) **Almost all terrorism these days is funded by crime,** although much of transnational crime remains independent of terrorism. Therefore we need to:
   a) Stop stovepiping the separate responses to crime and terrorism. Instead, we need to integrate our analyses and countermeasures. This is being done successfully by the Los Angeles and New York Police Departments.
   b) We need to focus on more than the drug trade and concentrate on the **smaller scale illicit trade that supports so much terrorism** in the US, Europe, and North Africa (i.e. one of the Kouachi brothers responsible for the Charlie Hebdo massacre in Paris traded in counterfeit Nikes and cigarettes, similar crimes are found as crucial support to terrorists by NYPD).
   c) Terrorists use corruption to execute their business activities, just as organized crime always has. **We need to integrate analyses of corruption into crime and terror analyses.**

III) Private-public partnerships are key in addressing the business of Terrorism:
   a) Businesses have insights on how to combat business competitors, these insights need to be shared with governmental personnel who have less experience with business.
   b) They collect intelligence on terrorist financing derived from diverted and counterfeit examples of their commodities. This information has been used successfully by Interpol and American law enforcement to combat terrorist funding.

IV What needs to be done?

a) **Focus on Terrorist business, rather than financing,** by taking an integrated view of terrorist trade in products, capitalizing on targets of opportunity, use of technology, and recruitment of personnel.

b) We need to **establish working and advisory groups with sectors of the business community whose products are likely targets of terrorists**. Many of these companies have well-established investigative units to discover illicit trade in their products. Target sectors include manufacturers of consumer goods, pharmaceuticals and cigarettes. Established mechanisms for information sharing need to be better developed.

c) **Use counter-crime and terror policing models based on LAPD and NYPD models in other major urban centers in the US**. Develop police systems in other major urban centers similar to NYPD and LAPD that allow information sharing on terrorist financing through crime. Federal agencies work closely with local government in these locales. These mechanisms need to be expanded to other cities and regions of the US.

d) **Develop more controls over cryptocurrencies such as Bitcoin and many other emerging web-based currencies** that are hard to trace and are key to the financing and trade of terrorists.

THE BUSINESS OF TERRORISM
How do terrorists function as business people?

Terrorists seek a product mix, professional services, conduct cost-benefit analyses, employ tax strategies, and exploit supply chains.[i] They seek market dominance, strategic alliances, competitive advantage, targets of opportunity, and try to employ innovation and technology effectively. They seek ways to obtain access to the best human capital through their global networks. ISIS illustrates all these concepts but it is only one of many terrorist groups that share these attributes. It is just the most successful of these.

Terrorists are always looking for new ways to fund themselves. In this way, they resemble multi-national businesses that need to diversify to survive in the global economy. To survive, they are proactive and are fluid and flexible, like the most nimble of businesses. We must appreciate their capacity as business people and not just explore their past streams of funding.

EXPLOITING COMPARATIVE ADVANTAGE

Terrorists exploit their comparative advantage. Terrorists near natural resources use these commodities to fund their activities, those near weapons stockpiles become weapons traders, and terrorists in border areas tax the cross-border flow of goods. They take advantage of their critical location. For example, Al-Qaeda, was involved in the diamond trade, particularly in Sierra Leone, Liberia, and Tanzania.[ii] The FARC and the Ejército de Liberación Nacional (National Liberation Army, or ELN) use their territorial control in different regions of Colombia to extort money and to lead attacks against energy infrastructure,[iii] such as has also been seen in Algeria and in territory controlled by ISIS and Boko Haram.

Terrorist and insurgent groups, located near populations of elephants and rhinoceroses sought for their horns and tusks are leading to the mass slaughter of these animals and irreversible damage

in ecosystems. This month's issue of National Geographic confirms earlier published research on the involvement of the Lord's Resistance Army in the illicit ivory trade, along with members of the Sudanese government,[iv] pointing to the role of both terrorists and corrupt officials in this trade. The US is the second largest importer of ivory after China. Therefore, our consumer culture is helping to fund terrorism. Only recently have some states passed laws trying to counter this illicit trade.

SECURING SUPPLY CHAINS

Terrorists share a major concern of legitimate businesses—supply chains—as they need to ensure the safe and timely delivery of goods without disruption. Terrorists are concerned with supply chains for illicit goods, such as narcotic drugs, counterfeit pharmaceuticals, and cigarettes (which are the lifeblood of many terrorist organizations), or high-value diverted goods, such as oil.

Terrorists make substantial money by controlling supply chains for delivery of their products, such as drugs, as well as by taxing the smuggling of others that pass through borders or territory that they control. The ability to tax the transit of commodities is one key to their financing. Organized crime groups' extortion of trade has been known for a significant period, which is why they are so deeply involved in ports and the trucking industry. Yet terrorist groups on many different continents also profit from exploiting supply chains and taxing trade. This insight has not merited sufficient attention from the counter-terrorism community.

Terrorists often generate revenues by taxing the supply chains that move legitimate and illegitimate products across territory they control. Through corruption of officials and application of violence, terrorist groups undermine the state presence and bolster their own in key border areas, ports, and other transport hubs. Therefore, they have learned from organized crime the

importance of controlling territory and have capitalized on the corporate world's need to move commodities long distances in the increasingly globalized economy.

SECURING PERSONNEL

ISIS has developed an effective model of international recruitment of personnel. It uses new technology such as twitter to identify potential recruits. Then it deploys geographically distinct messaging to recruit personnel to fight for it, or for women to join and provide support functions. Its well developed communications and marketing strategy in some respects mirrors that of legitimate multi-national companies.

HETEROGENEITY OF TERRORIST BUSINESSES

All terrorist groups do not function the same way in business. Cultural, historical and geographic conditions shape their approach to terrorist financing. For example, in the Middle East where trade has been at the heart of the economy since the first recorded language, trade or taxing trade is the major funding source of ISIS and other groups such as the PKK operating in the region. The long-standing growth of drugs in Afghanistan and in the Andes has contributed to a reliance on crop production and drugs in terrorist financing. In Africa, where man's dominance over animals has been a hallmark of rulers, trade in animal parts becomes an important funding source for terrorism.

Terrorists choose the crimes they will commit not only by profitability and ease of entry into this business sector, but also by the extent of competition in this sphere of criminal activity and the costs of corruption.[v] Yet determinations of risk of detection and asset loss are also associated with the calculations of the more sophisticated criminal-terrorists. Terrorists exploit their

strategic advantages, just as do legitimate business people. Understanding the comparative advantage of a terrorist group within this financing framework is key to determining their sustainability and deriving strategies to deprive them of revenues.

TERRORISTS USE CRIME TO FUND THEIR ACTIVITIES

Terrorists use crime as a means to generate needed revenues, to obtain logistical support, and use criminal channels to transfer funds. Criminals provide operational tools, such as falsified documents, new identities, and transit across borders to terrorists in need.[vi] Criminals can pay off officials, thereby providing terrorists and their commodities safe passage across borders. The criminal support structures can include either petty criminals or developed crime groups, such as the Camorra in Naples,[vii] complemented by the services of facilitators from the legitimate world, such as bankers, lawyers, and corporations that intentionally or inadvertently assist in the perpetration of terrorism.[viii] Corrupt military personnel can serve as suppliers of weapons to criminal and terrorist groups.[ix] There are also facilitators that serve the criminal world, especially drug traffickers and those moving dual-use materials.

PRODUCT MIX

Almost every known form of criminal activity has been used to fund terrorism. The choice of criminal activity reflects the geographic location of the group, its human capacity, and the profitability of the crime. Crimes are selected based on the ability to evade detection or prosecution, access corrupt officials, and obtain profits. Terrorists prey on ordinary citizens, as well as smaller and larger businesses through extortion and kidnapping. They commit fraud against legitimate financial institutions through credit card abuse and other financial

manipulation of markets.[x] Many of these illicit activities converge in supply chains and are handled by the same transport facilitators.

Apart from these high-profit and large-scale sources of criminal activity, terrorists and insurgents participate in a diverse range of criminal actions, including ones used by earlier generations of terrorists and guerillas, such as kidnapping, extortion, and bank robbery.[xi] But they also are at the forefront of technology, relying on credit crime and Internet fraud. They also use new technologies such as cryptocurrencies (such as bitcoin) to move money. The dark web is used to communicate undetected and to sell commodities.

There are many other forms of illicit activity that have become the lifeblood for terrorism, including art and antiquities smuggling, cross-border smuggling of goods, trade in counterfeit and diverted goods. Many of these crimes intersect with the legitimate economy and information from the business world can be used effectively to counter terrorism. Illicit trade in natural resources, oil, gold, and other commodities also provides funding.[xii] Commodities such as gold and diamonds are particularly sought because they have great inherent value and limited weight. Some activities, such as people smuggling and trafficking, are "dual use:" they both generate money and provide terrorist groups the ability to move operatives. Terrorists have developed a full product line that ranges from the most basic to the most sophisticated crimes.

PRIME ROLE OF SMALL-SCALE ILLICIT TRADE IN FUNDING TERRORISTS

The concept of narco-terrorism had meant that we have focused on such large financial generators as the drug trade. But increasingly smaller-scale illicit trade in commodities such as counterfeit goods, fuel, cigarettes, food, medicine, textiles and clothing are used by terrorists to fund themselves in the United States, Europe, North Africa and the Middle East. Weapons trade,

another dual-use crime is particularly prevalent in North Africa, particularly flowing out of Libya.[xiii]In aggregate, the funding from such activities is substantial, and rivals that of drugs, but has much lower risk of prosecution.

Money generated by illicit trade within the US from the illicit cigarette trade is sent out of the United States to fund terrorist groups in the Middle East. ISIS recruits from Europe can fund their voyages to join ISIS through the revenues generated from illicit trade. Recent terrorist attacks in Europe such as the recent train attack between Brussels and Paris have been perpetrated by terrorists with backgrounds in small-scale illicit trade. One of the Kouachi Brothers who killed the cartoonists of Charlie Hebdo had traded in counterfeit Nike sports shoes and smuggled cigarettes. This phenomenon is not confined to Europe. The New York Police Department (NYPD) is focusing on many smaller scale crimes, including cigarette smuggling, that are used by many diverse terrorist groups to fund themselves.

PROFESSIONAL SERVICES

Terrorists, when functioning as criminal entrepreneurs, require a variety of services.[xiv] They need accountants, bankers, and lawyers. But they also need corrupt officials and often witting and unwitting facilitators from the corporate world. Therefore, they have multiple forms of interaction with the legitimate economy. They also require professional services from the criminal world as they retain the services of human smugglers and specialists in "non-traceable communications, forgers, and money launderers."[xv] Without hiring this expertise, they cannot make their business function.[xvi]

As terrorist entrepreneurs, they are always looking for new product lines and seek to learn from regional successes in one area that can be transferred elsewhere. Therefore, the FARC, known as narco-terrorists, are really a much more diversified business that even generated income from the

exploitation of hydrocarbons. Diversification is as much a key to survival as it has been to the legitimate business world.

Terrorist businessmen share a key concern of their legitimate counterparts—the retention of professional services. These service providers allow them to move their money, corrupt needed officials, and obtain falsified documents.

WHAT CAN WE DO?

1) DEVELOP PUBLIC-PRIVATE PARTNERSHIPS, USE INSIGHTS FROM THE LEGITIMATE BUSINESS COMMUNITY

Insights from the corporate world have been valuable in understanding terrorist financing and the business of terrorism. Illustrative of this are:

Nike warned the French government that one of the Kouachi brothers who later killed the cartoonists of Charlie Hebdo was engaged in the sale of counterfeit Nikes and was transferring payment to China. This information was ignored.

Insights obtained from one multi-national cigarette company led to the tracing and freezing of money that could contribute to North Korea's WMD program. In another more recent case, American authorities were alerted that cigarettes sold en masse out of American military commissaries were being sent abroad to fund Middle Eastern terrorist groups.

Insights from a multi-national pharmaceutical company on Hezbollah funding through counterfeits of their products have raised awareness of the centrality of counterfeit prescription drugs to terrorist financing.

While the United States government has successfully used information from corporations, we have no institutionalized means to promote this cooperation. This is an underutilized approach that must be expanded.

Apart from the intelligence corporations collect, many have strong analytical teams that allow them to see trends and patterns in terrorist financing. We have an office of private partnerships in Homeland Security but we do not have strong corporate advisory bodies working with DHS or with the other agencies responsible for countering terrorist financing. Some are already working

with Interpol on joint programs that help the global fight, but we need programs tailored to promote corporate partnerships in the US. This gap must be closed. **Public-private partnerships are key in creating a counter-terrorism approach.**

2) REPLICATE LAPD AND NYPD MODELS THAT FOLLOW THE CRIME AND MONEY OF TERRORISTS

Replicate successful law enforcement models to other American locales

Both New York City and Los Angeles because of their size, economic strength and diversified economies and populations are important funding sources for terrorism. Los Angeles was targeted by the Millennium bomber and New York suffered the devastating consequences of 9/11. Both have set up highly successful programs, combining their resources against crime and terrorism to follow the money connected to terrorism. In my book, *Dirty Entanglements: Corruption, Crime and Terrorism*, I discuss the major criminal case initiated by LAPD that targeted a car theft ring in Los Angeles that helped fund Basayev who was responsible for one of the world's most deadly terrorist attacks in Beslan, Russia. Discussions with leading personnel in the departments reveal that this approach is still successfully being used to target terrorist financing and business. This approach needs to be expanded to other major US cities and used on a regional perspective rather than in just select urban areas.

3) TARGET ILLICIT TRADE IN CONSUMER GOODS

The limited penalties attached to trade in consumer goods such as counterfeit pharmaceuticals, food, alcohol, cell phones, cigarettes have made these important growth areas for terrorist

revenues. We need to prioritize these areas in counter-threat finance. We also need to focus on the convergence of these forms of illicit trade with other sources of terrorist financing—drugs, wildlife, human smuggling and trafficking. By focusing on network analysis and convergence of different forms of crime, we can make efficient use of existing resources.

4) TARGET TERRORIST FACILITATORS

Targeting these facilitators should be a much more central focus on US counter-terrorism efforts—accountants, money launderers, transport specialists. Some are even able to travel to the US and buy property here because we do not effectively coordinate our counter-measures against identified terrorist facilitators.

5) REGULATE CRYPTOCURRENCIES

The rise of Bitcoin and other unregulated currencies in the virtual world facilitates this trade. Cryptocurrencies are increasingly being used for payment on the web and on the dark web, making traceability of transactions more difficult. These currencies will facilitate the illicit activities of non-state actors as well as some corporate actors who choose to evade regulation. The possibility of so much international financial activity outside of state regulation is a force in favor of the expansion of illicit trade. **Therefore, legislation must be developed rapidly to enhance regulation of cryptocurrencies.**

6) SUPPORT RESEARCH TO IDENTIFY NEW TRENDS IN TERRORIST FINANCE AND BUSINESS

We presently have too limited independent research on the trends in terrorist financing and the development of terrorist business. Much of it is focused on a specific region or commodity, whereas the financing spans continents and the trade converges with many different products. A basic understanding of these phenomena is a necessary prerequisite for formulating effective policies to counter them. **There needs to be governmental support of independent broad fundamental basic research and the training of researchers from different disciplines to support this complex problem. This could be done through the NSF or other government agencies. Other mission agencies should fund basic research directly related to their targeted efforts.**

---

[i] For more in depth analysis of this see Louise I. Shelley, *Dirty Entanglements: Corruption, Crime and Terrorism* (Cambridge: Cambridge University Press, 2014), 173-217.

[ii] Global Witness, "For a Few Dollars More: How al Qaeda Moved into the Diamond Trade," April 2003, http://www.globalwitness.org/library/few-dollars-more; Greg Campbell, *Blood Diamonds: Tracing the Deadly Path of the World's Most Precious Stones* (Boulder, CO: Westview Press, 2002); Douglas Farah, *Blood from Stones: The Secret Financial Network of Terror* (New York: Broadway Books, 2004).

[iii] Frédéric Massé and Johanna Camargo, "Actores Armados Ilegales y Sector Extractivo en Colombia," V informe del Centro Internacional de Toledo para la Paz (CITpax) Observatorio Internacional, 2012,49 http://www.toledopax.org%2Fuploads%2FActores_armados_ilegales_sector_extractivo.pdf.http://www.askonline.ch/fileadmin/user_upload/documents/Thema_Wirtschaft_und_Menschenrechte/Bergbau_Rohstoff/Gold/Actores_armados_ilegales_sector_extractivo.pdf.

[iv] Bryan Christy, "Tracking Ivory," National Geographic, September 2015, 30-59; Kasper Agger and Johnathan Hutson, Kony's Ivory: How Elephant Poaching in Congo Helps Support the Lord's Resistance Army," June 3, 2013, http://enoughproject.org/reports/konys-ivory-how-elephant-poaching-congo-helps-support-lords-resistance-army.

[v] *Fondeo del terrorismo*, *Infolaft*, 1, no.4, 2009, 10–15, reveals that FARC's financial records calculated their expenditures for corruption as a cost of business.

[vi] C. J. de Poot and A. Sonnenschein, *Jihadi Terrorism in the Netherlands* (The Hague: WODC, 2011), 109–10.

[vii] Roberto Saviano, *Gomorrah,* trans. from the Italian by Virginia Jewiss (New York: Farrar, Straus, and Giroux), 2007, 181–86.

[viii] Mark Pieth, ed., *Financing of Terrorism* (Dordrecht, Netherlands: Kluwer Academic, 2003); Nikos Passas, "Terrorism Financing Mechanisms and Policy Dilemmas," in *Terrorism Finance and State Responses: A Comparative Perspective,* ed. Jeanne Giraldo and Harold Trinkunas

(Stanford, CA: Stanford University Press, 2007), 30, which discusses how the 9/11 hijackers used the established banking system. The nuclear proliferation of the A. Q. Khan network was facilitated by businessmen in Europe. Rebekah K. Dietz, Illicit Networks: Targeting the Nexus between Terrorists, Proliferators and Narcotraffickers, (Monterey, CA: U.S. Naval Post Graduate School, 2010), http://www.dtic.mil/dtic/tr/fulltext/u2/a536899.pdf; *IISS Nuclear Black Market Dossier: A Net Assessment* (London, 2007), 43–64, http://www.iiss.org/publications/strategic-dossiers/nbm/nuclear-black-market-dossier-a-net-assesment/.

[ix] Illustrative of this is the Cambodian military. See David Capie, "Trading the Tools of Terror: Armed Groups and Light Weapons Proliferation in Southeast Asia," in *Terrorism and Violence in Southeast Asia: Transnational Challenges to States and Regional Stability,* ed. Paul J. Smith (Armonk, NY: M. E. Sharpe, 2005), 191.

[x] Matthew Levitt and Michael Jacobsen, *The Money Trail: Finding, Following and Freezing Terrorist Finances,* Policy Focus 89 (Washington, DC: Washington Institute, November 2008), 50–51, http://www.washingtoninstitute.org/policy-analysis/view/the-money-trail-finding-following-and-freezing-terrorist-finances, and Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Columbia University Press,2002), 63–65; de Poot and Sonnenschein, *Jihadi Terrorism in the Netherlands,* 111.

[xi] R. T. Naylor, "The Insurgent Economy: Black Market Operations of Guerrilla Organizations," *Crime, Law and Social Change 20, no. 1 (1993): 13, 20.*

[xii] For a discussion of the underworld of gold, see R. T. Naylor, *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, rev. ed. (Ithaca, NY: Cornell University Press, 2004), 196–246; for extractive industries, such as oil, see Massé and Camargo, "Actores Armados Ilegales y Sector Extractivo en Colombia."

[xiii] Global Initiative on Transnational Crime, "Libya: Criminal Economies and Terrorist Financing in the Trans Sahara," May 2015, http://www.globalinitiative.net/libya-criminal-economies-and-terrorist-financing-in-the-trans-sahara/ ;International Crisis Group, "Tunisia's borders: Jihadism and Contraband", Middle East/North Africa Report, N°148, (2013) 31 http://www.crisisgroup.org/~/media/Files/Middle%20East%20North%20Africa/North%20Africa/Tunisia/148-tunisiasborders-jihadism-and-contraband-english.pdf

[xiv] Sherzod Abdukadirov, "Terrorism: The Dark Side of Social Entrepreneurship," *Studies in Conflict and Terrorism* 33, no. 7 (2010): 603–17; Douglas Farah, "Fixers, Super Fixers, and Shadow Facilitators: How Networks Connect," 2012, http://www.strategycenter.net/docLib/20120423_Farah_FixersSuperFixersShadow.pdf.

[xv] *Organised Crime in Australia Key Trends 2008*, 2, http://www.crimecommission.gov.au/publications/organised-crime-australia/organised-crime-australia-2008-report; Farah, "Fixers, Super Fixers, and Shadow Facilitators."

[xvi] For an analysis of an Auckland, New Zealand, facilitator for organized criminals and terrorists, see "Offshore Registration Business Halts Operations," June 28, 2011, http://www.reportingproject.net/occrp/index.php/en/ccwatch/cc-watch-indepth/930-offshore-registration-business-forced-to-halt-operations.

American Gaming Association

Best Practices for

Anti-Money Laundering Compliance

December 2014

Table of Contents

BACKGROUND 3
RISK ASSESSMENT 5
State Regulatory Requirements 5
Gaming Volume and Character 5
Range of Financial Services 5
Characteristics of Certain Games 5
Country Risk 6
Politically Exposed Persons (PEPs) 6
Patron Behaviors 6
Patron Characteristics 6
BSA/AML OFFICER 7
EMPLOYEE TRAINING 7
PREVENTIVE STEPS 8
CUSTOMER DUE DILIGENCE 8
Patron Identification and Verification 9
Ongoing Due Diligence 10
TRANSACTION MONITORING 11
POTENTIAL SUSPICIOUS ACTIVITY 12
SUSPICIOUS ACTIVITY REPORT REVIEW PROCEDURES 13
AUDIT PROCEDURES 15
Special Testing Procedures for CTRs 15
Special Testing Procedures for SARs 16
RECORDKEEPING AND RETENTION 16
CONCLUSION 16
GLOSSARY 17
Bank Secrecy Act ("BSA") 17
Cage 17
Chip Walk: 17
Credit 17
Front money 17
Marker 17
Monetary Instrument Log 17
Multiple Transaction Log 17
Ticket In/Ticket Out ("TITO") 17

BACKGROUND

The modern casino is an entertainment venue that offers its patrons highly regulated gaming, often combined with multiple dining options and live performances. To facilitate gaming activity, casinos ordinarily provide some financial services to their patrons. Although the vast majority of patrons visit casinos for entertainment, fun and diversion, those engaged in illegal activity may attempt to use the casino's financial services to conceal or transfer illicit wealth. To discourage such behavior and safeguard the integrity of the casino industry, casino companies have developed risk-based programs that ensure compliance with the legal requirements of the federal Bank Secrecy Act and associated anti-money laundering (AML) statutes and regulations. Risk-based compliance efforts are essential to the casino industry.

Since 1985, commercial casinos have been defined as "financial institutions" under the Bank Secrecy Act (BSA). Accordingly, they must file currency transaction reports (CTRs) when a patron either provides to the casino or takes away from the casino, more than $10,000 in currency during a casino's defined 24-hour gaming day.

Casinos also must file suspicious activity reports (SARs) when a casino knows, suspects, or has reason to suspect that a transaction aggregating at least $5,000 (i) involves funds derived from illegal activity; (ii) is intended to disguise funds or assets derived from illegal activity; (iii) is designed to avoid BSA reporting or recordkeeping requirements; (iv) uses the casino to facilitate criminal activity; (v) has no business or apparent lawful purpose; or (vi) is not the sort of transaction in which the particular patron would be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts.

More broadly, the BSA also requires casinos to design and implement risk-based AML programs that at a minimum:

- Include a system of internal controls to assure ongoing compliance;
- Internal and/or external independent testing for compliance;
- Training of casino personnel;
- An individual or individuals to assure day-to-day compliance (the "AML officer");
- Procedures for using all available information to determine:
  - when required by BSA regulations, the name, address, Social Security number, and other information, and verification of the same, of a person;
  - whether SARs need to be filed; and
  - whether any other records required under the BSA must be made and retained.
- Lastly, for casinos that have automated data processing systems, the use of automated programs to aid in assuring compliance.

In the interest of maintaining integrity of gaming, each casino company implements a comprehensive and robust anti-money laundering compliance program that identifies and mitigates its risks, and also ensures that it submits appropriate CTRs and SARs as required.

This risk-based compliance effort involves many challenges. For our patrons, casinos are generally not viewed as financial institutions, but rather are entertainment venues they enter and leave as it suits them. Many patrons are not, and never will be, personally known to casino employees. Even those patrons who become identified to the casino, because they are frequent visitors or because they require assistance with financial transactions, ordinarily have no reason to disclose to casino employees their business or professional activities. Most are, after all, at the casino to pursue entertainment. Some may not care to have their gambling activities known.

In addition, the relatively small number of patrons who may attempt to launder funds through casinos take considerable pains to conceal that purpose from the casino.

To help address these challenges, casinos have developed comprehensive risk-based programs to identify patrons whose gaming activity approaches the CTR reporting threshold. That requires the aggregation of currency transactions from several different parts of the casino: the gaming tables, electronic gaming machines, and casino cage activity, including credit (or marker limit) and front-money transactions.

To detect and report suspicious activity, casino employees and supervisors must make complex, nuanced judgments based on available information about a patron's activities. The legal standard for filing a SAR is a subjective one, applying to situations where the casinos "knows, suspects, or has reason to suspect" reportable activity. In some situations, suspicions can be confirmed or disproved only with information that is ordinarily unavailable to the casino, or by making inquiries of the patron -- for example, concerning the source of the patron's funds. Senior managers – rather than front-line employees – may be best-suited to determine whether to make such an inquiry and to conduct the inquiry. For example, the matter may involve issues that casino ordinarily would have no business reason to investigate, and some patrons may have little or no incentive to review those issues with the casino. Involvement of senior managers may facilitate the interaction with the patron, as well as signal the importance of the inquiry.

The basic framework of a BSA/AML compliance program involves the appointment of a compliance officer for the casino, the assignment of substantial employee time to compliance measures, and oversight of the compliance effort by a compliance committee, which includes representatives of the property's operations and financial staff. In order to promote a culture of compliance, casinos also may want to consider periodic updates regarding their AML programs to the Board of Directors. This line of communication could include regulatory developments, changes to the program, resources, and audit findings, among other issues.

This document is an attempt to distill the practices that a wide range of casinos and Internet gaming sites have adopted to meet these challenges. This document uses the term "casino" to cover both in-person and lawful Internet gaming venues, because the BSA/AML compliance effort applies to both.

This document is not intended to be a checklist of correct actions required of every casino or licensed Internet gaming site. In some instances, industry practices may go beyond a legal requirement established by statute or regulation, so this document should not be considered a guide to those legal requirements. In addition, a casino may have good reasons for departing from or modifying a procedure in this document, or for developing supplemental or alternative procedures, including appropriate approvals and documentation of decision-making.

The goal of this document is to provide a resource for industry and law enforcement to help guide their efforts to protect the gaming industry and the broader financial system from money launderers and others involved in illegal activity. A discussion of criteria for casino compliance programs appears at the website of the Financial Crimes Enforcement Network of the U.S. Department of the Treasury (FinCEN).

RISK ASSESSMENT

Because every financial institution is potentially at risk of being used for illegal purposes or accepting funds that were obtained illegally, casinos should identify and assess that risk in order to adopt effective measures to mitigate the risk. Many factors may be relevant to the risk assessment for a specific casino. Factors may carry different weights in different circumstances, but the risk assessment process begins with asking basic questions:

- First, what are the entry and exit points at the casino for patron funds that may come from illicit sources?
- Second, what casino departments or employees are best positioned to detect the entry and exit of such funds?
- Finally, what are characteristics of transactions that may involve illicit funds, or of patrons who are more likely to engage in suspicious activity?

In answering these questions, a casino will assess the BSA-related risks present at different parts of its business. There is no substitute for the exercise of judgment based on experience with casino transactions. Nevertheless, some basic characteristics of a casino's business can guide the assessment of the risk that a casino transaction will involve the proceeds of illegal activity or involve money laundering.

State Regulatory Requirements

Every state that grants casino licenses also imposes exacting regulation on casino operations, though specific requirements vary from state to state. State regulations define the games that can be offered and the rules of each game; they also establish what financial services can be offered and the procedures casinos must follow in providing them. State regulation also will extend to the nature of the surveillance and security measures employed at the casino.

Gaming Volume and Character

Because money launderers often deal with substantial amounts of money, they may be drawn to larger casinos with higher gaming activity, where large-value transactions are more frequent and less likely to draw attention, and where the casino's surveillance systems may have greater capacity.

For the same reasons, money laundering may be more likely to involve patrons bringing large amounts of money to a casino and playing games at higher-dollar values. Accordingly, larger gaming venues will likely need more robust AML/BSA compliance procedures. Nevertheless, smaller volume casinos must be alert to a patron's departure from ordinary patterns of play; similarly, the structuring of transactions to avoid reporting requirements can occur at any casino, regardless of business volume.

Range of Financial Services

The broader the array of financial services available at the casino (e.g., front-money deposit accounts, marker limit/credit extensions, wire transfer facilities, the receipt and issuance of negotiable instruments, the offering of safe deposit boxes), the greater the opportunity for a money launderer to exploit several different services for illicit purposes.

Characteristics of Certain Games

The rules of certain games may make money laundering more likely. For example, if a game allows patrons to bet either side of a bet (e.g., baccarat, craps or roulette), confederated patrons might bet both sides in order to launder funds through the game; similar risks may arise in the case of sports betting when a patron places a bet and another patron collects any winnings. Because poker is not a house-banked game, transactions at the poker tables may occur between

customers, rather than with the casino. Accordingly, the casino may be less likely to detect potential suspicious activity because it may not track win/loss and because cash-outs may not be frequent.

Country Risk

Some patrons with casino accounts may be deemed to present a higher risk if the casino learns that they are non-resident aliens or foreign nationals of countries that have been defined by the United States as jurisdictions of concern for narcotics trafficking, human trafficking, money laundering, terrorism, or other forms of illicit finance, or if the foreign nation has been identified as non-cooperative by the Financial Action Task Force, or if the foreign nation has been identified by Transparency International as having a high level of public corruption. [1]

Politically Exposed Persons (PEPs)

Also known as Senior Political Figures, PEPs are individuals who have been entrusted with a prominent public function, or an individuals who are closely related to such persons. PEPs and their transactions may warrant further inquiry and consideration by the casino. As appropriate, casinos will identify and assess the risks of both foreign and domestic PEPs.

Patron Behaviors

Patterns of patron behavior on the gambling floor may suggest the risk of money laundering. For example, a patron's betting activity or his financial transaction activity may increase significantly without explanation. Or a patron may appear to be coordinating his gaming with another patron or patrons (e.g., passing chips or cash back and forth) in an attempt to evade notice. Or a patron might abruptly change the methods he uses for bringing money into or out of the casino, or unexpectedly use multiple sources or multiple destinations for funds. A patron also may request multiple monetary instruments for a jackpot or wager win.

All of these behaviors may be entirely legitimate, but casinos should be attentive to the risk that they are not. Many of these considerations are detailed further in later sections of this document.

Patron Characteristics

In some instances, a casino may learn information about a specific patron which warrants further inquiry or examination of the patron's transactions. Examples of such information include formal actions against the patron by law enforcement agencies, public reports of negative information concerning the patron's integrity, or evidence that the patron is under investigation by law enforcement.

Because all of these criteria are necessarily general, individual casinos have adopted a range of implementation measures and guidelines that aim to detect, block, and report efforts to present illicit funds at casinos.

The following discussion of available compliance techniques should not be viewed as mandatory for every casino. Variations in patron mix, games offered, volume of gaming, and many other factors may render some steps listed below less applicable to a specific casino, or may warrant measures in that casino that are not identified in this document. A discussion of risk assessment factors for casinos appears at the FinCEN website, www.fincen.gov, along with responses to Frequently Asked Questions.

[1] For example, see the State Department's annual International Narcotics Control Strategy Report and regulations and guidance issued by FinCEN.

BSA/AML OFFICER

As required by the AML Program Rule, at least one employee at a casino must be designated as responsible for compliance with BSA and AML requirements, policies, and training, and should be available to other employees to consult on related questions as they arise. The BSA/AML compliance officer should be fully knowledgeable of the BSA and all related regulations.

The BSA/AML compliance officer should also understand the casino's products, services, customers, entities, and geographic locations, and the potential money laundering and terrorist financing risks associated with those factors.

The BSA/AML officer, along with the AML compliance function more broadly, should be vested with appropriate authority and resources to implement the program and assist the casino in managing risk.

EMPLOYEE TRAINING

Training on AML procedures and BSA compliance requirements should be provided to employees who have direct interaction with patrons or who handle or review patron transactions subject to the BSA. The extent and intensity of the training should vary according to the responsibilities of the employee, but should address CTR and SAR reporting and the casino's AML Program. Training materials should be updated regularly to reflect regulatory and enforcement developments under the BSA.

The following categories of employees should receive training at least once per year, and more frequently if changes in the law or circumstances require it. Following the training, the employees should be required to pass a test on the subjects covered and to sign an acknowledgement form agreeing to comply with company BSA/AML policies. Training should extend to the following general categories of employees:

- Those engaged in the operation of casino games (table games, poker, slots, keno and bingo, and sports betting), at least beginning with supervisors and above;
- Casino marketing employees, including domestic and international hosts, branch office employees, and if applicable special events employees;
- Cage employees;
- Surveillance employees;
- Audit employees, including property compliance, consolidated financial operations/Title 31 team, and Internal Audit and Fraud Department employees; and
- Senior management.

Training on BSA and AML policies of the casino also may be incorporated in job training for other casino employees, such as dealers.

The casino's AML compliance performance should be a factor in the calculation of compensation and bonus for individuals responsible for BSA compliance failures and successes.

PREVENTIVE STEPS

Casinos should consider adopting policies and procedures that have the purpose of preventing patrons from attempting transactions that have a higher likelihood of involving BSA violations or other violations of law. Such policies and procedures should be tailored to the casino's specific business, and some examples of such policies and procedures may include:

- Requiring that "ticket-in/ticket-out" (TITO) redemptions at slot machine kiosks be capped at an amount determined by the risk assessment for such transactions at that casino.
- Barring cash for cash exchanges above a threshold consistent with the risk assessment for such transactions at that casino, while permitting a senior cage official to approve such exchanges above that threshold for an appropriate business purpose (e.g., foreign currency exchanges for established patrons at reasonable levels). Such approvals should be documented.
- Declining to accept cash to purchase a casino check or other monetary instrument or to initiate a wire transfer. This would not restrict the cage from issuing a check or funds transfer for documented casino winnings, or from doing so in legitimate circumstances. Such approvals should be documented. Issuing casino checks and wires to a patron only for the amount of his/her winnings, in the absence of legitimate circumstances for such actions. In addition, a check for winnings should be payable only to the patron, and a wire transfer should be made only to the patron's account or, if applicable, to the account from which the originating wire was received. Cage management or senior management may approve making checks and/or wires payable to the patron's business or other account, or to someone other than the patron, when an appropriate business purpose for the action is documented, and/or an appropriate connection is documented between the patron and the business.
- Suspending a patron's loyalty club account and/or barring the patron if the patron's activity has generated the filing of an incomplete CTR and the patron has declined to produce the required information, until the missing information is provided. Filing a SAR for the episode should be considered. In such instances, the patron may be prohibited from further gaming and redemption of complimentaries. Senior management should have discretion on such matters if the patron is cooperative, the complimentaries were already earned, and the expectation is that acquisition of verifying identification will be facilitated by maintaining the patron relationship.
- Although not required by law, directing International Branch Offices of the casino to adhere to the same recordkeeping and reporting requirements under the BSA.
- Additionally, all traveling marketing executives, prior to travel outside the U.S. should be trained on the laws that relate to gaming and marketing for the specific jurisdiction(s) they are visiting. If a traveling marketing executive is authorized to conduct a financial transaction in an international location, the casino may also need to report the transaction under the BSA.

CUSTOMER DUE DILIGENCE

The Bank Secrecy Act requires that each casino follow a risk-based approach in developing and implementing an effective anti-money laundering program. A risk-based approach is driven by a periodic risk assessment that identifies those customers and transactions that potentially pose the greatest risk of money laundering so higher levels of scrutiny and evaluation can be applied, when appropriate. As noted above, the risk assessment allows casinos to determine and

implement proportionate controls to mitigate the different levels of risk present in differing circumstances.

Patron Identification and Verification

No front money or marker limit/credit account or safety deposit box agreement will be opened, nor will any transaction involving such services be conducted, unless the patron provides a full name, and a permanent address and (for U.S. citizens) a Social Security number (as required by law or regulation). This requirement does not apply to the establishment or use of player loyalty club accounts.

No transaction(s) known to be reportable under the BSA or AML procedures will be completed unless the individual conducting the transaction(s) provides valid, current, Government-issued photo identification and a permanent residence address.

If the patron asserts that his only permanent address is a post office box, the casino should confirm this assertion by examining available databases and acquiring the patron's attestation to this fact.

Examples of acceptable government-issued photo identification are:

- Driver's License (Domestic and Foreign)
- Passport
- Alien Registration Card
- State Issued Identification Card

A casino generally may rely on government-issued identification as verification of a customer's identity; however, if a document shows obvious indications of fraud, the casino must consider that factor in determining whether it can form a reasonable belief that it knows the customer's true identity.

In some instances, information in the casino's records will suggest that certain information on the official identification document – most often, the patron's permanent address – is no longer accurate. In those situations, if the casino is able to verify by reasonable inquiry the more recent information, and if the patron does not trigger greater scrutiny under the casino's risk assessment standards, it may wish to report the more recent information on any CTRs and SARs filed for that patron. The reason for using an address other than one on the customer's government-issued ID should be maintained in the casino's records.

If the patron is a U.S. citizen or a U.S. resident with a Social Security number, a U.S. Social Security number is also required. Patrons may verbally provide a U.S. Social Security number. If the casino knows that a previous Social Security number provided by the patron was incorrect, then the patron may be required to complete and sign a W-9 Form before any pending transaction can be completed. Casinos should consider filing a SAR if inconsistencies in identifying information are suspicious.

If a patron declines to provide a U.S. Social Security number when one is required, the casino should not complete any pending transaction with that patron. If the patron has exceeded the reporting threshold for a CTR without providing a U.S. Social Security number, a casino employee will attempt to acquire that information from publicly available information. Declining to provide a U.S. Social Security number may warrant completion of a SAR for the incident, although it is not, by itself, automatically and in all circumstances a suspicious activity that should trigger the filing of a SAR.

If the patron does not provide proper identification and/or required information, the casino should consider whether to continue engaging in transactions with that patron and whether the patron should be barred from further gaming activity until satisfactory identification and/or the required information is provided. A message recording the episode should be added to the patron's account in the management information system.

The same patron identification requirements apply to any person(s) who, acting as an Agent(s) for another person, performs transactions on behalf of that patron, and to any person who performs transactions in conjunction with that other patron, if the transactions trigger a CTR filing.

In those circumstances, both the person(s) conducting the reportable currency transactions as well as the person on whose behalf they are acting must provide the identification and required information described above. If any of these individuals cannot provide the identification and/or required information, that individual will be barred from further gaming activity, and the casino will consider filing a SAR.
For purposes of currency reporting, independent agents that contract with the casino are agents for the patron and not the casino if that designation has been established in the independent agent agreement. Independent agents should receive training on suspicious activity reporting.

Although separate from BSA/AML requirements, casinos should check whether patrons and related entities appear on the list of "Specially Designated Nationals" maintained by the Office of Foreign Assets Control of the U.S. Department of the Treasury.[2] Such due diligence may be conducted on a risk basis, and should encompass procedures for checking against updates to the OFAC list.

Ongoing Due Diligence

The casino's compliance policies should be calibrated to increase scrutiny of customer play and background in situations that pose greater risk of money laundering and the use of funds that may derive from criminal activity.

For high-volume patrons, whose activity (in terms of bills-in, marker play, or total play) exceeds a level determined by the risk assessment for that casino or who are otherwise identified as posing a risk of BSA/AML violations, the casino should review the patron's identity against public records and third-party database(s) to determine whether that person (or related entity):

- Is a Politically Exposed Person ("PEP");
- Is the subject of negative reports concerning possible criminal activity or doubtful business practices; or
- Has a prior criminal history, relevant to AML risk.

For high-volume patrons or transactions identified as possibly posing a risk of BSA/AML violations, the casino also may need to assess the source of the funds being used by the patron to gamble – whether they may derive from illegal activity or from legitimate sources. This may require the casino to obtain information concerning the patron's financial and business circumstances by querying public databases, through information-sharing arrangements with other financial institutions, or directly from the patron, to reach judgments whether the patron:

- Has sources of wealth commensurate with his or her gaming activity; and

[2] US persons and entities (including casinos) are prohibited from doing business with persons or entities designated by OFAC, and any assets of the designees must be "frozen" immediately.

- Has provided the casino with identification information and business-related information that can be readily confirmed.

Further due diligence may be warranted if the casino has information indicating that the patron:

- Has financial fiduciary obligations (*e.g.,* trustee, accountant, attorney, nonprofit/charity executive) that may create a risk of misappropriation or other illicit financial activity;
- Is associated with individuals or entities known to be connected with the illicit generation of funds;
- Claims connections with businesses that have no actual operations; or
- Otherwise may present an unacceptable risk of violating the BSA and related requirements or the casino's AML policies.

TRANSACTION MONITORING

On a regular basis, compliance personnel will complete a review of those transactions above thresholds determined by the risk assessment for that casino. As warranted by the facts of any situation reviewed, compliance personnel may further review third-party databases to determine the patron's business connections and history and any other information that will assist in explaining the patron's transactions or in determining the source of funds presented to the casino by the patron, in order to decide whether or not to file a SAR, and/or terminate the relationship. These circumstances may include the following:

- Patrons with large cash-in transactions with no cash-out transactions, which cannot be reasonably explained through transaction review (i.e., little or no gaming activity);
- Patrons with large cash-out transactions with limited cash-in transactions, which cannot be reasonably explained through transaction review;
- Patrons with large credit card advances with limited play;
- Patrons with multiple chip redemptions or cash buy-ins that are just below the CTR reporting threshold;
- Checks or wire transfers received for the benefit of the patron from third parties whose connection to the patron is not known;
- Multiple transactions over a period of time with the apparent purpose of avoiding BSA reporting requirements;
- A single payment received by the casino (e.g., negotiable instrument or wire transfer) for the benefit of multiple patrons; or
- Any other characteristic of the patron's activity that raises concern about possible BSA/AML issues.

Based on the result of due diligence reviews of high-volume patrons or of certain events identified by the risk assessment for that casino (e.g., the filing of one or multiple SARs for a patron, or the receipt of a law enforcement request for information concerning a patron), the casino may consider whether to terminate its relationship with a patron. The termination of a patron relationship will be warranted if the patron's activities present an actual or unacceptable risk of violation of Title 18, 1956 and 1957 and related requirements or the casino's AML policies.

In addition, Compliance personnel will conduct a review of relevant daily summaries, logs and reports, such as Marker Summaries, Front-Money/Safekeeping Summaries, multiple transaction logs, Monetary Instrument Logs and Check Logs to identify potential suspicious activity.

POTENTIAL SUSPICIOUS ACTIVITY

The BSA requires casinos to file a suspicious activity report (SAR) if the casino knows, suspects, or has reason to suspect that a transaction or attempted transaction aggregating at least $5,000 (i) involves funds derived from illegal activity; (ii) is intended to disguise funds or assets derived from illegal activity; (iii) is designed to avoid BSA reporting or recordkeeping requirements; (iv) involves the use of the casino to facilitate criminal activity, or (v) has no business or apparent lawful purpose; or (vi) is not the sort in which the particular patron would normally be expected to engage, and the casino knows of no reasonable explanation for the transaction after examining the available facts.

Given that the SAR rule encompasses attempted transactions, casinos should ensure that they track both attempted and completed transactions for potential SAR filings.
The following are examples of potentially suspicious situations that often will prompt consideration of whether a SAR should be filed under the casino's risk assessment criteria:

- Minimal gaming despite large financial transactions with the casino;
- Structuring of transactions to stay at or slightly below the $10,000 reporting threshold for CTRs;
- Placing currency in a slot machine, then cashing out after minimal or no play and redeeming the TITO ticket at a kiosk on the gaming floor ("bill stuffing");
- At a racing venue, inserting cash into a tote machine, cashing out for vouchers and then cashing vouchers at a teller's station with little or no wagering;
- A transaction that has no apparent business or lawful purpose (e.g., confederated gamblers placing offsetting bets on red and black on a roulette wheel);
- Presenting a third-party check or wire transfer – whether apparently deriving from a business or an individual – for payment of personal markers or for use in gambling-related activity in an amount at or above a threshold determined by the risk assessment for that casino. In such situations, the casino should ascertain whether the beneficiary (patron) has a documented connection to the sender (e.g., spouse or immediate family member or business with a documented and appropriate connection to the patron), either in the casino's records or by means of an Internet search or other reasonable inquiry. If no appropriate connection can be established between the source of the funds and the patron, those employees responsible for deciding whether to file a SAR also should consider whether or not to proceed with the transaction;
- A negotiable instrument or wire transfer is presented for the benefit of multiple patrons, or multiple patrons engage in play on a single patron account;
- A patron refuses to provide required information for the completion of a CTR, or identifying information more broadly;
- A patron requests information about how to avoid BSA reporting requirements;
- A patron leaves the gaming floor with a large volume of chips without any offsetting chip redemptions or chip buy-ins at another table. The transaction may not be deemed suspicious if there is a reasonable, experience-based expectation that the patron will

return to the casino in the near future. These situations may present different concerns depending upon whether the patron departs with chips acquired through a marker limit/credit transaction (sometimes called "chip walk"), or the patron takes chips won through gaming, or the patron takes chips initially purchased with his or her own funds.

- Patrons pass a large quantity of chips, cash, or TITO tickets between themselves in an apparent effort to conceal the ownership of the chips, cash, or TITO tickets; if patrons are closely related, such activity may not be suspicious;
- A patron presents funds in any form that derive from a foreign jurisdiction declared by the United States government to be a jurisdiction of concern for narcotics trafficking, human trafficking, money laundering, terrorism, or other illicit activity, or if the foreign jurisdiction has been identified as non-cooperative by the Financial Action Task Force, or by Transparency International as a country with a high degree of public corruption;[3]
- Law enforcement agencies deliver to the casino a formal request for records concerning the patron;
- News articles or other media reports alleged acts of financial wrongdoing by the patron;
- A patron raises his or her financial transactions to levels well above the ordinary levels for that patron;
- A patron requests establishment of an "AKA" account in a name other than the one by which the casino knows the patron;
- A patron attempts to deposit front money or to make payments using complex means, such as multiple sources of funds or multiple methods of transmission, which could mask the source of the funds transmitted; and/or
- A patron presents funds which the casino has a basis for suspecting to be the proceeds of illegal activity;

This list is by no means exhaustive; other patron activities may trigger BSA/AML concerns due to the circumstances in which they arise. Each casino should develop its own scenarios tailored to its business.

Further, the SAR requirement encompasses suspicious activity conducted by employees/insiders. Therefore, casinos should have adequate communication lines between the group(s) responsible for employee-related investigations and disciplinary issues, and the team(s) responsible for filing SARs.

SUSPICIOUS ACTIVITY REPORT REVIEW PROCEDURES

A suspicious activity report (SAR) review – aimed at determining whether a SAR should be filed for a situation – may be prompted by direct observations by property employees, by data analysis performed through back-of-house procedures, or by other means (e.g., incoming law enforcement inquiry).

On an annual basis and as part of its ongoing risk assessment, the casino should review its filed SARs for the previous year to analyze patterns of suspicious activity and develop guidelines for employees to apply going forward. The SAR review measures identified in this section ordinarily should be performed by AML/BSA compliance personnel.

[3] For example, see the State Department's annual International Narcotics Control Strategy Report and regulations and guidance issued by FinCEN.

- If prompted by direct observation, information about a transaction and the patron should be gathered promptly (e.g., patron name, Social Security number, player's card number, observed suspicious activity with supporting documentation) without alerting the patron that filing a SAR is being considered.
- The compliance officer or committee will examine the transaction in light of other available facts known about the patron or established during a due diligence review of the situation and the patron, plus the background or possible purpose of the transaction. Based on that investigation, the compliance officer may determine that there is a reasonable, non-suspicious explanation for the transaction and that no SAR should be filed, or that a SAR should be filed. In either event, the compliance officer will make a record of that review and its conclusions. The situation then may be reviewed by the casino's SAR Committee or those employees responsible for SAR filings. If that review determines that a SAR should not be filed, the reason for not filing should be documented.
- Among the further steps that may be warranted:
    - Review when a single patron conducted payments to or deposited funds with the casino through the use of multiple instruments deriving from more than one financial institution, in an aggregated amount exceeding a threshold determined by the casino's risk assessment, or in transactions spread over multiple days in an aggregated amount exceeding such a threshold;
    - Trace redeemed sports tickets above a certain transaction amount, consistent with the casino's risk assessment, to the original wagers to determine whether the patron redeeming the ticket was the same as the patron making the wager;
    - Ensure that the casino has identified those individuals (some of whom may be independent agents registered with state regulatory agencies) who have organized visits to the casino by patrons and that all patrons arriving due to the efforts of such individuals have been identified so that available funds for each patron are accurately reflected in the patron management system and the play of each patron is recorded as warranted;
    - For chip redemptions in excess of a threshold determined by the casino's risk assessment, examine recorded play to determine whether the patron had a significant value of unredeemed chips at the end of play and if the chips were obtained in a marker limit/credit transaction;
    - For front-money deposits and marker payments above a level consistent with the risk assessment for that casino, analyze that patron's deposit and payment patterns; and/or
    - If the casino participates in information sharing under Section 314(b) of the USA PATRIOT Act, it may contact officials at other participating casinos or banks or other financial institutions for additional information concerning a patron's business connections and other relevant matters.
- Receipts for purchased slot tickets will be reviewed by compliance personnel for method of payment from the patron. Tickets purchased with chips will be traced through the information system if the patron's redemptions exceed a threshold determined by the casino's risk assessment.
- Once a decision has been made to file a SAR, the fields on the SAR form must be completed correctly and thoroughly, and the narrative should be sufficiently detailed to explain the circumstances, individuals, and amounts involved. Explanatory documents

and other due diligence from the transaction/patron should, where appropriate, be attached to the SAR as part of the casino's recordkeeping processes.

- If a SAR is filed for a patron, compliance personnel should evaluate further activity by the patron for the following 90 days, and consider whether a continuing report of suspicious activity should be filed within 120 days of the previous SAR.
- When one or more SAR is filed for a patron's activities, casino management should consider whether the casino wishes to continue its relationship with that patron.
- Casinos also shall establish controls for maintaining the confidentiality of SARs and any information that reveals that a SAR was filed.

AUDIT PROCEDURES

The AML Program rule under the BSA requires independent testing of the casino's overall program, as well as specific functions, by qualified auditors. The independent test must cover all elements of the casino's AML program, including but not limited to: customer due diligence, transaction monitoring, required reporting and recordkeeping, training, and the AML Officer function.

Independent auditors of BSA/AML compliance (either external or internal to the casino) will have a reporting relationship to senior management officials with the authority to direct those corrective actions warranted by audit findings, in order to ensure the independence of the internal audit function. If the casino utilizes an internal audit function, that function must be independent from AML compliance. Casinos also may consider a reporting process to communicate to the Board of Directors the results of AML independent tests.

Special Testing Procedures for CTRs

On a scheduled basis, the casino's independent auditor or audit team for CTR filings will review currency transactions by using all relevant records, including but not limited to Multiple Transaction Logs (MTLs), player-rating records, and patron deposits and withdrawal records, that were prepared during the 24-hour reporting period, as well as all system reports for the period.

A detailed audit program should be maintained to document all audit procedures performed by independent auditors. After completion of the initial audit, a secondary review should be performed which should ensure (i) that a CTR has been prepared for all reportable transactions – either single or aggregated – that exceed $10,000; and (ii) that the information recorded on the CTR is complete and accurate. CTRs shall be electronically filed within 15 days of the transaction date.

The Negotiable/Monetary Instrument Log (MIL) will also be reviewed by independent auditors for proper completion and for retention for at least five years.

A system query should identify those patrons, if any, who inserted into a gaming device bill validator(s) funds in excess of a threshold determined by the casino's risk assessment. For patrons who have reached the log threshold for the gaming day, the total of their inserted bills shall be entered onto the multiple transaction log for reporting when required by law.

All currency transactions above an amount established by the risk assessment for that casino will be logged, with the exception of slot jackpots, which are not reportable on CTRs.

Exception notices will be prepared for all instances of noncompliance noted during the daily audit, including but not limited to logging errors, MIL completion errors, inaccurate identification, missing information and other requirements not met. The exception notices should be sent to applicable casino supervisory personnel at the conclusion of the independent audit and secondary review. Exception notices should be returned within a reasonable time indicating corrective action taken, and the results of these periodic audits should be part of the firm's overall independent testing.

Special Testing Procedures for SARs

The independent test function (whether internal or external) will establish testing parameters for both SAR and no-SAR decisions. This review will include completeness of investigation processes and documentation. In instances where SARs were filed, auditors will test completeness of SAR fields and narrative.

This review also should test the casino's monitoring systems (if appropriate) and how the system(s) fits into the casino's overall suspicious activity monitoring and reporting process. Auditors will test information flow across the casino, including but not limited to the fraud/security and host functions, as we as test whether information regarding employee misconduct is appropriately communicated to the group responsible for SAR decisions.

When evaluating the effectiveness of the casino's monitoring systems, auditors should consider the casino's overall risk profile (higher-risk products, services, customers, entities, and geographic locations), volume of transactions, and adequacy of staffing.

RECORDKEEPING AND RETENTION

The casino shall adopt a recordkeeping system to preserve -- for each patron who is the subject of customer due diligence procedures – (i) a record of those specific procedures performed to analyze a patron's gaming patterns and financial transactions; (ii) any due diligence report created; (iii) any risk determination; and (iv) any action taken as a result, including monitoring of patron, reports to law enforcement agencies, or changes in casino services available to the patron. Such records should be maintained for at least five years after the relationship is terminated.

The casino also shall maintain CTRs, SARs (and supporting documentation) for at least five years after filing. In order to assist law enforcement, the casino may elect to establish a protocol for receiving and responding to authorized requests for SAR supporting documentation without a subpoena.

CONCLUSION

These steps reflect the continuing efforts of the AGA members' commercial casino operators to mitigate the risks of money laundering and illegal activity connected with their businesses. The guidelines in this document must be adapted to match the specific circumstances of individual casinos and companies.

When dealing with businesses as complex as modern casinos, and with judgments as subjective as those required by the BSA, no compliance effort can be perfect or immune from retrospective re-evaluation.

Casinos should reconsider their AML/BSA compliance efforts on a regular basis to ensure they account for new risks and emerging patterns of illegal activity. Though perfection cannot be expected of a process that involves so many variables and periodic shifts in financial practices

and regulations, effective AML/BSA compliance programs should ensure that the gaming industry continues not to attract significant illegal money laundering activity.

GLOSSARY

Bank Secrecy Act ("BSA"): Adopted in 1970 and amended several times since, the statute authorizes the U.S. Secretary of the Treasury to impose on U.S. financial institutions the requirement to keep such records and submit such reports that have a high degree of usefulness in criminal, tax, and regulatory matters and in the conduct of intelligence activities to protect against international terrorism. 31 U.S.C. §§ 5311, et seq.

Cage: A secured area adjacent to the gambling floor of a casino where casino cashiers conduct marker/credit, front-money and other gambling-related transactions, and where currency and chips are often kept. Safe-deposit boxes are often available at the cage. A large casino may have more than one cage location.

Chip Walk: When a patron, after drawing upon a marker with the casino, leaves the casino floor with a significant amount of chips without offsetting chip redemptions or chip buy-ins at another table. "Chip walk" is distinct from situations in which a patron may take a significant amount of chips from the casino but those chips are the results of gambling wins ("walking with winnings") or are chips that the patron purchased with his or her own funds.

Credit: Under the regulations of many state licensing authorities, casinos are authorized to issue gaming chips or other representatives of value to patrons for gambling purposes up to the amount of a "marker" (see below), which is a negotiable instrument signed by the patron and made out to the benefit of the casino by the patron. Although state regulations refer to such arrangements as credit transactions, the markers may be negotiated immediately at the discretion of the casino.

Front money: Cash, wired funds, or negotiable instruments that are deposited with the casino by a patron who will draw down on those funds as he or she purchases chips for gambling. Front-money accounts are sometimes described as safekeeping accounts.

Marker: A negotiable instrument (sometimes called a "counter-check") executed by a casino patron and made payable to the casino that authorizes the casino to recover the amount of the marker from the patron's bank account. The casino will advance chips or TITO tickets to the patron up to the amount of the marker. Under state casino regulations, casinos are not required to conduct full credit investigations before issuing a marker, but will confirm that the patron's bank account contains sufficient funds to cover the requested marker.

Monetary Instrument Log: Required by the BSA, it must reflect transactions of monetary instruments (e.g., money orders, cashier's checks, traveler's checks and bank drafts) between the casino and the patron with a value above $3,000.

Multiple Transaction Log: This log, required by some state gaming regulations, should reflect cash-in or cash-out transactions at the casino of a predetermined amount while also recording identifying information about the patron.

Ticket In/Ticket Out ("TITO"): A system for slot machine play through the use of a barcoded paper ticket. The ticket may be purchased in advance of slot machine play, or issued from the slot machine if there are credits remaining at the conclusion of the patron's gaming session. When the patron has completed his play, balances on the ticket can be redeemed for cash at a kiosk or the casino cage, or used for further play at the casino that issued the ticket.